IEEE COMMUNICATIONS MAGAZINE

August 2017, Vol. 55, No. 8

- Advances in Optical Communications Technologies
- Software-Defined Vehicular Networks
- Fog Computing and Networking
- 5G Network Slicing

IEEE ComSoc IEEE Communications Society

A Publication of the IEEE Communications Society

www.comsoc.org

IEEE WCNC

IEEE | IEEE ComSoc
IEEE Communications Society

IEEE Wireless Communications and Networking Conference

15-18 April 2018 // Barcelona, Spain

LEADING THE WAY TO 5G AND BEYOND

CALL FOR SUBMISSIONS

IEEE WCNC 2018 will feature a comprehensive program with technical tracks on various aspects related to wireless research, technology, applications and services as well as workshops, tutorials, panel discussions and exhibits.

TECHNICAL PAPERS

Authors are invited to submit original technical papers in all areas of wireless communications, networks, services and applications. Potential areas include:

- PHY and Fundamentals
- MAC and Cross-Layer Design
- Wireless Networks
- Emerging Technologies, Architecture & Services

SUBMISSIONS DUE BY 15 SEPTEMBER 2017

TUTORIALS

Proposals for tutorials should focus on new and emerging topics within the scope of communications and networking.

PANELS

Proposals for panels should emphasize emerging topics of a particular interest to the industry and research communities in the field of wireless communications, networking, and associated applications and services.

For more information, visit **http://wcnc2018.ieee-wcnc.org**

IEEE COMMUNICATIONS MAGAZINE

AUGUST 2017, vol. 55, no. 8

www.comsoc.org/commag

IEEE COMMUNICATIONS MAGAZINE (ISSN 0163-6804) is published monthly by The Institute of Electrical and Electronics Engineers, Inc. Headquarters address: IEEE, 3 Park Avenue, 17th Floor, New York, NY 10016-5997, USA; tel: +1 (212) 705-8900; http://www.comsoc.org/commag. Responsibility for the contents rests upon authors of signed articles and not the IEEE or its members. Unless otherwise specified, the IEEE neither endorses nor sanctions any positions or actions espoused in *IEEE Communications Magazine.*

ANNUAL SUBSCRIPTION: $71: print, digital, and electronic. $33: digital and electronic. $1001: non-member print.

EDITORIAL CORRESPONDENCE: Address to: Editor-in-Chief, Osman S. Gebizlioglu, Huawei Technologies, 400 Crossing Blvd., 2nd Floor, Bridgewater, NJ 08807, USA; tel: +1 (908) 541-3591, e-mail: Osman.Gebizlioglu@huawei.com.

POSTMASTER: Send address changes to *IEEE Communications Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08855-1331. GST Registration No. 125634188. Printed in USA. Periodicals postage paid at New York, NY and at additional mailing offices. Canadian Post International Publications Mail (Canadian Distribution) Sales Agreement No. 40030962. Return undeliverable Canadian addresses to: Frontier, PO Box 1051, 1031 Helena Street, Fort Eire, ON L2A 6C7.

SUBSCRIPTIONS: Orders, address changes — IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855-1331, USA; tel: +1 (732) 981-0060; e-mail: address.change@ieee.org.

ADVERTISING: Advertising is accepted at the discretion of the publisher. Address correspondence to: Advertising Manager, *IEEE Communications Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08855-1331.

SUBMISSIONS: The magazine welcomes tutorial or survey articles that span the breadth of communications. Submissions will normally be approximately 4500 words, with few mathematical formulas, accompanied by up to six figures and/or tables, with up to 10 carefully selected references. Electronic submissions are preferred, and should be submitted through Manuscript Central: http://mc.manuscriptcentral.com/commag-ieee. Submission instructions can be found at the following: http://www.comsoc.org/commag/paper-submission-guidelines. All submissions will be peer reviewed. For further information contact Tarek El-Bawab, Associate Editor-in-Chief (telbawab@ieee.org).

BPA WORLDWIDE

IEEE ComSoc™
IEEE Communications Society

Join our Community!

IEEE

Networking • Conference Discounts • Technical Publications • Volunteer

Special Member Rates

50% off Membership for new members.

Offer valid March through 15 August 2017.

Member Benefits and Discounts

Valuable discounts on IEEE ComSoc conferences

ComSoc members save on average $200 on ComSoc-sponsored conferences.

Free subscriptions to highly ranked publications*

You'll get digital access to IEEE Communications Magazine, IEEE Communications Surveys and Tutorials, IEEE Journal of Lightwave Technology, IEEE/OSA Journal of Optical Communications and Networking and may other publications – every month!

*2015 Journal Citation Reports (JCR)

IEEE WCET Certification program

Grow your career and gain valuable knowledge by Completing this certification program. ComSoc members save $100.

IEEE ComSoc Training courses

Learn from industry experts and earn IEEE Continuing Education Units (CEUs) / Professional Development Hours (PDHs). ComSoc members can save over $80.

Exclusive Events in Emerging Technologies

Attend events held around the world on 5G, IoT, Fog Computing, SDN and more! ComSoc members can save over $60.

If your technical interests are in communications, we encourage you to join the IEEE Communications Society (IEEE ComSoc) to take advantage of the numerous opportunities available to our members.

Join today at www.comsoc.org

EVOLVING COMSOC'S TECHNICAL PORTFOLIO

Harvey Freeman

Heinrich Stüttgen

The driving force behind many of ComSoc's technical activities, such as publications and conferences, are its technical committees (TCs). Members of technical committees write papers, edit publications, organize meetings and conferences, and engage in other professional activities. Currently 26 technical committees cover most of ComSoc's technical field of interest. Although certain topics, and with it associated technical committees, may become obsolete over time, in reality technical committees tend to exist for a relatively long time evolving their technical area with the technology trends at hand. However, new technologies emerge all the time and not all of them are covered appropriately by the existing technical committees. To create a mechanism to allow ComSoc members, whether they are from academia, industry, or governments, to address new trends, ComSoc has established its Emerging Technologies Committee. ComSoc's ETC was first formed some 10 years ago to identify and promote new technology directions in the broader field of communications and related areas. While this is not intended, technical committees and Emerging Technology Initiatives (ETIs) accordingly today mostly focus on activities geared at the research community and do not cover activities relevant to our industrial membership equally well. The current Chair of the ETC is Heinrich (Heiner) Stüttgen.

Heinrich Stüttgen was a Fulbright scholar at the State University of New York at Buffalo (NY) from where he holds a Master of Science degree (1979). In 1984 he obtained a Doctor of Science degree in computer science from the University of Dortmund. In 1985 he joined the IBM Research and Development Laboratory in Germany, developing one of the first mainframe UNIX systems. In 1987 he moved to IBM's European Networking Center at Heidelberg, where he researched protocols for high-speed networks and multimedia communications. In July 1997 Heinrich joined NEC Europe Ltd. as founding manager of NEC's Network Laboratories in Heidelberg. Since June 2007 he has been Vice President of NEC Laboratories Europe, responsible for NEC's ICT related R&D activities in Europe, now focusing on network architecture, SDN/NFV, security and smart city related technologies, including the Internet of Things, data analytics and real world optimization problems.

Heinrich has widely published in various scientific conferences, journals and books. He was a guest lecturer at Mannheim University in computer networks and has been project auditor and proposal evaluator for the European Commission in the ICT area. Heinrich is an IEEE Fellow and an active volunteer within IEEE's Communications Society. Within IEEE ComSoc Heinrich has held various leadership positions.

ETC'S POSITION IN COMSOC

The ETC is a standing committee reporting directly to the Board of Governors (BoG) and the ComSoc President as well as the Vice President of Technical Activities. It consists of six members-at-large and a chair person, covering a wide range of technical fields. Every year two members "retire" and two new members are appointed. In 2017 the members are Shuguang (Robert) Cui (University of California at Davis), Gerhard Fettweis (Technical University of Dresden), Mathias Fischer (University of Hamburg), Thyaga Nandagopal (NSF), Besma Smida (University of Illinois), Tomohiko Taniguchi (Fujitsu Laboratories Kawasaki), and Heinrich Stüttgen (NEC Labs Heidelberg) as chair person. ComSoc members are encouraged to contact the ETC members directly to discuss related issues as well as to indicate their interest to contribute to and get involved in the ETC activities.

REGULAR ACTIVITIES OF THE ETC

Considering that it is rather difficult to predict and plan when new technologies arise and become relevant to larger groups of ComSoc's members such that a new ETI becomes of interest, the ETC works in two streams of activities. The first set of activities are supporting and reviewing activities of existing ETIs. The second and more irregular activities are those trying to generate new ETIs. Regarding existing ETIs, the ETC performs bi-annual reviews of the ETIs to track their activities and to recommend to the BoG elevation of the ETI to a full TC, to have another review two years later, or to disband. While in the past some ETIs (then called sub-committees) lived for many years without ever emerging as a full TC, a recent change in policy has been that every new ETI will be first reviewed after (roughly) two years, then elevated or be re-reviewed two years later. If it is still not elevated to TC after four years, that ETI will be disbanded. This policy has informally become known as the "Two-Plus-Two Up or Down Rule" and was first implemented in the 2016 ETI reviews. Based on this new policy only seven out of originally 15 ETIs continued to exist, while one ETI (Big Data) was elevated to TC and several others disbanded or merged. The currently active ETIs address the following topics:

- Backhaul/Fronthaul Networking & Communications
- Internet of Things (IoT)
- Nano-Scale & Molecular Networking
- Quantum Communications & Information Technology
- Software Defined Networking & Network Function Virtualization
- Tactile Internet
- Smart Grid

A second "regular" activity of the ETC is to edit a special issue each year in IEEE Communications Magazine addressing areas of particular relevance for the ETIs. In November 2017 the focus will be on software driven communications highlighting topics like Software Defined Networks and Network Function Virtualization (SDN/NFV), cloud communications and networking, as well as autonomic communications. The Call for Papers (CFP) generated high interest in the research community with more than 60 papers submitted for publications. For the 2018 issue the plan is to focus on Fronthaul/Backhaul Networks and Tactile Internet. The good turnout of the 2017 CFP will enable the related ETIs to better define their technical agenda as well as to establish a network of researchers working in the field such that the related ETIs gain critical mass to become full blown TCs. If the response to the CFP is too low, this may be an indication that the topic is not yet mature enough, already disappearing, or otherwise not attractive enough to sustain a TC.

GROWING THE COMSOC COMMUNITY: GENERATING NEW INITIATIVES

While the processes for supporting existing ETIs are well defined, there is no "one size fits all" process to generate new initiatives. The first question to address is whether a new topic is of growing interest to a larger community. The second is whether it should be rather pursued within an existing TC as part of the ongoing evolution of that TC, or whether it would be better addressed by a new ETI, bringing together experts from different TCs or not yet involved in ComSoc's technical activities. The third point that needs to be addressed is whether the topic is firmly grounded in ComSoc's (traditional) turf or whether it is a topic of overlapping interest with other societies. In recent years we have observed a growing softwarization of many communication technologies, topics like Cloud-Fog,-Edge Networking, SDN, NFV, SDR, etc. are good examples of this trend. Because of the change in implementation techniques, the borderline between societies, e.g. between the IEEE Communications Society and the IEEE Computer Society, is blurring. Consequently, the best venues to gather experts on these topics may be different today than they were in the past. In recent years most ComSoc TCs have been gathering at Globecom and ICC conferences. The center of gravity of these two ComSoc flagship conferences is in the lower, more transmission oriented communications areas. The above mentioned topics are new topics that are more closely related to the higher, more software oriented networking layers. Hence, it may be inconvenient trying to gather these researchers at venues where they may find relatively little related content in the conference program, and we should consider different conferences as meeting venues for these communities.

At the IEEE level a mechanism to initiate cross-society initiatives exists. Out of the IEEE Future Directions Committee, cross-society initiatives on GreenICT, Cloud, IoT, and others have emerged, which obviously are of interest to more than one society. At this time we do not have a process or scheme in place to link these cross-society initiatives with our technical committees and ETIs. ComSoc president Harvey Freeman has just initiated a small committee to work out this issue that is quickly gaining importance.

A second important aspect to consider is the different interests and requirements of our members from academia and industry. Their needs are different both in types of services, i.e., research conferences and publications on basic technologies as opposed to technology digests, standards and market trends, applications, training, and human networking platforms. However, there is also a difference in technical interest: whereas the mobile communications industry has a clear short-term target called "5G" to be deployed in the early 2020s, academic research often targets technologies five or 10 years away from deployment. Within ComSoc we have not been very successful bringing both communities together. The current 5G Initiative might be a positive exception here. Similarly successful initiatives in other areas such as Cloud/Edge/Fog or IoT are lacking, partially because we do not have the right structures in place to support this and partially because the communities are distinctly separate. Solving this issue will be vital to enable ComSoc to evolve into the future in an ever changing technological environment.

CURRENT STATE OF EMERGING TECHNOLOGY INITIATIVES

While we have disbanded several ETIs in 2016, we have failed to catalyze the formation of new ETIs at the same time, partly because of the problems described above, partly because our TC structure itself is historically grown and somewhat deficient without strategic perspective. Finally, a lack of awareness of the members about the available mechanisms to address new technologies and to start new initiatives within ComSoc may play a role.

HOW CAN YOU CONTRIBUTE?

Setting up a new Emerging Technologies Initiatives does not require much effort. It basically takes a group of supporting volunteers to define a technical scope and agree on an agenda for the next few years, such as organizing workshops and conferences, starting mailing lists or blogs, exchanging information related to the ETI's topics, conducting regular meetings to discuss ETSC matters, maintaining a website to make the ETI known to other ComSoc members, etc. Sometimes new topics come and go within a year or two. More often, however, the interest in a new topic or theme will be with us for several years. To get started you are encouraged to contact the ETC to set up a first discussion (Birds of a Feather Meeting) at one of our larger conferences to gather a community with a common interest and move it forward from there.

CONCLUSION

In this short article I have tried to summarize the structures and processes that ComSoc uses to incubate new technical activities within the Emerging Technologies Committee, including some of the structural problems ComSoc is facing with this approach. However, any community is only as agile and successful as the members that support it. If the ETI model is good for you, use it. If you have other ideas or suggestions, feel free to contact me by email or join any of the ETC meetings, which are typically held on the first day of ICC and Globecom.

5TH IEEE INTERNATIONAL BLACK SEA CONFERENCE ON COMMUNICATIONS AND NETWORKING

5-8 JUNE 2017, ISTANBUL, TURKEY

BY MEHMET ULEMA, ERDAL PANAYIRCI, SERHAT ERKUCUK, ROBERT SCHOBER

The 5th edition of this conference series took place on 5-8 June 2017, in Istanbul, Turkey. Istanbul is spread over two continents across the Bosphorus, which connects the Black Sea to the rest of the oceanic waters. Appropriately, the theme of the conference, "Connecting Black Sea to the Globe through Communications," fit well with the chosen venue.

The goal of the BlackSeaCom conference series is to bring together visionaries in academia, research labs and industry from all over the world to the shores of the Black Sea, and also to connect the researchers from the Black Sea region to the rest of the world.

Thanks to a great team effort and hard work, we put together an outstanding program, which included keynote presentations and tutorials by renowned industry and academic leaders, and top quality paper sessions (60+ paper presentations with zero no shows!) and demo sessions. (See the conference website: http://blackseacom2017.ieee-blackseacom.org)

We had three keynote speeches on forefront research topics:

•Prof. Mohamed-Slim Alouini, King Abdullah University of Science and Technology (KAUST), gave a talk on "Paving the Way Toward 5G Wireless Communication Networks."

•Prof. Thomas Magedanz, Technishe Universität Berlin, Germany, gave a talk on "Getting Ready for 5G and Edge Computing – Understanding the Role of ETSI MANO and OpenBaton."

•Prof. Erdal Arıkan from Bilkent University, Turkey, gave a talk on "Polar Coding for 5G."

We had four very interesting tutorials on diverse topics:

•"Signal Processing for Millimeter Wave Wireless Communications" by Prof. Nuria González Prelcic, University of Vigo, Spain.

•"Wi-Fi for 5G: Faster and Smarter" by Prof. Evgeny Khorov, Moscow Institute of Physics and Technology, Russia.

•"Backhaul/Fronthaul for Ultra-Dense HetNets: Requirements, Emerging Technologies and Industrial Practices" by Prof. Muhammad Zeeshan Shakir, University of the West Scotland, UK.

•"Flexible Radio Access Beyond 5G: A Future Projection" by Prof. Huseyin Arslan, University of South Florida, Tampa, FL, USA.

The Technical Program Committee did an enormous job in processing 129 submitted papers and managing the review process. Each paper was rigorously reviewed by three independent reviews, which led to a technical program of 62 very high quality papers distributed across 13 technical sessions on a broad range of topics on communications and networking. Accepted papers were published in the conference Proceedings and will also be published in IEEE Xplore. Three additional papers, not included in the Proceedings, have been selected for the demo session. We provided five students with travel grants.

EDAS was used for paper submission and processing. The papers were submitted from all over the world, including Europe, Asia/Pacific, Africa, America and the Middle East. Among authors who submitted papers, 60 percent hailed from countries around the Black Sea, and a total of 81 percent were from Europe and the Middle East. We are proud to see that our belief in the strength of the region is embodied in the resulting technical program. The technical program benefited from the valuable efforts of a large number of people to whom we are indebted. First, we thank all authors who kindly submitted their work to the conference. We also thank our distinguished Technical Program Committee members and reviewers who performed the arduous selection process.

IEEE BlackSeaCom 2017 would not have been possible without the tireless efforts of many people. All the Organizing Committee members devoted enormous time for a successful conference program preparation. We express our deep appreciation to our esteemed colleagues. The following is a list of the Organizing Committee.

General Co-Chairs: Erdal Panayirci, Kadir Has University, Turkey; Mehmet Ulema, Manhattan College, USA.

TPC Co-Chairs: Robert Schober, University of Erlangen-Nürnberg, Germany; Serhat Erkucuk, Kadir Has University, Turkey.

Industry Chair: Tuncer Baykas, Medipol University, Turkey.

Tutorials Chair: Wolfgang Gerstacker, University of Erlangen-Nürnberg, Germany.

Panel Sessions Chair: Tolga Duman, Bilkent University, Turkey.

Demo Sessions Co-Chairs: Metin Balci, Argela, Turkey; Larysa Globa National Technical University of Ukraine.

Publication Chair: Albena Mihovska, Aarhus University, Denmark.

Publicity Co-Chairs: Burak Kantarci, University of Ottawa, Canada; Carlos Becker Westphall, Federal University of Santa Catarina, Brazil; Yacine Ghamri Doudane, University of La Rochelle, France.

Finance Chair: Alex Gelman, Netovations, USA.

Treasurer: Bruce Worthman, IEEE Communications Society, USA.

Local Arrangements Chair: Taner Arsan, Kadir Has University, Turkey.

Webmaster: Tamer Dag, Kadir Has University, Turkey.

IEEE Turkey Section: Murat Uysal, Ozyegin University, Istanbul.

We are most grateful for the support of Kadir Has University (KHAS), located in Istanbul, Turkey. KHAS generously provided its premises to hold these activities.

This year IEEE BlackSeaCom in Istanbul was collocated with the IEEE 5G Summit. There was a strong synergy between these two events. Both were financially and technically successful. The IEEE 5G Summit Istanbul was attended by approximately 200 people and included distinguished speakers from industry, academia, and government organizations.

We think IEEE BlackSeaCom 2017 was a memorable experience from both professional and personal perspectives. There was a welcoming reception in the evening of the first day, and an unforgettable banquette on a boat on the Bosphorus in the evening of the second day. The conference was also successful financially, producing a surplus well above the ComSoc threshold. The number of total attendees was 83. The venue was excellent. The conference provided lunch and coffee break amenities as well.

The current plan is to hold the next IEEE BlackSeaCom in 2018 in Batumi, Georgia. We are always looking to strengthen the IEEE BlackSeaCom series and we are open to suggestions and volunteers. Please do not hesitate to contact us, the Steering Committee, with ideas and contributions.

REGISTRATION OPENS FOR IEEE VERTICAL AND TOPICAL SUMMIT
18-20 SEPTEMBER 2017, ANCHORAGE, ALASKA

With its dispersed population, cultural diversity, vast area, varied geography, climate extremes, importance to world ecosystems, and a richness of natural resources, Alaska is uniquely positioned to explore both the potential and challenges facing the Internet of Things (IoT) in its quest to create sustainable value. To facilitate this exploration in a global context, the IEEE IoT Multi-Society Technical Group has opened registration for a Vertical and Topical Summit at the Hilton Anchorage from 18-20 September 2017.

You should plan to attend this summit if you would like to understand IoT's revolutionary role and learn about practical applications in government, industry, and individual lives. Among the featured experts and decision-makers will be Anchorage Mayor Ethan Berkowitz, along with representatives from Cisco, Google, AT&T, Carnegie Mellon University, the U.S. Arctic Research Commission, the Department of Homeland Security, the Federal Bureau of Investigation, the University of Washington, and the IPv6 Forum. The University of Alaska is contributing organizational expertise.

These experts will focus on five vertical and five topical themes. The vertical themes are:

- Education
- Healthcare
- Arctic Region and Alaska Challenges
- Aviation and Unmanned Aerial Systems
- Oil, Gas, Natural Resources

The topical themes, applying to all vertical themes, are:

- Connectivity and Communications
- Big Data, Analytics and Artificial Intelligence
- Security and Privacy
- Economics of IoT and Sustainability
- Public Policy and Regulations

We look forward to your participation in our stimulating program. In addition to interactive sessions, there will be ample networking opportunities at a welcome reception and gala dinner. At the same time, we hope that you can take this opportunity to explore some of the wonders of Alaska near Anchorage or further afield. To register for this event, please visit http://anchorage2017.iot.ieee.org.

IEEE Collabratec™

Bright Minds. Bright Ideas.

Introducing IEEE Collabratec™

The premier networking and collaboration site for technology professionals around the world.

IEEE Collabratec is a new, integrated online community where IEEE members, researchers, authors, and technology professionals with similar fields of interest can **network** and **collaborate**, as well as **create** and manage content.

Featuring a suite of powerful online networking and collaboration tools, IEEE Collabratec allows you to connect according to geographic location, technical interests, or career pursuits.

You can also create and share a professional identity that showcases key accomplishments and participate in groups focused around mutual interests, actively learning from and contributing to knowledgeable communities. All in one place!

Network.
Collaborate.
Create.

Learn about IEEE Collabratec at
ieeecollabratec.org

IEEE

GCN GLOBAL COMMUNICATIONS NEWSLETTER

August 2017
ISSN 2374-1082

CHAPTER REPORT

Distinguished Lecturer Tour of Professor Albert Banchs in Central America and Mexico

By Carlos Eugenio Martínez-Cruz, El Salvador Chapter Vice Chair

Since October 2016 ComSoc colleagues from Guatemala and Mexico have been trying to organize a tour for one of our Distinguished Lecturers. In November 2016, by chance we met at the Regional Chapter Chairs Congress for Latin American Region, held in Medellin, Colombia. There, four of our chapters decided to request the visit of one of our finest speakers, professor Albert Banchs. From both sides of the Atlantic Ocean emails started to interchange. After several dozen electronic communications, a schedule was confirmed. He would visited Guatemala, El Salvador and two Mexican cities from March 26 to April 4.

From Guatemala, Albert Banchs arrived in El Salvador on March 28. I personally went to pick him up. Previously, I had warned I would be carrying a big IEEE poster with me. There I was, elbow to elbow, among taxi drivers who happen to be waiting for arriving travelers to take them to San Salvador's hotels. In the taxi, on our way to San Salvador, during the long one hour trip from the airport to the city, there was a lot of time to talk. We found out that for three years, unknowingly, we were researchers at the same university, in the same faculty and in the same building. He was in the Department of Computer Networks and I, one floor above, was in the Department of Signal Theory and Communications. We never met each other and I have no recollection of having seen him before. However, we share many stories in common. The world is very small and this is how IEEE and its societies always put us together.

The first talk was given on March 29 at 10 o'clock in the morning at the Universidad Don Bosco. This private university is 15 kilometers east of San Salvador, and holds one of the best engineering schools in the country. Besides students from the host university, there were students from the Universidad de El Salvador where, recently, a new student ComSoc chapter was founded. The subject of the talk was "Offloading Cellular Traffic through Opportunistic Communications." Professor Banchs explained some very disruptive technologies that would break with very established paradigms in the world of mobile communications. Opportunistic communication has to consider the random mobility of the network members, which makes it very unreliable, and a solution is challenging. Professor Banchs addressed optimization approaches. It was very interesting that one of its solutions is based on an adaptive control theory algorithm.

Lecture of Professor Banchs in San Salvador, El Salvador.


Professor Banchs (right) received a diploma of recognition.

In the afternoon a second meeting was held. This time the audience was made up of industry professionals. More than 40 people attended the meeting. The subject of the talk was "A Global Vision of 5G Mobile Networks and the Network Slicing Technology." At the end of the talk many questions were asked by the attendees. People from our local government regulator were very interested in learning about these new mobile communication technologies, as were local communication engineers. 4G deployment has just started very recently, so they wanted to know what the future would look like. At the end cocktails were offered by a local company called SETISA and the American manufacturer Keysight Technologies.

On Thursday, March 30, Banchs departed to Mexico. His first destination was the city of Puebla. The Puebla ComSoc chapter organized the talk at Complejo Cultural Universitario. On Sunday, April 2, he made his last stop of the tour at Cuernavaca City, hosted by the Morelos ComSoc chapter. People were very happy with Albert Banchs. He is a great lecturer, a fine speaker, and a very special person.


Professor Banchs gave a talk at Universidad Don Bosco, Soyapango, El Salvador.

CHAPTER REPORT

IEEE ComSoc Lahore Section Celebrates World Telecom Day 2017 in Pakistan

By Kashif Bashir, Chair, IEEE ComSoc Lahore Section, Pakistan

IEEE Communication Society Lahore Section and KICS-UET organized World Telecommunication Day (WTC) on 16 May 2017. The event was held at Seminar Hall at the University of Engineering and Technology Lahore, embraced by many high-ranking officials and experts from academia and industry. The event, which had the theme "Big Data for Big Impact," was attended by: Mr. Kashif Bashir, IEEE ComSoc Lahore Section Chair, Edwart Zhang, Vice President of Huawei Technologies China, Mr. Javed Aslam, EVP Technical PTCL, Dr. Amjad Hussain, Director, Fast University, Mr. Sajjad Kirmani, CEO, Infogistic, Mr. Fysal Gill, Senior Director, SpeedCast, Prof. Dr. Waqar Mahmood, Director KICS, Mr. Moeez Ahmad Faizi, and the Deputy Chief, Telecom Punjab Safe City Authority. The purpose of WTD was to highlight the importance of communication in our lives.

The event began with a video message by Prof. Dr. Vincenzo Piuri, who is a full professor at the University of Milan, Italy. He emphasized the importance of Big Data in today's world and thanked the organizers for organizing the World Telecom Day 2017 at KICS UET Lahore.

The chief guest of the occasion, Edward Zhang, Vice President of Huawei Enterprise Wireless Solutions, spoke about the strong friendship between Pakistan and China and how beneficial it has been since the outset in terms of business development between the two countries. He also spoke about ICT solutions, and Huawei Pakistan's functions. Mr. Zhang then presented an overview of the Safe City Project Lahore, and the Smart City Services Development and IoT Services.

Javed Aslam, Executive Vice President Technical PTCL, expressed his views on "How PTCL Connects us to the World."

Edward Zhang, bottom left, with attendees.

Amjad Hussain, Chair of the IEEE Lahore Section and Director of FAST, presented his views on technology enhancements and communication development.

Fysal Gill, Head SpeedCast (Central & South Asia), talked about topics such as GPRS technology and satellite systems.

Sajjad Kirmani, CEO Infogistic, discussed his views on legacy systems, advancements in technology, cloud computing, and the explosive growth of telecom in Pakistan.

Moeez Ahmad Faizi, Deputy Chief of Telecommunication, Punjab Safe City Authority, discussed the safe city projects and speed connectivity.

Prof. Fazal Ahmad Khalid, Vice Chancellor of UET Lahore, thanked the guests and stressed the importance of technology in today's world. He also made special mention of Huawei's collaborations with UET.

Prof. Waqar Mahmood, Director of KICS, also spoke about the importance of Big Data and gave a presentation on the IEEE and the KICS' Labs.

The event concluded with the distribution of souvenirs among the guests.

A post panel discussion followed in which the distinguished guests and high-ranking officials of the Al-Khawarazmi Institute discussed their views on the impact of Big Data. Kashif Bashir, IEEE ComSoc Chair and Manager at HUTIC, elaborated on Big Data's impacts on the masses and told the panel about conducting more events like these in the future. He also thanked all the guests and members of IEEE who attended this event.

Edward Zhang, fifth from left, with attendees.

MEMBER AND GLOBAL ACTIVITIES

ITU/APNIC Internet and IPv6 Infrastructure Security Program, May 2017, Nonthanburi, Thailand

By Leo Hwa Chiang and Ewell Tan, IEEE APO Office, Singapore

On behalf of IEEE ComSoc, the Director of IEEE Asia Business Development, Leo Hwa Chiang, jointly organized a one-week "Internet and IPv6 Infrastructure Security Program" with the International Telecommunication Union (ITU), the Asia Pacific Network Information Centre (APNIC), and the Ministry of Digital Economy and Society (Thailand). This training program was held at the TOT Academy, Nonthanburi, Thailand on the 8–12 May 2017.

With the explosive growth of smart IT devices and the increasing popularity of cloud computing and the Internet of Things (IoT), IPv6 is becoming a critical innovation for future Internet communications. In view of this growing demand, this program is essential to the policy makers, regulators, telecom operators and enterprise network administrators to build their skills and knowledge regarding the deployment and management of IPv6 network infrastructure, especially as it relates to security.

The training program at TOT Academy.

This program was well attended by 40 participants from 18 countries, including Afghanistan, Bangladesh, Bhutan, Brunei, Cambodia, India, Indonesia, Iran, Laos, Malaysia, Mongolia, Pakistan, Philippines, Qatar, Sri Lanka, Sudan, Thailand and Vietnam. This intensive training program was conducted by Philip Smith,

(Continued on Newsletter page 3)

REGIONAL ACTIVITIES

IEEE Spain Section Student Branch - Women in Engineering and Young Professionals (SWYP'17)

By Josemaría Malgosa, Maite Torres, Juan Pedro Muñoz, Pilar Manzanares, Universidad Politécnica de Cartagena, Spain

Among the most interesting and promising organizations developed in the IEEE as a regional organization are the student branches. They provide an opportunity for students to begin networking in their areas of interest and future profession. They also carry out activities related to bringing engineering closer to society. Most of these activities are focused on schools, where they seek to demystify the dark and serious image that most students have of engineering work. Not surprisingly, when pupils realize the wide variety of applications that can be developed with current market technology (mobiles, drones, Arduino, Odroid, etc.), they take their studies a little more seriously.

The youth of their members provides many benefits to the IEEE, including the fact that most of the high quality scientific publications of the IEEE conferences and journals come from the hard work of pre-doctoral students. However, their youth also gives them a touch of inexperience. This may explain why some seem to think they constitute a sort of second-order organization. However, the amount, interest and frequency of their activities reveal rather the contrary.

The Spain section of the IEEE includes all the student branches of every Spanish university. All of them have a well defined regulation that, in short, provides them with the legal framework within which to develop their activities. Recently, however, this framework has changed a little in order to better suit the growth of the student branches. To date there has been one Section Student Representative (SSR) in Spain, who has been in charge of both supervising the activities of the branches and creating new ones. However, to support the SSR in his management tasks, this year all branches have agreed on a less centralized management with the incorporation of four additional coordinators.

One of their main tasks is the organization of the annual congress known as Student Branch, Women in Engineering and Young Professionals (SWYP, formerly Congreso Nacional de Ramas, also known as CNR). The first session of the SWYP was held in Granada, Spain on March 9-11. The SWYP gave members an opportunity to share their expertise, but even more important, a platform to discuss the challenges they face and different ways to deal with them. In addition, there were several presentations on the topics of both Women in Engineering and Young Professionals, which were very interesting in giving a different view on the roles that women are able to play in engineering as well as new future working opportunities. Finally, the SWYP is also in charge of monitoring the activities of all branches. The assessment takes into account indicators such as the number of projects and dissemination activities developed, the quality of the web page of the student branch, and so on. It is not an easy task, since all branches have done good work. This could explain the surprising fact that this year there were two winners in a hard-fought tie: The Universitat de València and the Universidad Miguel Hernández, both of them located in the València region of Spain.

The next SWYP congress will be held in Cartagena, Spain. We all wish the very best for this and future SWYP meetings.

Some of the participants in the SWYP'17 happily posing for a group-photo in front of the Cathedral of Granada (Spain).

GCN GLOBAL COMMUNICATIONS NEWSLETTER

STEFANO BREGNI
Editor-in-Chief
Politecnico di Milano — Dept. of Electronics and Information
Piazza Leonardo da Vinci 32, 20133 MILANO MI, Italy
Tel: +39-02-2399.3503 — Fax: +39-02-2399.3413
Email: bregni@elet.polimi.it, s.bregni@ieee.org

FABRIZIO GRANELLI
Associate Editor-in-Chief
University of Trento
Email: fabrizio.granelli@unitn.it

IEEE COMMUNICATIONS SOCIETY

STEFANO BREGNI, VICE-PRESIDENT FOR MEMBER AND GLOBAL ACTIVITIES
CARLOS ANDRES LOZANO GARZON, DIRECTOR OF LA REGION
SCOTT ATKINSON, DIRECTOR OF NA REGION
ANDRZEJ JAJSZCZYK, DIRECTOR OF EMEA REGION
TAKAYA YAMAZATO, DIRECTOR OF AP REGION
CURTIS SILLER, DIRECTOR OF SISTER AND RELATED SOCIETIES

REGIONAL CORRESPONDENTS WHO CONTRIBUTED TO THIS ISSUE

JOSEMARIA MALGOSA SANAHUJA (josem.malgosa@upct.es)
EWELL TAN, SINGAPORE (ewell.tan@ieee.org)

IEEE ComSoc IEEE Communications Society

www.comsoc.org/gcn
ISSN 2374-1082

ITU/APNIC INTERNET AND IPV6/*Continued from page 2*

Fakrul Alam and Ashish Narayan, with topics covering IPv6 security issues, deployment challenges, policy considerations, operator experience, and transition technology. Through a series of case studies, working group exercises and hands on lab work, upon completion of this training program, participants had acquired the skills to manage IPv6 Internet infrastructure security threats, and had learned methods for network monitoring and configurations. This program was very informative as it gave the participants an in-depth understanding of Internet infrastructure security, particularly focusing on the similarities and differences between IPv4 and IPv6.

UPDATED ON THE COMMUNICATIONS SOCIETY'S WEB SITE

www.comsoc.org/conferences

2017

AUGUST

ISWCS 2017 — Int'l. Symposium on Wireless Communication Systems, 28–31 Aug.
Bologna, Italy
http://iswcs2017.org/

SEPTEMBER

ITC29 2017 — International Teletraffic Congress, 4–8 Sept.
Genoa, Italy
https://itc29.org/

IEEE CSCN 2017 — IEEE Conference on Standards for Communications & Networking, 5–7 Sept.
Helsinki, Finland
http://cscn2017.ieee-cscn.org/

ICACCI 2017 — Int'l. Conference on Advances in Computing, Communications and Informatics, 13–16 Sept.
Udupi, India
http://icacci-conference.org/2017/

IEEE Sarnoff Symposium 2017, 18–20 Sept.
Newark, NJ
https://ewh.ieee.org/conf/sarnoff/2017/

SOFTCOM 2017 — Int'l. Conference on Software, Telecommunications and Computer Networks, 21–23 Sept.
Split, Croatia
http://softcom2017.fesb.unist.hr/

IEEE CLOUDNET 2017 — IEEE Int'l. Conference on Cloud Networking, 25–27 Sept.
Prague, Czech Republic
http://cloudnet2017.ieee-cloudnet.org/

OCTOBER

I3C 2017 — IoT Int'l, Innovation Conference, 5–7 Oct.
Saodoa. Morocco
http://i3c2017.emena.org/index.html

IEEE PIMRC 2017 — IEEE Int'l. Symposium on Personal, Indoor & Mobile Radio Communications, 8–13 Oct.
Montreal, Canada
http://pimrc2017.ieee-pimrc.org/2015/08/21/sample-news-post/

IEEE CNS 2017 — IEEE Conference on Communications and Network Security, 9–11 Oct.
Las Vegas, NV
http://cns2017.ieee-cns.org/

HONET-ICT 2017 — Int'l. Conference on Smart Cities: Improving Quality of Life Using ICT & IoT, 9–11 Oct.
Irbid, Jordan
http://honet-ict.org/

WCSP 2017 — Int'l. Conference on Wireless Communications and Signal Processing, 11–13 Oct.
Nanjing, China
http://www.ic-wcsp.org/

CyberC 2017 — Int'l. Conference on Cyber-Enabled Distributed Computing and Knowledge, 12–14 Oct.
Nanjing, China

IEEE HEALTHCOM 2017 — IEEE Int'l. Conference on e-Health Networking, Application & Services, 12–15 Oct.
Dalian, China
http://healthcom2017.ieee-healthcom.org/

IEEE SmartGridComm 2017 — IEEE International Conference on Smart Grid Communications, 16–19 Oct.
Dresden, Germany
http://sgc2017.ieee-smartgridcomm.org/

CSNet 2017 — Cyber Security in Networking Conference, 18–20 Oct.
Rio de Janeiro, Brazil
http://csnet2017.dnac.org/

ICTC 2017 — Int'l. Conference on Information and Communication Technology Convergence, 18–20 Oct.
Jeju Island, Korea
http://ictc2017.org/

ATC 2017 — Int'l. Conference on Advanced Technologies for Communications, 18–20 Oct.
Quynhon, Vietnam
http://atc-conf.org/

INTEC 2017 — Int'l. Conference on Internet of Things, Embedded Systems and Communications, 20–22 Oct.
Gafsa, Tunisia
http://www.iintec.org/

IEEE/CIC ICCC 2017 — IEEE/CIC Int'l. Conference on Communications in China, 22–24 Oct.
Qingdao, China
http://iccc2017.ieee-iccc.org/

MILCOM 2017 — Military Communications Conference, 23–25 Oct.
Baltimore, MD
http://events.afcea.org/milcom17/public/enter.aspx

Fog World Congress 2017, 30 Oct.–1 Nov.
Santa Clara, CA
http://www.fogworldcongress.com/

NOVEMBER

WINCOM 2017 — Int'l. Conference on Wireless Networks and Mobile Communications, 1–4 Nov.
Rabat, Morocco
http://www.wincom-conf.org/?p=welcome

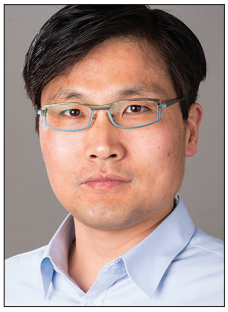
IEEE NFV-SDN 2017 — IEEE Conference on Network Function Virtualization and Software Defined Networks, 6–8 Nov.
Berlin, Germany
http://nfvsdn2017.ieee-nfvsdn.org/

FRUCT21 2017 — Conference of Open Innovations Association (FRUCT) 2017, 6–10 Nov.
Helsinki, Finland
http://fruct.org/conference21

–Communications Society portfolio events appear in bold colored print.
–Communications Society technically co-sponsored conferences appear in black italic print.
–Individuals with information about upcoming conferences, Calls for Papers, meeting announcements, and meeting reports should send this information to: IEEE Communications Society, 3 Park Avenue, 17th Floor, New York, NY 10016; e-mail: p.oneill@comsoc.org; fax: + (212) 705-8996. Items submitted for publication will be included on a space-available basis.

FOG COMPUTING AND NETWORKING: PART 2


Mung Chiang


Sangtae Ha


Chih-Lin I


Fulvio Risso


Tao Zhang

Due to the large number of submissions responding to the Call for Papers on "Fog Computing and Networking," the Guest Editors selected additional papers based on reviewer comments that are now published in Part 2. The overview provided by the Guest Editors in the form of Q&A was published in Part 1 in April. Here, in this August issue of the magazine, we continue to see a range of perspectives, some qualitative and others quantitative. Collectively, they expand the scope of edge research labs that started a decade ago to the current momentum in fog research and deployment and academia-industry collaboration such as the OpenFog Consortium. In the following, we briefly overview the articles in this issue.

In "Architectural Imperatives for Fog Computing," the author presents an industry perspective on the use cases, requirements, and techniques for the fog-enabled Internet of Things (IoT). Driven especially by latency-sensitive applications, the author discusses a list of attributes that are useful for such fog networks. Some of these are natural advantages of fog: lower latency, reduced network bandwidth usage, enhanced security and privacy, geographic locality of control, data rich mobility, reliability and robustness, support for analytics and automation, hierarchical organization, energy efficiency, and so on, while others are desirable goals to achieve in designing fog networks: scalability, agility, modularity, and openness.

In "IoT Stream Processing and Analytics in the Fog," the authors present the general models and architecture of fog data streaming services by analyzing the common properties of several typical applications. Based on the above considerations, they analyze the design space of streaming services by focusing on four essential dimensions: system, data, human, and optimization. In this respect, the article presents both the new design challenges and the issues that may arise when leveraging existing techniques, such as cloud stream processing, computer networks, and mobile computing.

"The Unavoidable Convergence of NFV, 5G, and Fog: A Model-Driven Approach to Bridge Cloud and Edge" argues that fog computing will become part of the convergence between IoT, network functions virtualization (NFV), and fifth generation (5G). As a consequence, the article introduces an architecture that offers uniform management of IoT services spanning the continuum from the cloud to the edge that is compliant with European Telecommunications Standards Institute (ETSI) management and orchestration (MANO). The proposed architecture also introduces the first YANG models for fog nodes for IoT services involving cloud, network, and/or fog, and expands the concept of "orchestrated assurance" to provision carrier-grade service assurance in IoT. Finally, the article discusses the application of the proposed model in a pilot in the Spanish city of Barcelona.

Also, "TelcoFog: A Unified Flexible Fog and Cloud Computing Architecture for 5G Networks" proposes a novel convergent architecture that targets the extreme edge of a wired/wireless network and is particularly suitable for low-latency services. The architecture includes a scalable computing node, operating at the edge of the network, and a controller, aimed at guaranteeing service assurance and based on YANG data models.

"A Fog Operating System for User-Oriented IoT Services: Challenges and Research Directions" presents the high-level introduction of a fog computing architecture for IoT services, FogOS. It is composed of service/resource abstraction, a resource manager, an application manager, and edge resource identification/registration. The article further identifies some of the challenges facing IoT services and possible solutions through FogOS; notably, how the diversity and heterogeneity of IoT services and edge devices can be managed.

In "A Hierarchical Game Framework for Resource Management in Fog Computing," the authors consider a scenario with three types of entities: fog nodes (FNs), authorized data service subscribers (ADSSs), and data service operators (DSOs). Resources in FNs are owned by independent users or providers. ADSSs request data from DSOs in the cloud, which communicate with FNs. This is a particular realization of fog-cloud interaction. The authors propose a three-layer hierarchical game, with three types of game theoretic models for each of the three pair-wise interactions, leveraging the specific nature of the interaction in each case. The goal is to obtain stable and optimal utilities for three parties in a distributed way.

BIOGRAPHIES

MUNG CHIANG (chiangm@princeton.edu) is the Arthur LeGrand Doty Professor of Electrical Engineering at Princeton University. He serves as the inaugural chairman of the Princeton Entrepreneurship Council and director of the Keller Center for Innovation in Engineering Education. The recipient of a Waterman Award, an IEEE Tomiyasu Award, and a Guggenheim Fellowship, he works in areas such as NUM, SDP, and fog. He created the Princeton Edge Lab and co-founded the OpenFog Consortium. His MOOC has reached 250,000 people, and his textbook received an ASEE Terman Award.

SANGTAE HA is an assistant professor in computer science at the University of Colorado Boulder. He received his Ph.D. in computer science from North Carolina State University. He is a co-founder and founding CTO/VP Engineering of DataMi, a mobile network startup. His research focuses on building and deploying practical network systems. He received the INFORMS ISS Design Science Award in 2014, and serves as an Associate Editor for the *IEEE Internet of Things Journal*.

CHIH-LIN I received her Ph.D.E.E. from Stanford University. She is CMCC Chief Scientist of Wireless Technologies, launched 5G R&D in 2011, and leads the C-RAN, Green, and Soft initiatives. She was on the IEEE ComSoc Board, GreenTouch EB, and was IEEE M&C Board Chair and WCNC SC Founding Chair. She is on the IEEE 5G Initiative SC and is Publication WG Chair, ComSoc SPC and SDB, ETSI/NFV NOC, WWRF SB, and Singapore NRF SAB. She received the *IEEE Transactions on Communications* Best Paper Award and the ComSoc Industrial Innovation Award.

FULVIO RISSO (Italy, 1971) received his B.Sc. and Ph.D. degrees from Politecnico di Torino, Italy, in 1995 and 2000, respectively. Since 2000, he has been with Politecnico di Torino, where he is currently an associate professor and in charge of the Network and Multimedia Lab. His main areas of research interest are high-speed and flexible in-network processing, SDN, and NFV. He is an author of 90+ papers and is very active in open-source software, starting with WinPcap in 1999.

TAO ZHANG [F] joined Cisco in 2012 as the chief scientist of its Smart Connected Vehicles business. He is a cofounder and Board Director of the Open Fog Consortium, and CIO and a member of the Board of Governors of IEEE Communications Society. He has been directing R&D for over 25 years, holds 50+ U.S. patents, and has co-authored two books, *Vehicle Safety Communications: Protocols, Security, and Privacy* (2012) and *IP-Based Next Generation Wireless Networks* (2004).

Architectural Imperatives for Fog Computing: Use Cases, Requirements, and Architectural Techniques for Fog-Enabled IoT Networks

Charles C. Byers

Fog computing is an architecture that extends the traditionally centralized functions of cloud computing to the edge and into close proximity to the things in an Internet of Things network. The author discusses some of the more important architectural requirements for critical Internet of Things networks in the context of exemplary use cases, and how fog computing techniques can help fulfill them.

ABSTRACT

Fog computing is an architecture that extends the traditionally centralized functions of cloud computing to the edge and into close proximity to the things in an Internet of Things network. Fog computing brings many advantages, including enhanced performance, better efficiency, network bandwidth savings, improved security, and resiliency. This article discusses some of the more important architectural requirements for critical Internet of Things networks in the context of exemplary use cases, and how fog computing techniques can help fulfill them.

INTRODUCTION

Fog computing is an architectural construct in Internet of Things (IoT) networks, built on the foundations of well-known technologies including cloud computing, distributed control systems, cloudlets, industrial networks, and wireless infrastructure. Where many information technology (IT) and IoT architectures seek to move the intelligence as far up into the cloud or as deep into intelligent endpoint devices ("things") as they can, the fog architecture places computation, networking, and storage resources in a hierarchy of levels arranged between the cloud and the things. The focus of this article is on key requirements for fog computing, and architectural techniques to satisfy them. There are many exemplary use cases where the advantages of fog computing are clear, leading to a set of architectural imperatives for moving applications to fog. Once the *architectural imperatives* are well understood, it is possible to partition systems into their fog elements, and generate effective system architectures and high-level designs for those elements. The basic elements of fog computing, called fog nodes, can be designed and deployed in many ways to best fit the needs of the IoT applications that run on them.

Architecture in this context is the arrangement of physical and logical network elements, hardware, and software to implement a useful IoT network. Key architectural decisions involve the physical and geographical positioning of fog nodes, their arrangement in a hierarchy, the numbers, types, topology, protocols, and data bandwidth capacities of the links between fog nodes, things, and the cloud, the hartware and software design of individual fog nodes, and how a complete IoT network is orchestrated and managed. In order to optimize the architecture of a fog network, one must first understand the critical requirements of the general use cases that will take advantage of fog and specific software application(s) that will run on them. Then these requirements must be mapped onto a partitioned network of appropriately designed fog nodes. Certain clusters of requirements are difficult to implement on networks built with heavy reliance on the cloud (intelligence at the top) or intelligent things (intelligence at the bottom), and are particularly influential in the decision to move to fog-based architectures. I call these decision criteria *architectural imperatives for fog computing*. Understanding these architectural imperatives and effectively addressing them in IoT network architectures and network element high-level designs should allow the reader to more effectively implement IoT systems able to meet the critical requirements of their applications.

Foundational work for distributed intelligence in operations networks has a rich history, dating from well before cloud, IoT, or fog. Examples of this history include distributed intelligent systems in the space program, voice telephone networks, fly-by-wire systems, and industrial programmable logic controllers for machine automation. The cloudlet work at Carnegie Mellon University [1] is highly influential in its consideration of latency impact of the cloud and reducing it via distributed intelligence. The MAUI project at Microsoft Research [2] addresses several problems in mobile devices, including energy use for computational tasks

Much of the groundwork for fog computing in its current incarnation was presented by Flavio Bonomi, Rodolfo Milito, *et al.* in [3]. Several standardization efforts, including mobile edge computing [4], the Industrial Internet Consortium [5], central office re-architected as a data center (CORD) [6], and OpenEdge computing [7] have focused on edge computing in specific markets. Finally, the OpenFog Consortium [8] has been launched to focus on open models for fog computing across the entire IoT ecosystem, and has produced a valuable white paper [9] and reference architecture.

Digital Object Identifier:
10.1109/MCOM.2017.1600885

Charles C. Byers is with Cisco Systems, Inc.

0163-6804/17/$25.00 © 2017 IEEE

The following section of this article is an overview of fog network architecture, as background for the discussion of architectural imperatives. Then we describe a set of architectural imperatives in detail, including exemplary use cases, and quantifiable requirements derived from these use cases. The final section is a discussion and conclusions.

Fog Computing Network Overview

Fog computing is applicable to a wide variety of potential IoT use cases, serving many key vertical markets. Table 1 lists some examples of the vertical markets, with several selected use cases in each market that have requirements to which fog techniques are potentially applicable. The list of markets and use cases is by no means exhaustive. It is more illustrative of the sorts of problems fog can help solve. Many of these use cases will experience significant challenges (or perhaps be impossible to satisfactorily implement) without the use of fog techniques. The last column lists by letter some of the architectural imperatives (to be described in detail below) that are especially important to each vertical. Some verticals care (at least to some extent) about all architectural imperatives.

A fog computing network architecture is shown in Fig. 1. Fog nodes are located in a logical and physical hierarchy, arranged in layers between the cloud on top and the IoT things at the bottom. Their symbol is similar to the graphics used for edge routers, but also contains the "C," "N," and "S" glyphs to remind us that they each implement distributed computation, networking, and storage capabilities. Fog nodes in this network cooperate to implement distributed IoT applications.

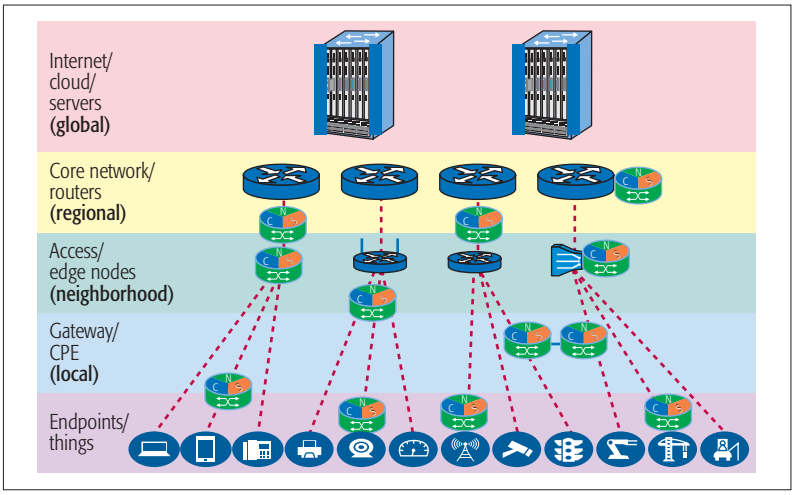


Figure 1. Fog computing network architecture.

IoT vertical	Example fog-enabled use cases	Imperatives
Transportation	Smart roads, autonomous vehicles, PCT/rail, parking, UAV ground support , maritime, ports, logistics	A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q
Utilities	Smart grid, smart meters, water distribution, sewer monitoring, energy management, renewables	A, B, C, D, F, G, H, J, L, N, O, P
Smart cities/smart buildings	City-level fog, smart buildings, lighting, emergency services, sanitation, carpeted spaces	A, B, C, D, F, G, H, J, K, L M, N, O, P, Q
Manufacturing	Plant automation, robotics, analytics, smart supply chain, QC, distribution, logistics	A, C, F, G, H, J, K, L, M, N, O, P, Q
Retail/enterprise	Smart store, branch-in-a-box, security, asset tracking, digital signage, analytics, thin clients	C, E, F, G, I, K, L, O
Service providers/FaaS	Smart networks, fog-as-a-service, media caching, microcells, resiliency, MEC	B, C, D, E, F, H, J, K, L, M, N, O, P, Q
Oil/Gas/mining	Exploration, rig-in-a-box, production monitoring, pipeline control, refinery control	A, B, C, D, E, F, G, H, I, J, K
Health care	Continuous patient monitoring, aging in place, cognitive assistance, exercise	B, C, E, F, G, H, I, L, N
Agriculture	Irrigation, crop monitoring, yield assessment, pest control, autonomous equipment	B, D, E, G, H, I, J, K, L, N, P
Government/military	Homeland Security, C4ISR, autonomous vehicles, electronic warfare, connected fighter	A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q
Residential/consumer	Home automation, residential networking, security, social media, haptics, AR, games	A, B, C, D, E, G, I, K, L, M, N, O, P, Q
Hospitality	Front desk, bell robots, entertainment, security, cruise ships, campgrounds, dormitories	B, C, E, F, G, I, K, L, O

Table 1. IoT vertical markets and fog use cases.

Application examples	Latency	Implementation
Big data file download, offline backup	100 s	Easy with cloud
YouTube, home automation, video surveillance	10 s	
Web search, sensor readings	1 s	Challenging with coud
Interactive web site, smart building, analytics	100 ms	
Virtual reality, smart transportation, games, finance	10 ms	Impossible with cloud, needs fog
Haptics, robotics, real-time manufacturing	1 ms	

Table 2. Application examples and allowable latency.

Architectural Imperatives for Fog

Many important IoT use cases in commercially important vertical markets have certain critical requirements that make them difficult or impossible to implement in exclusively cloud-based or intelligent thing-based architectures. A fog architecture that locates computation, networking, and storage at intermediate levels is needed. The architectural imperatives listed below include use cases and key requirements, and describe some fog architecture and implementation concepts.

Low Latency (A)

Minimizing latency in IoT networks is perhaps the most pressing requirement that fog techniques will satisfy. In the fog context, latency measures the absolute delay control information takes in a real-time system. This delay may be one way (e.g., when a cloud-based process is controlling an actuator or collecting sensor readings), but will more typically be round-trip. For example, a sensor may monitor a physical process and send its readings to a processor that runs control algorithms, which send their outputs back to an actuator to adjust the process parameters. If this latency exceeds a certain application-specific threshold, the process can go unstable, results arrive too late, and control is lost. If the control algorithms run on far-flung cloud servers, the round-trip network transport latency could exceed 100 ms, compounded by any queueing delays in the network or servers. Even highly optimized, geographically diverse gaming cloud server networks have difficulties guaranteeing application latency under 80 ms [10]. More generalized cloud applications, perhaps using cloud servers physically located on remote continents, can experience much higher latency, up to several hundred milliseconds, due to large packet flight and router queueing delays.

Many IoT use cases have critical latency requirements. Table 2 includes some example use cases, their typical latency targets, and if fog techniques are likely to be needed.

Once the latency requirements fall below a few tens of milliseconds, fog techniques become essential. By physically locating fog nodes close to the sensors and actuators with which they interact, the transmission component of latency can be greatly reduced. If the fog node is located within a 100 km radius of the things it serves, the round-trip time of flight in a fiber optical cable (assuming a velocity factor of 0.67c) or over a radio link (assuming reasonable delay for encoding and decoding the transmissions at both ends) is less than 1 ms.

Reduced Network Bandwidth (B)

Network bandwidth between things and the cloud is often a serious constraint in IoT networks. Sometimes data sets are so large that the transmission delay to move data to the cloud, even over fast access facilities, is unacceptable. Sometimes sensor data streams are too high in average bandwidth to be affordably carried on available data transmission facilities. And sometimes the data sources are so remote that no terrestrial network connection is available.

A concrete example: A single 5 megapixel IP surveillance camera requires a streaming bandwidth of 12–16 Mb/s (at 30 FPS) [11]. Continuously streaming this bandwidth from a camera at the edge of a network to the cloud will require the transportation of approximately 4.5 TB/mo of data traffic on the access network. At the US$10/GB incremental cost typical of consumer cellular data plans, this would incur a charge of US$45,000/mo. Satellite data plans currently cost roughly 10 times the cost of cellular data. Hence, backhaul of full UHD video streams is plainly cost prohibitive for all but the most critical applications. Fog nodes can perform local analytics computations to greatly reduce the size of the data that requires transport to the cloud and can implement local storage.

Enhanced Security and Privacy (C)

IoT networks often carry private information and control potentially dangerous physical systems. If these networks are compromised due to data security breaches, severe consequences to society could result.

IoT networks pose unique security and privacy concerns due to their ability to control actuators. In many previous IoT systems, networks carried sensor readings and IT data between servers and clients. Data breaches and hacking episodes were costly, but physical harm as a result was rare, because these systems could not directly and immediately impact the physical world. Now, IoT systems are fully connected to the public Internet and cloud, and their actuators directly control multi-megawatt systems like locomotives, potentially dangerous systems like refineries or medical implants, and privacy-critical systems like surveillance drones. If the security of these networks is compromised, there is a real danger that people will die.

The locality of fog nodes can reduce the attack surfaces and distances over which data must flow. Since fog nodes often have larger physical size, power envelope, and cost than distributed IoT things, they can have stronger crypto processing than many intelligent things could support internally. Fog nodes can be mechanically more resistant to damage, unauthorized tampering, or outright theft than highly constrained IoT devices, making them more trustworthy.

Fog nodes are often the first set of processors data encounters in IoT networks that have the resources to implement a full hardware root of trust. This root of trust can be extended to all the processes and applications running on it, and

thence to the cloud. Without a hardware root of trust, various attack scenarios can compromise the software infrastructures of IoT networks, allowing hackers to gain a foothold. The requirements of life safety-critical systems will mandate the sorts of security capabilities available on fog.

Geographic Locality of Control (D)

Often, in IoT networks, information is most useful near its point of creation or use, and of limited use at longer distances. For various political, regulatory, and policy reasons, it is sometimes required to maintain control of information so that it does not cross some physical or logical boundary (e.g., staying within a country, corporate campus, military base, or private network).

IoT networks should have the ability to control the flow of information based on physical or logical boundaries, and limit the flow based on rules and policies. If a network of local fog nodes implements all the computation and storage capabilities of a cloud-based service, there is little reason to send the data beyond its boundaries.

Also, the dispersed nature of fog resources incentivizes fog nodes to work together. Fog devices collaborate with each other, and with nearby things and the cloud, depending at least in part on their geographic location.

Data Rich Mobility (E)

Many IoT things are mobile. The data and network resources that support them can be architected in certain ways to greatly improve their performance and efficiency.

Consider a connected city bus, with many sensors and actuators and cellular data connectivity. Unfortunately, due to dead spots, network overloads, interference, and so on, the connection between the bus and the internet may occasionally be unavailable. During these times, it would be helpful if local fog computing resources were present on the bus to continue to operate the applications. In essence, the mobile fog node riding on the bus performs much of the computation, networking and storage the bus authority's applications require, and if network access is temporarily down, it can fill in for the cloud-based components of the services until it is restored.

Reliability and Robustness (F)

Some IoT networks perform functions that must continue to function (at least at a minimal level) in the presence of many types of failure.

One example is the E911 service used to report fires, medical emergencies, and police assistance requests. This is considered a "lifeline" service, and therefore is expected to achieve very high availability — approaching .99999 uptime. In a highly evolved IoT world, the mechanisms for communicating with emergency authorities will go well beyond landlines and smartphones, including sensors and actuators blanketing smart cities.

Availability requirements are not necessarily limited to life-critical applications. Some business-critical applications may also use fog techniques to improve their availability.

Robustness is a related property. Should networks experience a failure (or a cluster of failures, perhaps following some sort of disaster), the applications running on those networks can adapt to use whatever resources are still functioning.

Fog techniques can improve the reliability and robustness of IoT networks by pushing some of the decision making from the cloud/Internet to more local resources. The hierarchical nature of fog permits many different fault tolerance and redundancy scenarios. If a fog node experiences a failure, nearby fog nodes on the same layer or on adjacent layers could step in to carry the load.

Supporting Advanced Analytics and Automation (G)

The huge volume of data flowing through IoT networks will necessitate the inclusion of advanced analytics algorithms and automated decision making systems. These algorithms may span multiple levels of the fog hierarchy, with the data bandwidth-intensive and low-level portions being executed low in the fog, and the higher-level heuristic algorithm components executing higher in the hierarchy. Geo-distributed analytics of this sort have been shown to offer several advantages [12].

An illustrative example of mapping analytics to the fog is multi-camera video surveillance. Several cameras photograph a scene from different angles, and the analytics algorithms detect movement, objects, people, and other properties of interest in the video streams. All this raw video could be transported to cloud servers for analysis, but this has network bandwidth efficiency, privacy, and performance concerns.

Low-level fog nodes close to the cameras can receive their video streams and perform first stage analysis, such as contrast enhancement and motion detection, passing their results to intermediate fog layers for more detailed analysis like pattern matching and object recognition, and ultimately sending their results to the cloud.

Hierarchical Organization (H)

Fog networks will usually be deployed in a hierarchy of levels, from the bottom of the cloud to just above the things/endpoints. This hierarchical organization, shown in Fig. 1, allows the processing, networking, and storage carried out at each level to match the topology and distributed workload properties of the applications running on the fog network.

Consider a fully connected, fully fog-enabled smart city. There may be widely distributed local fog nodes, perhaps deployed in street corner cabinets arranged on a grid spaced every few hundred meters. They connect to local sensors, run local WiFi hotspots, process surveillance cameras, and run smart highway, street lighting, utility monitoring, and hosts of other municipal services. A large city may have thousands — one plan for Barcelona has approximately 3300 local fog nodes [13].

Next up the hierarchy would be neighborhood fog nodes, each supporting a few dozen to perhaps a few hundred local fog nodes. Above these would be regional fog nodes managing city-wide coordination.

Energy Efficiency (I)

A global network of 50 billion IoT sensors and actuators is projected by 2020 [14]. As it is built out, the energy consumption of the global IoT will become a serious concern. Also, many things,

IoT networks should have the ability to control the flow of information based on physical or logical boundaries, and limit the flow based on rules and policies. If a network of local fog nodes implements all the computation and storage capabilities of a cloud-based service, there is little reason to send the data beyond its boundaries.

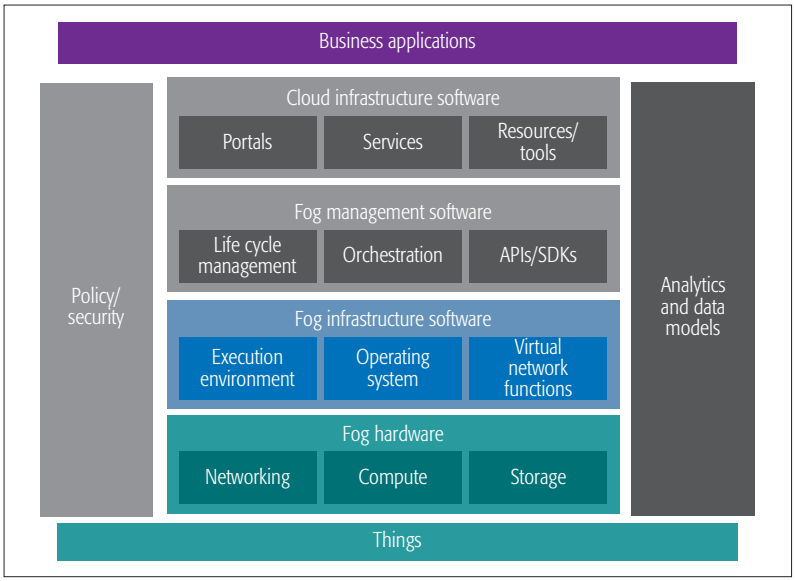


Figure 2. Fog software architectrue.

including sensors, smartphones, and so on, will have individual energy constraints imposed by their size, weight, and internal battery capacity. Fog techniques can assist with these constraints.

One example use case with significant energy constraints is smart agriculture. A farm may have hundreds of sensors distributed throughout its fields measuring soil moisture, growing conditions, and crop health, and watching for signs of pests. These sensors are often battery powered and seriously energy constrained. They periodically wake up, take some readings, send the raw data to the fog using a low-power radio link, and go back to low-power sleep mode. Fog allows the sensor network to use extremely low-power techniques, and manages the energy-intensive computation and WAN functions on their behalf.

Fog nodes themselves must be energy-efficient. As they will typically be left in some state of power-on 24/7/365, they must minimize their internal power consumption. Their loads will change as their application mix changes, and at different times of the day. Energy-efficient techniques and low-power semiconductors will be valuable in fog deployments.

Environmental Constraints (J)

Many IoT things must survive in harsh and space constrained environments, where it is simply impossible to provide high-performance computing, networking, and storage due to the physical constraints of the electronics. Fog nodes can be located in more controlled conditions, and are easier to harden against harsh environments.

A use case example from military systems would be the connected warfighter. A soldier carries many sensors, user interfaces, and actuators, and these are subject to very harsh environmental conditions (including extreme temperature, humidity, contamination, and shock/vibration). For some applications, that warfighter may also require specialized capabilities like very fast CPU cores, graphics processing unit (GPU) arrays, special signal processors, or large storage arrays, and these may not survive the harsh battlefield environment. In these cases, the devices carried by the warfighter are environmentally hardened front-ends. They communicate with specialized, more sensitive capabilities that are implemented in a nearby fog node that may have a more hospitable environment, for example, on a mobile fog node on a Humvee.

Programmability at Multiple Levels (K)

IoT will be a largely software driven technology. It must be simple to program all levels of the fog hierarchy, by many different classes of stakeholders. The economic value of IoT networks will be largely driven by the application software and infrastructure that runs them. It is essential that this software be easy to create, modify, and maintain.

In the fog as a service (FaaS) use case, a fog service provider (e.g., a mobile phone company, municipality, or web-scale company) owns an array of fog nodes. Enabling fog-based services requires multiple elements of the software stack to be programmable at all levels.

Figure 2 illustrates a simplified software stack for fog networks, starting with the sensors, actuators, and other things. The lowest layer is the fog hardware, including networking, compute, and storage elements and their device drivers. Next is a layer of fog infrastructure software, including a versatile execution environment, one or more operating systems, and functions to optimize virtualization and the use of containers. Fog management software performs operational functions like life cycle management and orchestration. It also provides rich application programming interfaces (APIs) to permit the development of applications, well defined interfaces between the components. Software development kits (SDKs) are needed to permit programmers to start quickly and develop efficiently in the programming environment. Part of the software supporting the fog can also run on the cloud, providing portals, services, resources, and tools. Business/user applications run at the top of the stack. Also, note that the policy/security and analytics/data model blocks span the vertical hierarchy, providing their capabilities at all levels.

There may be many different constituencies of software developers simultaneously implementing software for a fog network. These programmers could be associated with fog node manufacturers, service providers, application domain experts, or end users. The fog software architecture must ensure effective programmability at all of these levels and by all of these groups. In the limit, this programmable nature of fog should help create an open applications marketplace where many different software options are available for many diverse IoT applications on fog.

Multi Tenancy (L)

Fog nodes are capable of virtualizing their functions. Multiple applications can run concurrently but independently on these virtualized resources. The owner of the physical fog node could be a "landlord," and multiple independent users of the virtualized infrastructure could be considered "tenants."

Smart cities are good examples of where multi-tenancy may come into play. If a municipality builds out a network of municipal fog nodes,

it may lease capacity on them to many different customers, internal and external.

Advantageously, a single correctly sized fog network can efficiently host all of these tenants, sharing resources appropriately, and ensure secure isolation of services and resources between them. Fairness can be enforced based on service level agreements and policies. If it were not for the multi-tenant municipal fog network, the city could end up with a dozen or more parallel, independent fog networks owned by many different enterprises, creating great inefficiencies, and blanketing the city's street corners with innumerable redundant fog node cabinets.

Virtualization, Orchestration, and Management (M)

Fog networks, like the cloud, are highly virtualized. Resources like CPU cycles, network bandwidth, and storage blocks are pooled, and virtualization software allocates the required amount to each application. Virtualized networks are much more efficient and responsive than networks where specific resources are dedicated to individual processes or users.

Orchestration is the process through which the fog systems determine how the virtualized resources will be allocated and interoperate. It is essential that orchestration is aware of the instantaneous state of the fog network, and react quickly to any changes in its configuration, load, or status.

Fog orchestration and virtualization must be optimized for the multi-tenant and FaaS models. Complete isolation must be maintained between tenants by the virtualization system to avoid cross-disclosure and privacy compromise of application-specific data. The orchestrator must accommodate quality of service and service level agreements to ensure all tenants receive the minimum levels of resources for which they pay. Ideally, the same virtualization and orchestration models that are in operation in the cloud will be seamlessly extended down the fog hierarchy.

Fog networks will be inherently complex. In order to maintain reasonable control over their installation and ongoing management, and software update, significant attention must be paid to their management infrastructure. Configuration and routine management must be highly automated. Many innovations are occurring in IoT provisioning, including systems like Cisco Jasper [15].

Scalability (N)

Fog networks will be called on to serve many different use cases, and grow with minimal disruption to have adequate capacity in step with growing application demands. Scalability can have many dimensions, including capacity, performance, reliability, and security. Many organizations who install fog networks will want to start modestly to avoid too much initial capital expense, and grow that same initial network seamlessly and without disruption in order to serve complex web-scale services with millions of users.

Fog networks should be architected with scalability in mind. Fog nodes should have modular hardware platforms, permitting the configuration of additional compute, networking, and storage modules as the load on specific nodes increases. Networks should also allow the simple installation of additional fog nodes, permitting the load that was previously on other nodes to be shared by the new one. Network links should support scalable physical layers.

Software is also scalable. Fog nodes can start small, with the basic fog platform software and just a few applications, and grown in stages through the addition of more software modules. Licensing models could also permit the incremental activation of fog node capacity through software as the network's demands grow.

Software is also scalable. Fog nodes can start small, with the basic Fog platform SW and just a few applications, and grown in stages through the addition of more SW modules. Licensing models could also permit the incremental activation of Fog node capacity through software as the network's demands grow.

Agility (O)

Widely different use cases will be applied to fog networks. They must be agile enough to adapt to serve them seamlessly. Time to service is going to be a key metric used to rate fog networks, and the fog platform should do everything it can to enable the quick creation and wide deployment of new services and applications.

As application mixes evolve over time, agile fog networks can adapt their resource allocation to keep pace. Time to service will be very rapid on advanced fog networks, going from conception through application creation to rollout on the fog hierarchy in hours or days. Many other fog capabilities support agility, including programmability, modularity, and scalability.

Modularity (P)

Fog nodes will be multi-function devices, and should be customizable to include the hardware and software modules necessary to efficiently perform the functions required. Hardware modules could include various choices of CPUs, processing accelerators, networking modules, and storage engines. Software modules could include choices of operating systems, plug-ins for security, network protocols, analytics algorithms, and layers of applications software modules.

As shown in Fig. 3, modular fog nodes will include a number of "slots" into which the specific complement of modules needed to implement a node's functions will be installed. The figure depicts the hardware of a moderately capable fog node, with a number of modular slots for CPUs, GPUs (or other acceleration hardware like field programmable gate arrays [FPGAs] or digital signal processors [DSPs]), I/O interfaces to IoT things and other fog nodes, and storage modules. The software analog to this is a modular software platform infrastructure that permits the installation of custom complements of software to exactly match the application needs of every fog node.

Openness (Q)

To be the most useful in the marketplace, fog networks need to be open. Customers will not accept being locked into proprietary, vendor-specific, closed architectures. The OpenFog Consortium is taking steps to ensure an open, interoperable fog ecosystem. [8] They have published a white paper [9] on the basic properties of OpenFog systems, and a full OpenFog Reference Architecture.

Openness can also encourage competition among suppliers. That will facilitate innovation, improving the efficiency, quality, and control the cost of fog networks. Openness also lowers the barriers to entry into the fog market. Small companies can easily learn about the open fog architec-

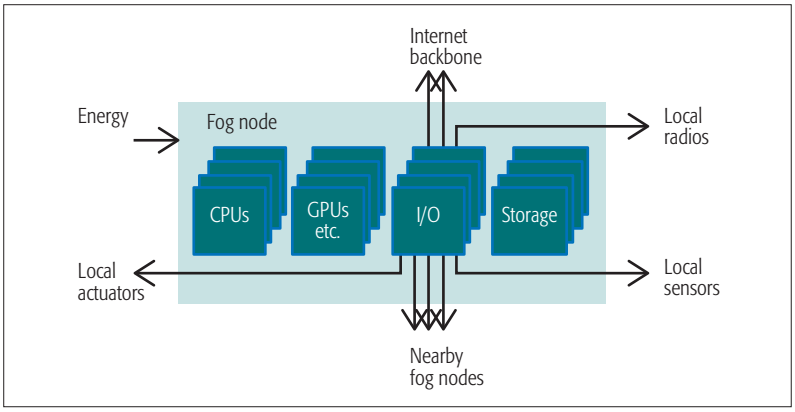


Figure 3. Modular architecture of a Fog node.

tures, add their specific value in the components of the open system they choose to produce, and quickly enter the marketplace for a reasonably small investment. Finally, openness can remove some of the intellectual property risks associated with new, fast growing technologies like fog. If the industry agrees to open standards, with a reasonable intellectual property sharing policy, the freedom to innovate should be enhanced.

Discussion

As we have seen, the architecture of fog networks is a rich canvas with many different attributes and sometimes competing requirements. The list of key architectural imperatives helps identify the use cases where fog will be particularly helpful, extract the key requirements from these use cases, and understand architectural techniques that can be applied to fog to help meet these requirements. Some of the architectural imperatives are interrelated (e.g., latency, network bandwidth, and geographic locality; or scalability and modularity).

Using the guidelines shown in this article, it should be possible to make more informed decisions in the architecture, partitioning, design, and deployment of fog computing in IoT networks. Although certain complexities are introduced by the fog model (compared to a pure cloud network), the advantages of fog are clear for many applications, and fog's support of automation should reduce the impact of this complexity. Many trade-offs exist, and knowing the requirements implied by these imperatives should help us develop highly effective fog nodes, and deploy them in essential roles in IoT networks.

References

[1] M. Satyanarayanan *et al.*, "The Case for VM-Based Cloudlets in Mobile Computing," *Pervasive Computing*, Oct.–Dec. 2009, pp. 14–23.
[2] E. Cuervo *et al.*, "MAUI: Making Smartphones Last Longer with Code Offload," *Proc. 8th Int'l. Conf. Mobile Systems Applications Services*, 2010, pp. 49–62.
[3] F. Bonomi *et al.*, "Fog Computing and Its Role in the Internet of Things," *MCC '12 Proc. 1st Ed. MCC Wksp. Mobile Cloud Computing*, pp. 13–16.
[4] M. Patel *et al.*, "Mobile Edge Computing — Introductory Whitepaper," issue 1, ETSI, Sept. 2014.
[5] Industrial Internet Consortium, "Industrial Internet Reference Architecture" v. 1.7, June 2015.
[6] http://opencord.org/, accessed 5 May 2017.
[7] http://openedgecomputing.org/, accessed 5 May 2017.
[8] http://www.openfogconsortium.org, accessed 5 May 2017.
[9] OpenFog Consortium, "OpenFog Architecture Overview," white paper, Feb. 2016, http://www.openfogconsortium.org/white-paper-reference-architecture/, accessed 5 May 2017.
[10] S. Choy *et al.*, "The Brewing Storm in Cloud Gaming: A Measurement Study on Cloud to End-User Latency,", *Proc. 2012 11th Annual Wksp. NetGames;* http://www.cctvcameraworld.com/ip-cameras-frame-rate-bandwidth/Network and Systems Support for Games (NetGames).
[11] http://www.cctvcameraworld.com/ip-cameras-frame-rate-bandwidth/; accessed 5 May 2017.
[12] Q. Pu *et al.*, "Low Latency Geo-Distributed Data Analytics," *Proc. 2015 ACM Conf. Special Interest Group on Data Commun.*, SIGCOMM '15 pp. 421–34.
[13] M. Yannuzzi *et al.*, "A New Era for Cities with Fog Computing," *IEEE Internet Computing*, vol. 21, Mar.–Apr. 2017, pp. 54–67, doi:10.1109/MIC.2017.25.
[14] D. Evans, "The Internet of Things — How the Next Evolution of the Internet Is Changing Everything," Cisco, Apr. 2011; http://www.cisco.com/c/dam/enus/about/ac79/docs/innov/IoTIBSG0411FINAL.pdf, accessed 5 May 2017.
[15] http://www.jasper.com/, accessed 5 May 2017.

Biography

Charles C. Byers (chbyers@cisco.com) is a principal engineer with Cisco's Corporate Strategic Innovation Group. He works on the architecture and implementation of fog computing platforms, media processing systems, and IoT, and is Technology Chair of the OpenFog Consortium. Before joining Cisco, he was a Bell Labs Fellow at Alcatel-Lucent. He received a B.S. in electrical and computer engineering and an M.S. in electrical engineering from the University of Wisconsin, Madison. He holds 62 U.S. patents.

IoT Stream Processing and Analytics in the Fog

Shusen Yang

ABSTRACT

The emerging fog paradigm has been attracting increasing interest from both academia and industry, due to the low-latency, resilient, and cost-effective services it can provide. Many fog applications, such as video mining and event monitoring, rely on data stream processing and analytics, which are very popular in the cloud, but have not been comprehensively investigated in the context of fog architecture. In this article, we present the general models and architecture of fog data streaming, by analyzing the common properties of several typical applications. We also analyze the design space of fog streaming with the consideration of four essential dimensions (system, data, human, and optimization), where both new design challenges and the issues that arise from leveraging existing techniques are investigated, such as cloud stream processing, computer networks, and mobile computing.

INTRODUCTION

The increasingly ubiquitous and powerful smart devices such as sensors and smartphones have been promoting the fast development of data streaming applications, such as augmented reality, interactive gaming, and event monitoring. The massive data streams produced by these applications have made the Internet of Things (IoT) a major source of big data. Currently, most mobile and IoT applications adopt the server-client architecture with frond-end smart devices and the back-end cloud. However, the long-distance interactive communications between billions of end devices and the cloud at the network center result in two major issues.

Latency: The end-to-end delay may not meet the requirement of many data streaming applications. For instance, the augmented reality applications typically require a response time of around 10 ms, which is hard to be achieved by using the Could solution with typical end-to-end latency of hundreds of milliseconds.

Capacity: The big data streams may not be affordable by today's network infrastructure. For example, the massive video streams produced by increasingly deployed cameras put great pressure on today's high-end metropolitan area networks (MANs) with a typical bandwidth of only 100 Gb/s [1].

The emerging fog architecture [2] paves the way for an ultimate solution that addresses the two issues above, by offloading the back-end computing tasks from the cloud to fog servers (i.e., physical or virtual edge servers such as Cisco IOx — https://developer.cisco.com/site/iox/ and the cloudlet — https://en.wikipedia.org/wiki/Cloudlet) at the network edge. Due to its shorter distance to the end devices and users, the fog paradigm has great potential to not only reduce the backbone Internet traffic, but also provide services with lower latency and better resilience than the traditional cloud paradigm, and therefore is receiving increasing interest from both academia and industry (e.g., the OpenFog Consortium — https://www.openfogconsortium.org).

This article presents a systemic study of data stream processing and analytics in the context of fog architecture. Based on the discussions of several typical applications, we present the functional architecture and general models for fog streaming systems, including the life cycle of data streams, work flow of stream processing tasks, and application-specific processing operations. A holistic analysis on the design space of fog streaming is also presented, with consideration of key technical issues in four essential dimensions: system, data, human, and optimization.

FOG STREAMING APPLICATIONS

This section presents an overview of four typical fog streaming applications, shown in Fig. 1, in order to demonstrate their typical features, and to clearly illustrate the conceptual fog architecture in the contexts of different real examples.

IOT STREAM QUERY AND ANALYTICS

The fast development of IoT promotes a large class of applications for high-level query and analytics over massive sensor data streams. A typical example of such applications using fog architecture is Gigasight [1], shown in Fig. 1a, an Internet-scale repository system of crowdsoured video streams generated by various cameras that aims to avoid massive video stream transmissions over the backbone Internet. Here, video processing tasks such as categorization and segmentation are carried out at a virtual machine (VM)-based cloudlet over all video streams within the associated MAN, and only the video metadata is transmitted to the cloud for the Internet-wide SQL search on catalog.

Besides Gigasight, which explicitly exploits the Internet edge, the existing database systems developed for wireless sensor networks (WSNs)

The author presents the general models and architecture of fog data streaming, by analyzing the common properties of several typical applications. He also analyzes the design space of fog streaming with the consideration of four essential dimensions (system, data, human, and optimization).

Shusen Yang is with the National Engineering Laboratory for Big Data Analytics Technology, Xi'an Jiaotong University.

Digital Object Identifier:
10.1109/MCOM.2017.1600840

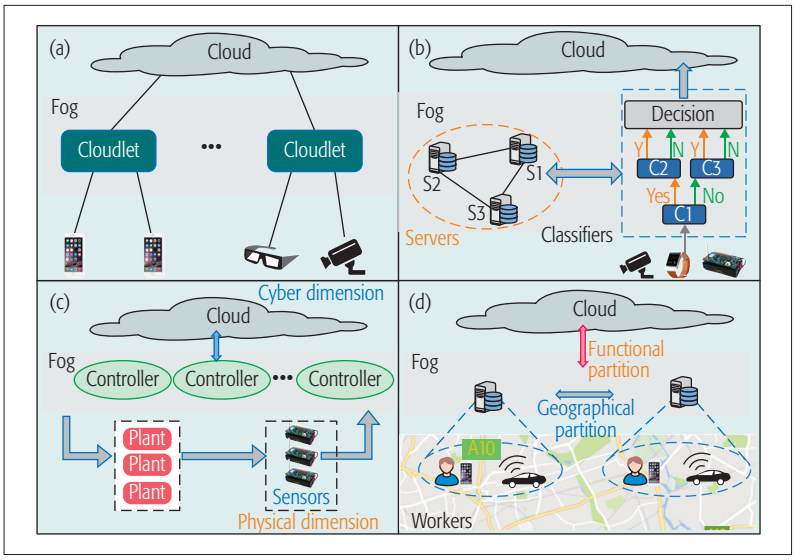


Figure 1. Examples of typical fog data streaming applications: a) IoT stream query and analytics; b) real-time event monitoring; c) networked control systems for industrial automation; d) real-time mobile crowdsensing.

[3], such as TinyDB (http://telegraph.cs.berkeley.edu/tinydb/overview.html), implicity adopt the fog architecture, because both the low-power sensors and resource-rich gateways (at the network edge) jointly manage and process sensor data streams. These WSN databases mainly focus on the energy minimization of low-power sensors, and can only provide basic support of sensor data management and SQL-like stream queries. In addition, there are several databases such as MongoDB (https://www.mongodb.com/) for high-performance and NoSQL IoT streaming applications, which can be implemented on both the cloud servers at the Internet center and the fog servers at the Internet edge.

Real-Time Event Monitoring

Event detection applications such as vandalism and accident detection are based on real-time mining of IoT data streams, which are spatially and temporally correlated in nature. Figure 1b illustrates an event detection system using fog architecture [4]. In this system, the high-level event detection job is divided into different low-level classification tasks (i.e., classifiers) according to the specific application logic and data stream features. The work flow of the event detection job is modeled as a reversed binary tree topology with the root as the data stream source (i.e., sensors), each leaf as a detection result and corresponding actions, and all other vertices as classifiers. These classifiers are allocated to the different fog servers in a distributed way, by considering the available computing resources of these servers such as CPU, memory, storage, and network bandwidth.

Networked Control Systems for Industrial Automation

As a typical cyber-physical system (CPS), the networked control system (NCS) [5] greatly promotes many critical industrial automation applications. As shown in Fig. 1c, the NCS control loop includes controllers, sensors, and control plants (actuators and physical processes), which produce real-time information streams, including continuous sensor data flows and control signals, over a communication network. Adopting the fog architecture to process such information streams can provide the following.

High-Quality Communications: To ensure the desired control performance such as system stability, NCS applications typically require very high-quality communications for the control feedback loop, such as 10 ms delay, 5 Mb/s data rate, and 10^{-8} bit error rate. To satisfy such stringent requirements, local fog networks should be adopted to minimize distance between all control components, while the cloud can provide Internet-scale remote administration services, shown in Fig. 1c.

Rich Computing Resources: Many advanced NCS applications require computation-intensive control algorithms for solving high-order differential equations, learning system dynamics, and addressing the disturbance and faults caused by communication uncertainty. Fog servers can provide rich computing resources for these complex control tasks, which cannot be supported by the embedded controllers hosted in the resource-limited end devices.

Real-Time Mobile Crowdsensing

Mobile crowdsensing (MCS) is becoming a vital sensing paradigm for urban IoTs, which collects spatio-temporal sensing contents from enormous participating mobile devices on a city-wide scale (https://en.wikipedia.org/wiki/Mobile_Crowdsensing).

Many MCS applications require real-time data collection and processing, such as traffic monitoring and collaborative people searching. In the context of MCS with "human-in-the-loop," the concept of stream processing indicates:

- Processing of sensor data flows such as query and mining, similar to systems with pure machines
- Processing of human-related information streams, such as streams related to incentivization, worker selection, and quality control.

In general, the processing of data streams requires lower latency and higher bandwidth than that of human-related information streams, such as paying participating workers. As shown in Fig. 1d, the hierarchial fog architecture can provide MCS applications with both *geographical partitioning* of mobile participants and *functional partitioning* of different stream processing tasks, resulting in much better performance than current cloud-based MCS in terms of scalability, interactive responsive, and bandwidth savings.

Models and Architecture

This section presents the general models and architecture to characterize the common features of typical fog streaming systems and applications, including the four examples discussed above.

Life Cycle of Fog Data Streams

As shown in Fig. 2, the typical life cycle of the fog data stream can be divided into the following four stages.

Create: Fog data streams are mostly created by end devices, including smartphones, sensors, vehicles, microphones, video cameras, wearable

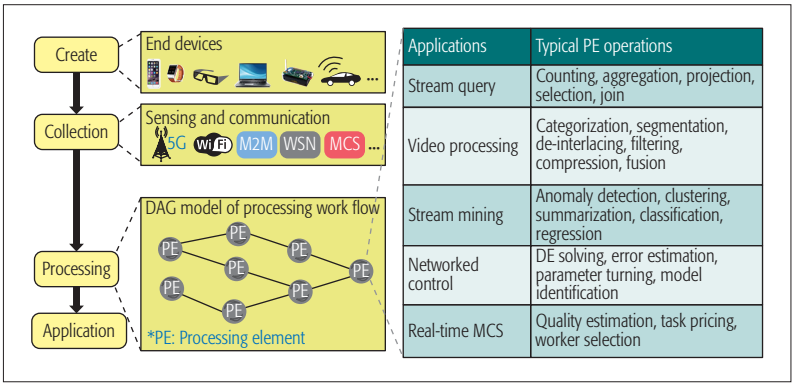
devices, control plants, and so on. It can be seen that the fog data sources are a subset of cloud data sources, which also include Internet data produced by social media, logs, emails, financial transactions, databases, e-commerce, and web services.

Collection: At this stage, the created data streams are transmitted from end devices to fog servers. A large set of sensing and communication techniques can be utilized for data collection, including WiFi, fifth generation (5G) cellular networks, WSNs, MCS, and machine-to-machine (M2M) communications. Besides the above IoT data collection methods, cloud data can also be collected using more "soft sensing" methods, such as a web crawler for obtaining web contents.

Processing: This stage carries out application-specific processing tasks based on the collected data streams at a single fog server, multiple individual fog servers, a small cluster of fog servers, or a combination of fog and cloud servers. Here, some processing tasks are specific for fog stream applications, such as the networked control and real-time MCS tasks shown in Fig. 2.

Application: The processing results are consumed by applications and may also be stored for offline batch processing.

It is worth noting that applications may also produce data streams (e.g., control signals in NCS), resulting in loops in the typical life cycle shown in Fig. 2.



Applications	Typical PE operations
Stream query	Counting, aggregation, projection, selection, join
Video processing	Categorization, segmentation, de-interlacing, filtering, compression, fusion
Stream mining	Anomaly detection, clustering, summarization, classification, regression
Networked control	DE solving, error estimation, parameter turning, model identification
Real-time MCS	Quality estimation, task pricing, worker selection

Figure 2. The typical life cycle, DAG model of stream processing work flow, and operations for fog stream processing tasks.

Work Flow and Operations of Fog Stream Processing

Generally, the high-level logic work flow of a stream processing job can be modeled as a directed acyclic graph (DAG), as shown in Fig. 2. Here, each vertex represents a processing element (PE) performing a variety of low-level computation tasks according to specific fog streaming applications summarized in Fig. 2, and an edge indicates a stream flowing downstream from the producing vertex to the consuming vertex. For instance, the aforementioned Gigasight application [1] adopts a multistage pipeline for its work flow of denaturing video streams, and the processing process of the event detection application [4] follows a binary tree-like topology. Both of them are specific forms of DAGs. Besides naturally describing the high-level abstractions of processing jobs, DAG models greatly facilitate parallel computations of PEs, which are adopted by many high-performance distributed stream processing engines. For example, Apache Storm (http://storm.apache.org/) uses a DAG topology consisting of "spouts" and "bolts," where spouts produce new streams, and bolts consume injected streams as input and produce streams as output.

Fog Data Streaming Architecture

By using the relatively sophisticated cloud streaming system as a reference, we propose a fog streaming architecture, shown in Fig. 3, which includes six functional layers.

Application Layer: This defines the objective and logic of fog streaming jobs.

Processing Layer: This carries out the application-specific processing jobs. Recently, a number of real-time stream processing engines have been developed [6], such as Apache Storm, Spark Streaming (http://spark.apache.org/streaming/), and Flink (https://flink.apache.org/). Although these stream processing engines were originally designed for the cloud and large-scale data centers, they also support the installation on a single or a small cluster of fog servers. Related technique issues are discussed in the next section.

Data Management Layer: This addresses data storage and organization, including file systems, databases, data caches, data warehouses, data lakes, and so on. There are many data management systems working together with stream processing engines in the cloud, such as the publish-subscribe messaging system Apache Kafka (http://kafka.apache.org/) and the NoSQL database Apache Cassandra (http://cassandra.apache.org/). Similar to stream processing engines, these data management systems can be applied in fog servers. In addition, data management schemes for local networks such as data-centric caching [7] and WSN databases [3] can also be exploited for fog data management.

Resource Management Layer: This mainly focuses on the utilization and scheduling of the virtualized system resources, including network and disk I/O bandwidths, CPUs, GPUs, memory, storage, and also energy (e.g., for battery-powered and energy-harvesting devices [8]).

Virtualization Layer: This addresses the configuration and virtualization of the system hardware resources. Virtualization techniques such as Openstack (https://www.openstack.org/), software-defined networking (SDN — https://en.wikipedia.org/wiki/Software-defined_networking), and network functions virtualization (NFV — https://en.wikipedia.org/wiki/Network_function_virtualization) supports both cloud and fog architectures [2]. For instance, both SDN and NFV are considered as the key techniques to facilitate the management of future 5G networks and the next-generation Internet. Also, a set of cloudlet-specific application programming interfaces (APIs) are provided in the extension of Openstack. Besides cloud-like service paradigms such as Infrastructure as a Service (IaaS), fog virtualization can also provide APIs for sensing, caching, mobility, and control services.

Physical Network Layer: As shown in Fig. 3, the fog system has a much more heterogeneous and dynamic physical network infrastructure than data center networks for the cloud, although both of them have similar hierarchal network architectures.

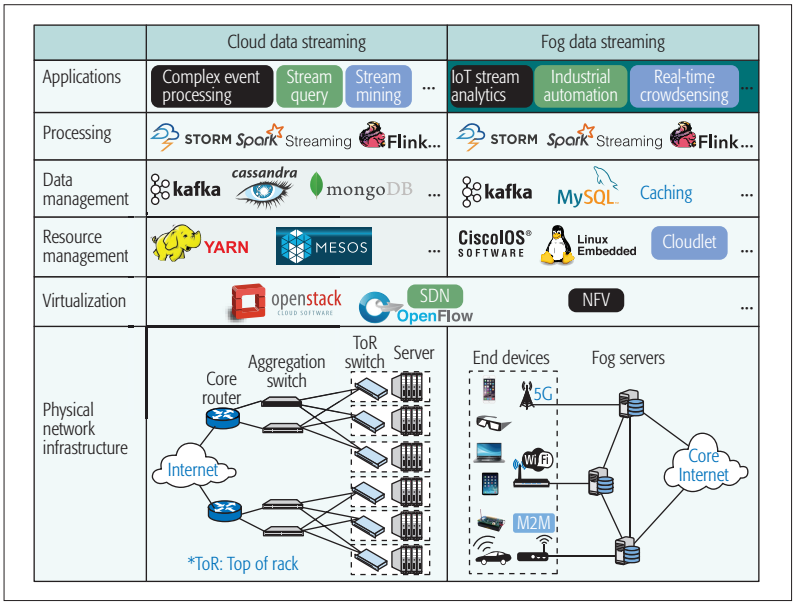


Figure 3. Functional architectures of cloud and fog data streaming systems.

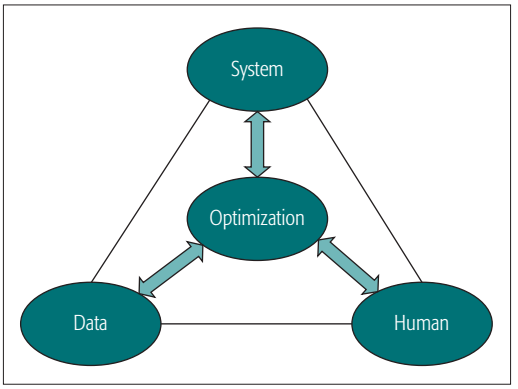


Figure 4. The four dimension in the design space of fog data streaming.

It can be seen that many existing cloud streaming techniques can be leveraged for the fog. However, fog streaming systems have many features that are significantly different from cloud data streaming systems, including highly delay-sensitive applications, dynamic physical network infrastructures (majorly caused by user mobility), more types of resources (e.g., sensors, actuators, and wireless connectivity), and potentially unreliable services provided by self-interested users. Therefore, cloud-based approaches may not be able to be directly applied in fog streaming systems, and new fog-specific designs considering the above features are highly desired.

The Design Space of Fog Data Streaming

This section discusses the design space of fog data streaming from the viewpoints of four essential dimensions: system, data, optimization, and human, where both new design challenges and the issues that arise from applying existing techniques in fog streaming are considered. As shown in Fig. 4, these four dimensions are not orthogonal, meaning that a technical issue in one (the most relevant) dimension is normally also related to the other dimensions.

System

The system dimension refers to the functional components (including algorithms, protocols, and software) related to the fog streaming architecture illustrated in Fig. 3. Specifically, the following three issues are most critical for establishing the fog-specific data streaming system.

Stream Processing Engine: Since there are several well developed open source stream processing engines such as Apache Storm and Spark Streaming that can run on fog servers, there is no need to develop a complete new tool for the fog. However, the following two issues need to be addressed.

Latency-Oriented Processing: A key objective of existing stream processing engines is to achieve both high throughput and low latency (typically around 100 ms), while fog servers typically require much less processing capacity (due to the geographic partitioning of data stream sources), but probably more stringent end-to-end delay (less than 10 ms) such as industrial control applications. Therefore, we need to study how to optimize the models and configurations of existing stream processing tools (e.g., the number of bolts in the Storm DAG topology and the micro-batch size of Spark streaming) to support ultra low-latency fog streaming applications. Bandwidth-hungry fog streams without such stringent delay requirements (e.g., video streams in Gigasight) can be processed in the same way as normal big data streaming applications or even using offline batch processing tools, but at the fog servers rather than the cloud.

APIs Specific to Fog Streaming: There are many libraries that provide rich APIs for advanced data processing, such as Apache Mahout (http://mahout.apache.org/) for machine learning and Spark GraphX (http://spark.apache.org/graphx/) for graph processing, which can also be used for related fog streaming applications. However, APIs for some important fog streaming applications are missing, such as differential equation (DE) solvers and control error estimators for fog-based real-time networked control applications.

Streaming Task Partitioning: Due to the three-tier hierarchy of fog architectures and the geographically distributed end devices and users, the following two types of partitioning of fog streaming tasks should be considered in the system deign.

Application Partitioning: This allocates different streaming tasks to end devices, fog servers, and cloud servers, according to available resources, privacy concerns, latency requirement, fault tolerance, and so on. Different granularity levels of partitioning can be adopted such as partitioning of multiple applications, multiple data streams, and functional components in a single application. Existing work [9] for the mobile cloud computing (MCC) paradigm (typically two-tiered architecture with end devices and cloud servers) can also be extended for the three-tiered fog.

Geographic Partitioning: This allocates streaming tasks among different fog servers. Here, load balancing among fog servers is particularly important for fog systems with heterogeneous server capacities and end device density.

Streaming Service Migration: When a user moves away from the fog server that he or she

is currently using, the corresponding streaming service should be migrated to a new server seamlessly, with minimal degradation of end-to-end streaming quality. However, existing approaches for cloud computing (e.g., live migration — https://en.wikipedia.org/wiki/Live_migration) would perform poorly in the fog environment due to the high uncertainty and dynamics caused by user mobility, while current fog service migration schemes such as [10] are limited to unrealistic mobility patterns. Therefore, the design of new streaming-specific service migration algorithms with real-time and fault tolerance support are highly desired.

Data

Existing data streaming algorithms (including data stream acquisition and mining) assume that their underlying computing infrastructure is a single server, a local distributed network (e.g., a WSN), or the cloud. The fog paradigm creates several new design opportunities for these algorithms.

Data Stream Acquisition: Data stream acquisition refers to the processes of sensing and data collection from local networks to the fog servers.

Sensing: The spatio-temporal correlation of IoT data streams enables advanced sensing techniques such as compressive sensing to minimize the sampling rate and therefore the network traffic loads. However, for city-wide (or real-time multimedia streaming) applications [11], current compressive sensing algorithms would suffer from heavy computation for the sensing matrix reconstruction, and intensive communications between end devices and the cloud server. It is promising to address these issues by exploiting the three-tiered fog architecture. For instance, each fog server communicates with its associated end devices and reconstructs a local sensing sub-matrix, based on which the cloud server can further recover the global one. To achieve this, new compressive sensing algorithms utilizing the hierarchical fog architecture should be designed.

Data Stream Cleansing: To improve data acquisition quality, raw data streams should be processed by removing abnormal (faulty, incorrect, or false) data records. Many real-time anomaly detection algorithms such as [12] are based on exploiting spatio-temporal correlations of the raw data time series. Since data sources in geographical proximity are more likely to be correlated, each fog server can perform as the local processing center to detect anomalies of the highly correlated data streams collected from its associated local network. This results in much higher fault tolerance than using end devices to perform the detection tasks [12].

Stream Mining and Analyltics: Existing research on real-time data mining such as [4] provide the theoretical foundation of distributed stream mining (e.g., feature abstraction and classification) in networked systems, such as fog systems. In addition, recently released open source software (e.g., TensorFlow — https://www.tensorflow.org/) significantly facilitates the implementation of advanced machine learning and data mining algorithms (e.g., deep neural networks) in the fog servers and even end devices (e.g., Mobile TensorFlow). Although these theoretical results and engineering supports open a new door for fog streaming mining and analytics, a new set of challenges arise, especially how to balance the computation loads among fog servers and end devices in real time, while ensuring the mining performance.

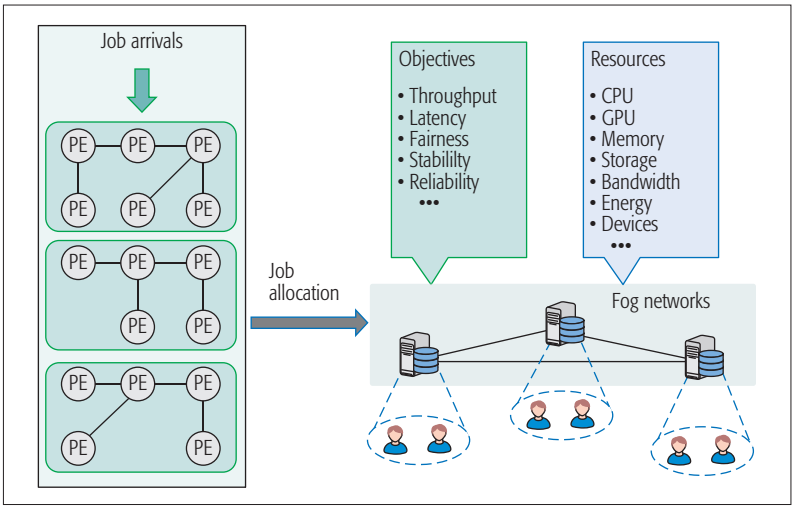


Figure 5. Dynamic resource allocation for DAG-like fog streaming jobs.

Human

Compared to the cloud, fog systems are closer to users and end devices (and thus their owners). Therefore, humans play a more important role, and their behaviors must be considered in the holistic fog streaming design.

Pricing and Incentivization: From the economics viewpoint, people in a fog streaming system can be classified into two types:

- *Service providers*, including private owners of end devices and fog servers, who have data and resources, and can provide various streaming services
- *Service consumers*, who discover, subscribe to, and consume the streaming services

Due to the inherent self-interest and strategic behaviors of both service providers and consumers, proper incentivization and pricing mechanisms are essential to ensure the efficiency and trustworthiness of economic activities between service providers and consumers. There is a large body of related research such as cloud data pricing, smart grid pricing, and crowdsensing auctions. These results can be leveraged for fog streaming applications, while specific attention should be paid to addressing the heterogeneity and dynamics of fog systems.

Privacy: An important issue in fog streaming is to balance the trade-off between the data value and the risk of privacy exposure. For instance, Gigasight [1] performs the denaturing process of video streams at the network edge cloudlet to abstract video features while preserving the privacy of video providers. Actually, the hierarchical fog architecture can be exploited to provide resilient privacy preservation at each of the three tiers, according to different application contexts.

Quality Control: Since crowdsoured workers are different in their problem solving abilities, quality control is essential for real-time MCS, a typical fog streaming application mentioned before.

For instance, in the real-time speech captioning application [13], audio streams with different speaking rates are allocated to crowdsourced

Due to the inherent self-interest and strategic behaviors of both service providers and consumers, proper incentivization and pricing mechanisms are essential to ensure the efficiency and trustworthiness of economic activities between service providers and consumers.

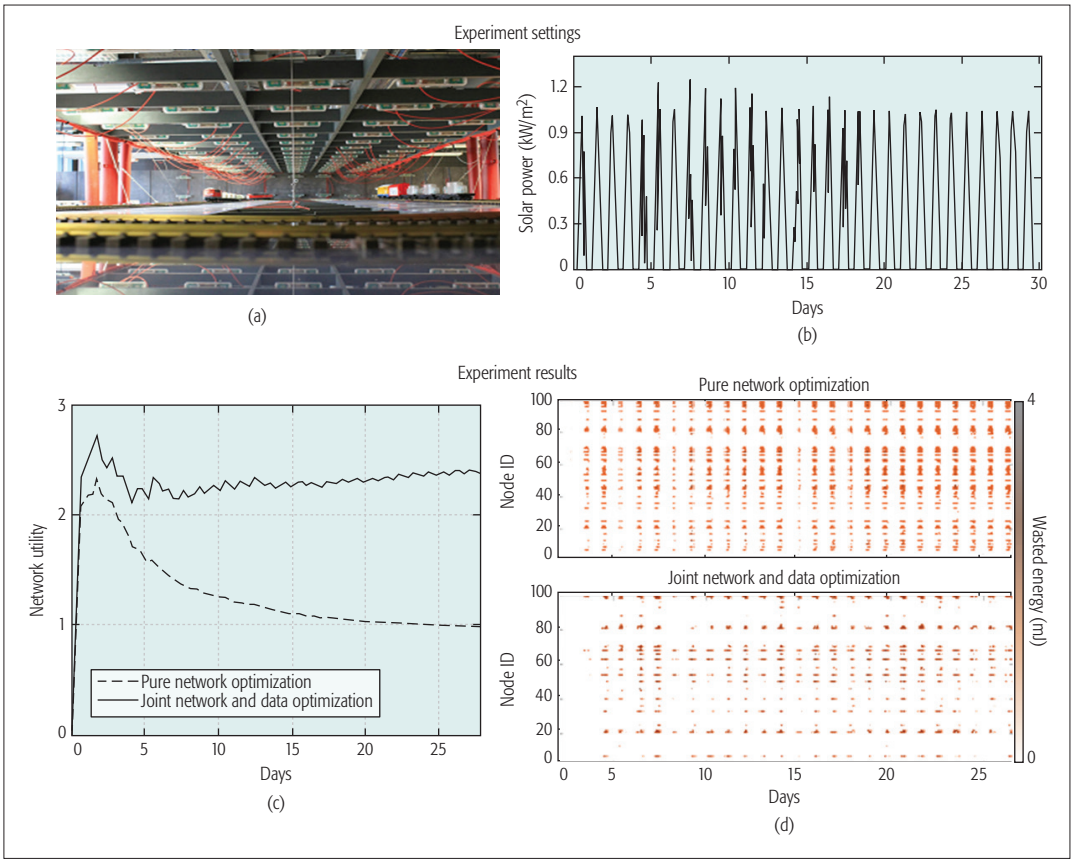


Figure 6. In-network data processing [8] as an example to demonstrate the performance gain of joint data and network optimization: a) network deployment in FIT IoT-Lab; b) dynamic solar power over a month; c) time-average network utility; d) wasted energy over time.

workers according to their abilities to ensure their online task completion qualities.

With the fog architecture, both the functional partitioning of task allocations and the geographic partitioning of crowdsourced workers can be exploited to optimize the real-time quality control process.

Optimization

To better understand and solve the issues in the system, data, and human dimensions, new theoretical models and methods are required, which are referred to as the optimization dimension.

Dynamic Optimization: Fog streaming systems are inherently dynamic and uncertain, due to various causes, including mobility, wireless communications, physical events, unreliable data providers, fault-prone sensors, server failures, and so on. Therefore, analytical models of fog streaming problems should pay specific attention to corresponding dynamics and uncertainties. For instance, the algorithm proposed in [10] uses a Markov decision process to address the edge-cloud service migration caused by mobility, and the algorithm proposed in [14] can support dynamic service configurations with arbitrary stochastic processes of service arrivals.

Complex Resource Allocation: All stream processing jobs consume resources. As shown in Fig. 5, due to the complex DAG structure of dynamically arriving streaming jobs and the heterogeneous types of resources in the networked fog system, resource allocation for fog data streaming are challenging optimization problems. Ghaderi *et al.* [15] propose an optimization approach for the resource allocation of DAG-like streaming jobs of Apache Storm for data center networks, which shares similar topology to fog network infrastructure shown in Fig. 3, and therefore is possible to extend to support fog stream processing.

Optimization over System, Data, and Human Dimensions: Due to the multidisciplinary nature of fog data streaming, joint optimization over the system, data, and human dimensions would outperform the optimization in each individual dimension. For instance, our in-network processing algorithm [8], which optimizes the data processing and network (system) operations jointly, manages to achieve better practical performance than pure network optimization in terms of energy resource utilization and network throughput, as shown in Fig. 6. To achieve cross-dimension optimization, new analytical models and methods should be developed by leveraging mathematical methods in each dimension, such as queuing theory for system, signal processing for data, and game theory for the human dimension.

Conclusion

This article presents a systemic investigation on data stream processing and analytics in the context of fog architecture. We study four typical fog streaming applications, including IoT stream analytics, event monitoring, networked control, and real-time mobile crowdsourcing, which demonstrate their common properties and the multi-disciplinary nature of fog streaming research. These

practical applications result in discussion of the general fog streaming models and architecture, as well as the opportunities and challenges in future design in terms of networked systems, data processing and management, human factors, and optimization methods. We expect that the increasingly important roles of both the network edge and stream processing will further promote their combination, and thus the development of fog data streaming in both academia and industry.

Acknowledgments

This work is sponsored by the China "1000 Young Talents Program" and the "Young Talent Support Plan" of Xi'an Jiaotong University.

References

[1] M. Satyanarayanan *et al.*, "Edge Analytics in the Internet of Things," *IEEE Pervasive Comput.*, vol. 14, no. 2, 2015, pp. 24–31.
[2] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet of Things J.*, vol. 3, no. 6, 2016, pp. 854–64.
[3] O. Diallo *et al.*, "Distributed Database Management Techniques for Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Sys.*, vol. 26, no. 2, 2015, pp. 604–20.
[4] L. Canzian and M. Van Der Schaar, "Real-Time Stream Mining: Online Knowledge Extraction Using Classifier Networks," *IEEE Network*, vol. 29, no. 5, 2015, pp. 10–16.
[5] R. A. Gupta and M.-Y. Chow, "Networked Control System: Overview and Research Trends," *IEEE Trans. Ind. Electron.*, vol. 57, no. 7, 2010, pp. 2527–35.
[6] H. Zhang *et al.*, "In-Memory Big Data Management and Processing: A Survey," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 7, 2015, pp. 1920–48.
[7] G. Zhang, Y. Li, and T. Lin, "Caching in Information Centric Networking: A Survey," *Computer Networks*, vol. 57, no. 16, 2013, pp. 3128–41.
[8] S. Yang *et al.*, "Distributed Optimization in Energy Harvesting Sensor Networks with Dynamic Innetwork Data Processing," *Proc. IEEE INFOCOM*, 2016, pp. 1–9.
[9] L. Yang *et al.*, "A Framework for Partitioning and Execution of Data Stream Applications in Mobile Cloud Computing," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 4, 2013, pp. 23–32.
[10] S. Wang *et al.*, "Dynamic Service Migration in Mobile Edge-Clouds," *Proc. IFIP Networking*, 2015, pp. 1–9.
[11] L. Wang *et al.*, "CCS-TA: Quality-Guaranteed Online Task Allocation in Compressive Crowdsensing," *Proc. ACM Ubicomp*, 2015, pp. 683–94.
[12] P. Chen, S. Yang, and J. A. McCann, "Distributed Real-Time Anomaly Detection in Networked Industrial Sensing Systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, 2015, pp. 3832–42.
[13] W. S. Lasecki, C. D. Miller, and J. P. Bigham, "Warping Time for More Effective Real-Time Crowdsourcing," *Proc. ACM SIGCHI*, 2013, pp. 2033–36.
[14] I.-H. Hou *et al.*, "Asymptotically Optimal Algorithm for Online Reconfiguration of Edge-Clouds," *Proc. ACM Mobihoc*, 2016, pp. 291–300.
[15] J. Ghaderi, S. Shakkottai, and R. Srikant, "Scheduling Storms and Streams in the Cloud," *ACM Trans. Modeling and Performance Evaluation of Computing Systems*, vol. 1, no. 4, 2016, pp. 1–28.

Biography

Shusen Yang [SM] received his Ph.D. in computing from Imperial College London in 2014. He is currently a professor at Xi'an Jiaotong University (XJTU). Before joining XJTU, he worked as a lecturer at the University of Liverpool from 2015 to 2016, and a research associate at Intel ICRI from 2013 to 2014. His research interests include networking, big data processing, and data-driven networked systems. He received the China "1000 Young Talents Program" award. Shusen is a member of ACM.

To achieve cross-dimension optimization, new analytical models and methods should be developed by leveraging mathematical methods in each dimension, such as queuing theory for system, signal processing for data, and game theory for the human dimension.

The Unavoidable Convergence of NFV, 5G, and Fog: A Model-Driven Approach to Bridge Cloud and Edge

Frank van Lingen, Marcelo Yannuzzi, Anuj Jain, Rik Irons-Mclean, Oriol Lluch, David Carrera, Juan Luis Pérez, Alberto Gutierrez, Diego Montero, Josep Martí, Ricard Masó, and Juan Pedro Rodríguez

The advances made in managing hyper-distributed infrastructures involving the cloud and the network edge are leading to the convergence of NFV and 5G, supported mainly by ETSI's MANO architecture. The authors propose that fog computing will become part of that convergence, and they introduce an open and converged architecture based on MANO that offers uniform management of IoT services spanning the continuum from the cloud to the edge.

Abstract

The interplay between cloud and fog computing is crucial for the evolution of IoT, but the reach and specification of such interplay is an open problem. Meanwhile, the advances made in managing hyper-distributed infrastructures involving the cloud and the network edge are leading to the convergence of NFV and 5G, supported mainly by ETSI's MANO architecture. This article argues that fog computing will become part of that convergence, and introduces an open and converged architecture based on MANO that offers uniform management of IoT services spanning the continuum from the cloud to the edge. More specifically, we created the first YANG models for fog nodes, for IoT services involving cloud, network, and/or fog, and expanded the concept of "orchestrated assurance" to provision carrier-grade service assurance in IoT. The article also discusses the application of our model in a flagship pilot in the city of Barcelona.

Introduction

Several technologies relevant to the expansion of the Internet of Things (IoT) have emerged, including network functions virtualization (NFV) [1], the fifth generation (5G) wireless systems [2], and fog computing [3, 4]. In particular, the European Telecommunications Standards Institute (ETSI) has standardized the reference architecture for NFV management and orchestration (MANO) [5], a cornerstone for building, deploying, and managing services in NFV environments. Advances in the 5G radio access network (RAN) and Multi-access Edge Computing (MEC) group at ETSI [6] are also key for the IoT evolution. MEC proposes a virtualized platform built on an NFV infrastructure, and is expected to leverage the NFV MANO architecture and application programming interfaces (APIs). The majority of service providers (SPs) will exploit NFV infrastructures not only for virtualized RANs and MEC, but also for other services, including enterprise, residential, and cloud offerings. Thus, the convergence of NFV and some of the key building blocks of future 5G architectures seems unquestionable (Fig. 1).

Fog computing addresses use cases with requirements far beyond cloud-only solution capabilities. For instance, a set of oil wells can produce petabytes of data daily, and all these data cannot be sent to the cloud due to limited or unreliable backhaul connectivity. Fog allows data to be filtered and analyzed locally, and actionable decisions to be made in real time (for safety reasons, preventive maintenance, etc.).

The complementarity between fog and cloud has traditionally been seen as a mandatory feature in any fog platform. In this article, we advocate for a different approach. Rather than specifying an architecture where fog and cloud are complementary by design, we focus on a service management architecture that literally fuses fog and cloud. We contend that the research community must start thinking about one computing fabric, managed as a single entity, in a service-centric way. With this approach, an infrastructure composed of fog nodes, network nodes, and cloud nodes is exposed to service administrators as a unified resource fabric. Administrators can then define where to instantiate resources according to the service requirements.

Compute nodes in the cloud or fog are treated architecturally the same, as the service management platform unifies the life cycle management of services that might require instances running in the fog, cloud, or a combination. Distinctive features of a fog, network, or cloud node will be captured by their corresponding YANG models [7]. A main advantage of this approach is that different IoT services can coexist and be managed in a uniform way.[1] Consider services where fog is not required (e.g., sensor communications supported through long-range radio, such as LoRA or NB-IoT [8]) vs. applications where fog is mandatory (e.g., industrial machines producing data filtered and analyzed by a fog node that is directly connected to the former through a wired interface [9]). System integrators and SPs can leverage our unified infrastructure and uniform service management to provide services to customers in both segments simultaneously.

The requirements to host and manage NFV, MEC, and fog computing services are undeniably

[1] IoT services are compositions of software services, hardware, and connected things like sensors to enable business outcomes.

Digital Object Identifier: 10.1109/MCOM.2017.1600907

Frank van Lingen, Marcelo Yannuzzi, Anuj Jain, Rik Irons-Mclean, and Oriol Lluch are with Cisco Systems; David Carrera, Juan Luis Pérez, and Alberto Gutierrez are with the Barcelona Supercomputing Center; Diego Montero is with the Technical University of Catalonia; Josep Martí, Ricard Masó, and Juan Pedro Rodríguez are with NearbySensor.

similar. SPs and enterprises embracing NFV will seek to maximize their investments, leveraging their NFV infrastructure and MANO systems to the largest extent possible. It is only a matter of time until fog computing becomes part of the convergence that we are already witnessing between NFV and 5G/MEC, driven by SPs and enterprise investments (Fig. 1).

This article describes an architectural approach that addresses some of the technical challenges behind the convergence shown in Fig. 1, with special focus on bridging the gap between cloud and fog. We introduce a model-driven and service-centric architecture that is, at the time of writing, perfectly aligned with the OpenFog Consortium (OFC) reference architecture [4].

A Model-Driven and Service-Centric Approach

Our model is based on a two-layer abstraction:

- The separation of the "service intention" (i.e., "what") from the "service instantiation" (i.e., "how")
- The decoupling of the "service instantiation" from the specifics of the devices where the instances will be ultimately deployed — independent of whether they will be instantiated in the cloud or network, or at the edge

The left side of Fig. 2 shows how this abstraction is achieved through utilization of a standardized data modeling language, YANG [7]. The right side shows a small YANG model snippet that is part of a sensor telemetry use case and multi-protocol data aggregation described later. The YANG model shows various parameters related to the tenant, the fog node, and analytics components.

YANG is used for service and device modeling. Models are machine-readable, and can be interpreted and processed by an orchestration system, which is one of the basic components of our NFV MANO implementation. A main role of the orchestration system is to translate the "what" to the "how," and enforce corresponding configurations on specific device models. The translation process is captured by mapping functions depicted on the left side of Fig. 2, which transform service definitions and input parameters to device configuration parameters. Configurations are enforced through NETCONF interfaces exposed by any device present in our infrastructure (cloud, network, or edge). NETCONF is a standard Internet Engineering Task Force (IETF) protocol used to install and update device configurations. The protocol was chosen because of its ubiquitous presence, as it has been largely adopted by SPs and enterprises as part of their service management operations.

The two-layer abstraction is not new. We believe, however, that this is a safe bet toward the convergence shown in Fig. 1, since this is precisely what many SPs and large enterprises are starting to use when adopting NFV. The novelties introduced in this article are:

- The extension of the model to cover fog and IoT. Although the utilization of NETCONF and YANG has traditionally focused on network configuration, these standards are sufficiently generic to be leveraged for any kind of device or service model. We have expanded the reach of NETCONF and YANG to fog nodes.
- The extension of orchestrated assurance to cover IoT services (i.e., service assurance is an intrinsic part of the IoT service definition in YANG).

In our model, everything is reduced to services. Infrastructure services (i.e., those dealing directly with physical resources) become an inte-

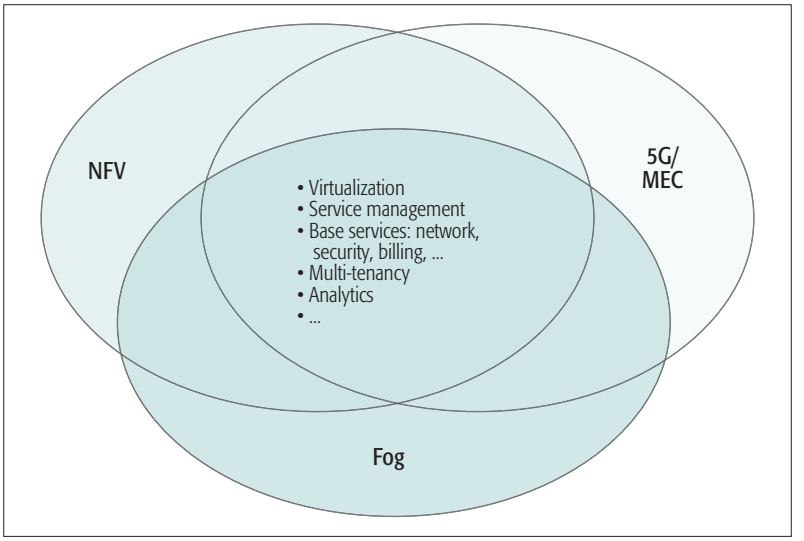


Figure 1. Different technologies with overlapping needs and challenges.

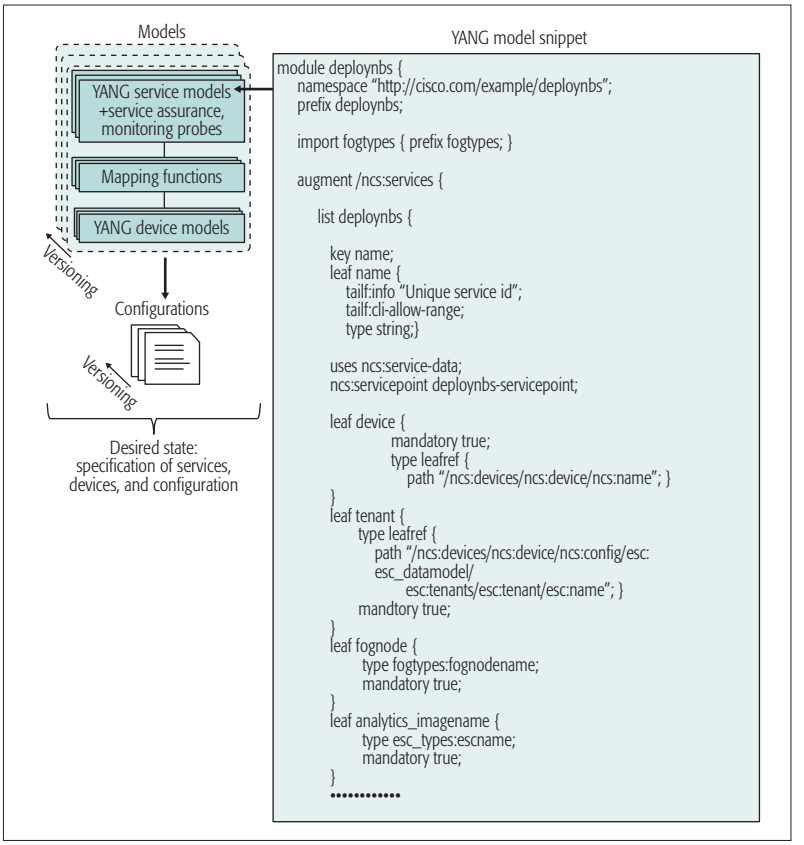


Figure 2. YANG is used for both service and device modeling, making devices transparent to service management. Service assurance is supported through distributed monitoring across the infrastructure and feeds a transactional orchestration system, which can deal with any discrepancy between the current state and the desired state of an IoT service.

This approach is proven to facilitate life cycle management of large collections of services in NFV environments, and is critical to reduce complexity when designing IoT services, with much more infrastructure heterogeneity beyond the datacenter.

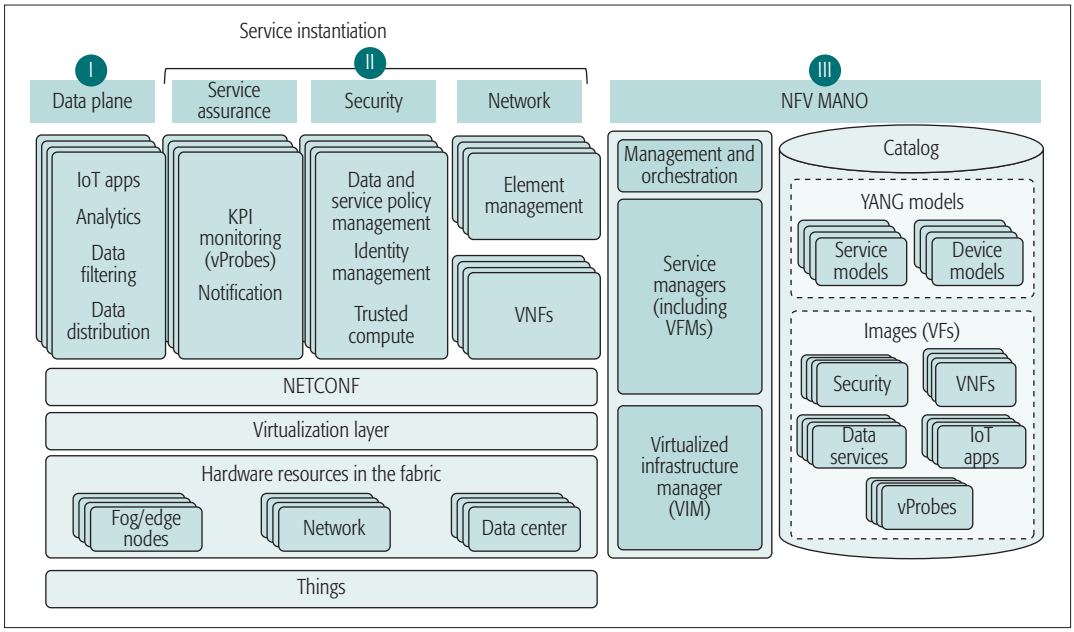


Figure 3. ETSI MANO architecture extended to cover service management beyond the traditional NFV and networking domains. The building blocks are grouped into three main categories, each of which offers a set of services that are common to the large majority of IoT deployments.

gral part of modeling and enabling higher-level services. The composition of YANG models for building services is key to breaking down the complexity of service modeling and for reusing parts of existing service catalogs. This approach is proven to facilitate life cycle management of large collections of services in NFV environments, and is critical to reduce complexity when designing IoT services, with much more infrastructure heterogeneity beyond the data center.

The workflow for deploying a service starts from a service model definition. Subsequently, the service is instantiated and the configuration is enforced on one or more devices in the infrastructure. As shown in Fig. 2, YANG models and corresponding device configurations are stored, and can be rolled back to previous models and/or configuration versions should this be necessary.

The designer of a service model can include key performance indicators (KPIs), and compare the "actual state" of the instantiated service to the "desired state" as part of the service assurance. In case of discrepancy between states, service assurance components depicted in Fig. 3 notify the service managers within the NFV MANO architecture, and orchestration services take action to align the actual state with the desired state.

Toward Converged Service Management

Our approach uses the well-known NFV MANO architecture and extends it to other service categories, beyond NFV and network devices. Figure 3 shows the main building blocks, split into three categories: the data plane; basic components to support data plane functionality (service assurance, security, and networking); and the management plane based on NFV MANO.

The first category consists of services to manipulate, share, and distribute data to other services over the cloud to edge continuum. The second category provides services to ensure secure and reliable service operation and efficient data delivery. The third category encompasses the usual MANO components extended with new models to cover fog nodes and IoT services, and IoT-specific features, especially in the areas of security and service assurance. Except for the presence of NETCONF and YANG, the blocks shown in Fig. 3 are technology-agnostic. NETCONF and YANG are present to emphasize the need for the adoption of standardized and broadly accepted interfaces and data modeling languages.

The main components and implementation (Table 1) are described in more detail below.

Data Plane: Includes data distribution and data sharing services. The data and service policy management module present in the security block (II) allows administrators to share data between tenants in a controlled and secure way. This enables sharing of data between services on multiple fog nodes, and also across fog and cloud, while adhering to policies defined in the data and service policy management module. These policies could be leveraged to build so-called data and resource pricing models [10] as an incentive to optimize resource usage in multi-tenant environments.

The platform supports the utilization of different message brokers if needed. The analytics component can be supported by databases deployed at the edge and the data center. The setup should offer multi-tenancy, and enable streaming and/or historian analytics depending on requirements.

Service Assurance: Services are linked to a certain quality of service, specified by KPIs. An effective technique starting to be used in NFV scenarios is to monitor the KPIs through a set of virtual probes (vProbes), instantiated at the points where relevant parameters need to be monitored, and usually deployed in a distributed way. A combination of passive and active vProbes can efficiently detect violations to KPIs directly at the problem source.

This technique has proven simpler and more

accurate than traditional approaches, which are often based on gathering information from multiple sources, including measurement tools, logs, monitoring systems, and so on, for root cause analysis. In our platform, KPI violation is notified to the service owner, and orchestrator or service manager, to resolve the discrepancy between observed and desired service state. Service assurance forms an integral part of the service definition and composition developed in YANG (captured through service models). The role of vProbes, their locations, and actions that need to be taken upon KPI violations are specified in the service model. Service assurance covers both the infrastructure and the services that multiple tenants will deploy on top of it.

Security: An integral part of the architecture, since the extension of NFV MANO to cover fog and IoT substantially increases the attack surface. Security elements are categorized into the following three groups.

Network-Based Security and Role-Based Access Control: Provided through specific virtual network functions (VNFs), such as firewalls, intrusion detection applications, and so on. Many of these will be instantiated in fog nodes, and service designers decide whether a security VNF is instantiated to protect an entire node (e.g., a fog node), a specific tenant execution environment (TEE) within a node, or a pool of TEEs instantiated in a single chassis or spanning across several of them. This category also covers mechanisms for controlling which services can access what data and when, as well as which users can access what services and resources and when. Mechanisms for authentication and authorization are essential to control data sharing policies and grant access to specific resources for each tenant. Different tenants usually deploy different services, and require different KPIs to be monitored. In the case of Barcelona, data associated with service assurance of different tenants was stored in a geo-distributed historian database. Enforcement of access control on the database ensured separation of information between tenants. Internal communication between components of the platform were also secured using encryption.

Host-Based Security: Includes aspects such as trusted compute based on the trusted platform module (TPM), operating system hardening, disk encryption, vulnerability management and patching policies, security information and event management (SIEM), enforcing isolation among TEEs, and so on. The Barcelona pilot covered the majority of these aspects, with strong focus on securing fog nodes.

Fog-Based Security: Security the system can provide to help protect "things" connected to fog nodes, and protect the fabric and its services from malicious things located at the network edge. The IETF has recently proposed the manufacturer usage description (MUD) specifications [11] as a first step toward a standardized and secure way of onboarding, and connecting, simple "things" to an IoT system. Fog can play an enabling role for MUD, to mediate and automate the process of device onboarding, and to enforce security policies ensuring such devices can only establish communications subject to their intended use.

Network: This covers the core networking VNFs and ancillary systems, such as virtualized switches, routers, DHCP servers, load balancers, WAN optimizers, and so on.

Component	Technology Ecosystem
Analytics	**Cisco ParStream**, Cisco Edge and Fog Fabric (EFF), Apache Storm, GE Predix, SAP, etc.
Data filtering and normalization	**Various processes for anomaly detection including Kalman filters, NearbySensor Agent for data normalization, etc.**
Data distribution	**RabbitMQ**, Cisco EFF, Apache ActiveMQ, DDS, etc.
vProbes (service assurance)	**netrounds probes, NearbySensor Assurance, etc.**
Data and service policy management	**Specifically implemented during the project.**
Identity management	**LDAP and distributed replicas**, Cisco ISE, Active Directory, etc.
Trusted compute	**TPM/TXT, OSSIM, Open Attestation, LUKS, SELinux, AppArmor, QEMU, and secured configuration files.**
VNFs	**Cisco CSR1kv, Cisco Firewalls**, Cisco ESR, Palo Alto Firewalls, load balancers, etc.
Management and orchestration	**Cisco tail-f NSO**, Puppet, Chef, etc.
Service managers (VFMs)	**Cisco Elastic Services Controller (ESC)**, Ciena Blue planet, Brocade, etc.
Virtualized infrastructure manager (VIM)	**OpenStack**, vSphere, etc.
Fog hardware	**Cisco IOx devices, Nebbiolo Technologies, NearbySensor Box, ADLink, Darveen, etc.**
YANG models	**Various models for services and devices: data sharing, analytics, NearbySensor VFs, Fog nodes, etc.**

Table 1. Potential technologies for implementing the main components depicted in Fig. 3. In bold are the ones used in Barcelona, and we also list other alternatives where applicable.

NFV MANO: Unlike traditional NFV deployments, where services are instantiated in environments with homogeneous IT and network infrastructures, for many hyper-distributed IoT environments, heterogeneity of devices and communications is more the rule than the exception. Capturing this heterogeneity in simple, standard, and machine-readable ways is essential. YANG models provide this, since not only can network elements be modeled but also fog nodes, elementary things using MUD specifications [11], as well as IoT services to be deployed. The YANG model snippet in Fig. 2 was used in Barcelona, and was part of the catalog of services and device models shown on the right of Fig. 3.

The NFV MANO block in Fig. 3 is based on ETSI's three-tier model:

- Management and orchestration
- Service managers, supporting multiple vendors
- The virtualized infrastructure manager (VIM)

Traditional VNFs in ETSI's MANO terminology correspond to a subset of virtual functions (VFs) managed by our architecture, with many of our VFs containing IoT-related functions rather than only network functions. A certain level of atom-

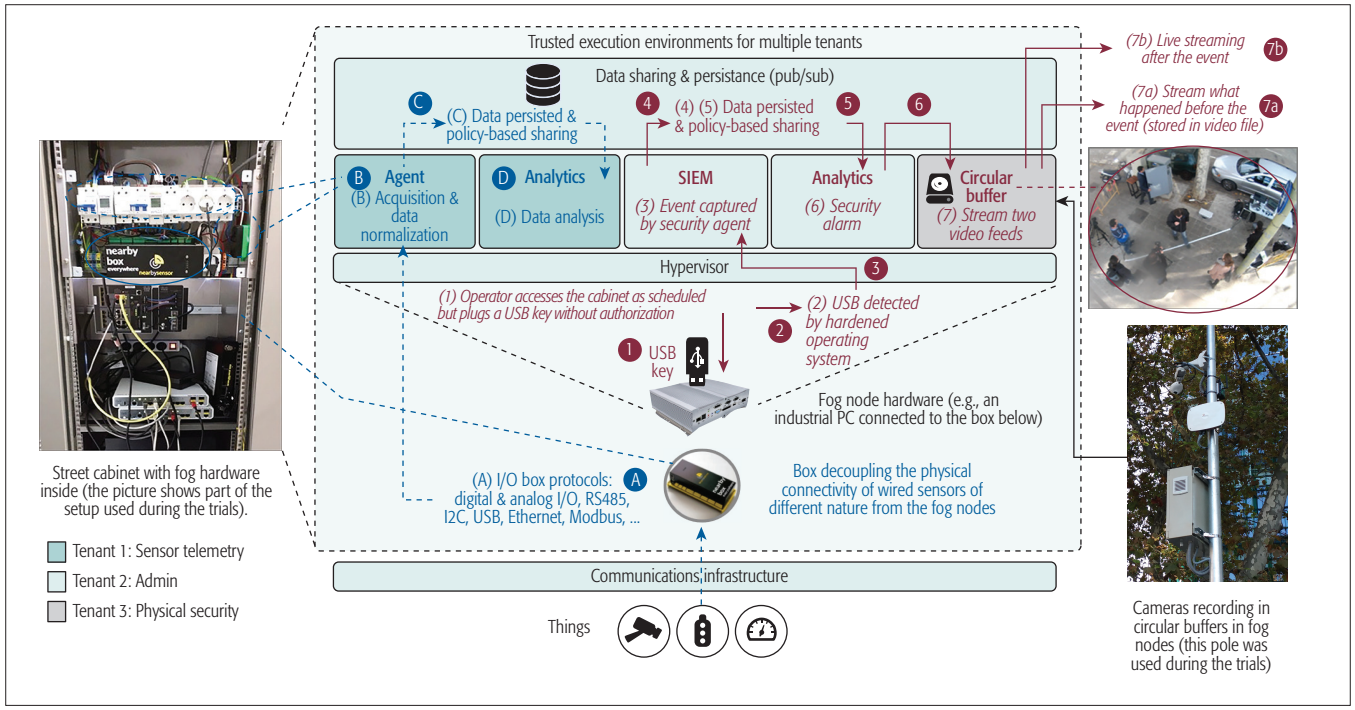


Figure 4. Two use cases deployed and managed through our converged architecture. They involve different tenants and different VFs running concurrently in a single fog node housed in a street cabinet. Sequence A–D represents the data flow for the first use case (sensor telemetry), while sequence 1–7 represents the flow for the second one (physical security of fog nodes outdoors). All the services and devices shown in the figure have their corresponding YANG models.

ic behavior when updating many services at the edge is a necessity. The MANO system achieves this through transactional operations across services involved. This is similar to a two-phase commit across multiple databases, ensuring physical devices associated to these services continue to function properly, and the system as a whole stays in a consistent state.

Services are deployed by combining the YANG models, associated images for the VFs to be instantiated and configurations of networks, message brokers and data flows, security policies, databases, and so on supporting the service. Either a user will specifically push a new service to a set of edge, network, or data center nodes, or, depending on the KPIs and overall system state, MANO will determine the best possible location for services to be deployed. Because all fabric hardware resources have NETCONF interfaces and are described through appropriate YANG device models, from a deployment perspective, there is no distinction between edge, network, or data center nodes.

Technologies for Implementing the Architecture

While previous paragraphs describe the main architectural components, Table 1 shows various technologies that can be leveraged to implement them, including ones used in the Barcelona pilot. YANG models of fog nodes or service components can be implemented by various hardware and software vendors (or developed by the open source community). These models can become part of our implementation. Indeed, several YANG models and service templates could become part of the OFC interoperability trials [4], and, together with the extended MANO architecture presented in this article, form part of a reference framework for open implementations.

Motivation and Pilot Implementation in the City of Barcelona

Barcelona realized that the more than 3000 street cabinets deployed in the city form a natural infrastructure to build out their smart city vision. Their goal is to have a single, extensible, and distributed platform from edge to cloud to address opportunities that current and future technologies for urban services will bring in an integrated way. The incentives behind this approach are described in detail in [12], but one of the aims is to reduce solution silos and the cost of operating different solutions in the city. While [12] addresses multiple use cases where fog is mandatory, this section delves into the orchestration needs, and outlines the automation and uniform life cycle management of two use cases spanning the cloud to edge continuum (Fig. 4). These use cases were recently demonstrated in Barcelona, and extend those described in [12].

Dealing with Scale and Management Complexity

Fog nodes were housed inside cabinets, such as the one shown on the left of Fig. 4. For resiliency, some services require more than one fog node per cabinet. A large fraction of cabinets will host instances of the same service, so managing the life cycle of a single service across the city may involve the configuration of thousands of fog nodes.

The development of an IoT service usually entails the integration of multiple technologies supplied by a partner ecosystem, including sensors, application-specific gateways, fog and network nodes, data brokers, security, and so on. Thus, managing the life cycle of an IoT service (i.e., onboarding devices, performing day zero

configurations, as well as managing the state and configurations after the initial deployment) can become quite complex — a challenge faced in Barcelona, and other cities and industries.

The NFV and 5G communities have addressed similar challenges, both heavily betting on the ETSI MANO architecture. We argue that this architecture will not only facilitate the convergence of NFV, 5G/MEC, and fog, but will also offer the automation means to deal with the scale and complexity posed by IoT. The goal is to hide underlying complexity from administrators, and turn IoT service management into simple and intuitive operations. The success of platforms such as Amazon's AWS Lambda, Google's search engine, or legacy technologies like TV is largely due to the way they manage scale, and the way they have abstracted the underlying complexity from end users. The pilot conducted in Barcelona followed the same principles.

Setup in Barcelona

Figure 4 offers a schematic view of a setup used during the Barcelona pilot. The left side shows a cabinet interior with several elements:

- A power distribution board with different monitoring elements and circuit breakers
- A box that enables decoupling and aggregating the physical connectivity of different families of wired sensors, simplifying the I/O requirements of the fog nodes
- The fog nodes themselves
- Others

The central part of the figure provides a logical representation of the setup, and shows data flows for two different use cases demonstrated in Barcelona. The bottom shows a set of "things" (e.g., sensors and control and actuation elements), which can be located both within and outside cabinets.

We used fog nodes supplied by different vendors (Table 1). The example in the figure shows an industrial PC, connected through Ethernet to the NearbySensor box. The top of the figure illustrates the hypervisor as well as several TEEs, which belong to three different tenants running in the fog node. The right side shows part of the external setup for one of the use cases, including a pole, a camera, and a snapshot of one of the videos captured by the latter.

We proceed to describe two use cases depicted in Fig. 4, with emphasis on automation enabling the data flows illustrated therein.

Use Case 1: Sensor Telemetry through Street Cabinets

From a data plane standpoint, this use case is depicted as sequence A–D in Fig. 4. Step A shows how specialized hardware at the network edge can help aggregate and simplify communication with different types of sensors (e.g., for monitoring temperature, power, and access), as well as a number of controllers, such as circuit breakers and uninterruptible power supplies, using various protocols and interfaces.

Data collected through the box in A is sent to an agent (B), which normalizes the data. This agent is part of a TEE that belongs to the city department in charge of monitoring the cabinets and the environment (tenant 1 in Fig. 4), and can run in a Docker container or a VM depending on security and performance requirements. Data processed by the agent can be maintained and shared in a policy-based and secure way with other processes running either on the fog node, on other fog nodes, or in the cloud (C). The data sharing and persistence block on the top belongs to the administrative tenant in charge of managing common services across tenants (tenant 2), such as data sharing policies, system-level analytics, and the security of the fog node itself. Step D shows tenant 1 subscribed to different data topics, enabling the gathering and examination of data from different sources, and triggering actionable decisions based on the result of the analysis. Applications (and their YANG service models) running in B and D can be supplied by different providers.

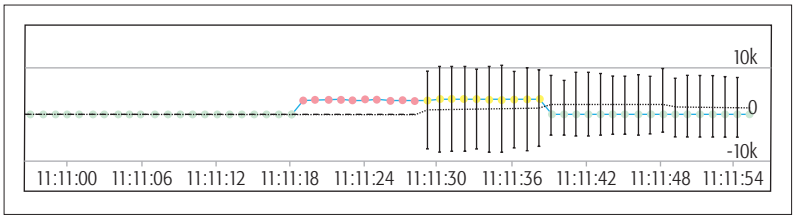


Figure 5. Power consumption data (in Watts) associated with sequence A–D depicted in Fig. 4. The dots represent the observed values B–C; the dotted curve represents estimated values and uncertainty using a Kalman filter (D).

In the example, the process in D analyzes — among other things — power consumption obtained from monitors connected to the box in A, and estimates upcoming values based on a Kalman filter (Fig. 5). The goal of the analysis is three-fold:

- Estimate and control the power consumed to prevent spikes in energy use from multiple devices.
- Dynamically manage which devices remain operatonal in case of a power outage.
- Control the service level agreement (SLA) with the energy supplier. Since the processes run locally in the fog node, this analysis and control will remain operative even if the node loses backhaul connectivity to the cloud.

The deployment of services supporting the use cases depicted at the center of Fig. 4 was entirely automated, and managed using the architecture shown in Fig. 3. Configuration of fog nodes was performed as follows:

- Zero-touch provisioning including full installation of operating system, initial configurations, security, and so on
- Deploying and configuring initial function packs, such as data sharing and persistence elements, a set of vProbes for service assurance, and more
- The tenant's TEEs, the security configurations enforcing segmentation and isolation between tenants, including their corresponding networks
- Configuration of message brokers enabling the data workflows (A–D) shown in the figure

All stages required for deploying and configuring the IoT services shown in Fig. 4 were managed with a few clicks. More importantly, instantiations

Cameras record continuously and send video to associated Fog nodes, where they are stored in circular buffers. Only when an event occurs, such as inserting a USB key, the Fog-based system triggers two video streams: what happened before the event (stored in the circular buffer); and what happens right after the event in real-time.

can be done in an individual cabinet or thousands of them across the city once the service models and the corresponding images are available from the catalog illustrated on the right side of Fig. 3. This approach reduces the operating expenditure for managing a smart city infrastructure considerably.

Use Case 2: Physical Security of Fog Nodes

Physical security of cabinets and the devices inside is of utmost importance for the city, so we implemented several security layers. This section describes how unauthorized USB access to a fog node is detected and recorded on video (cf. the right side of Fig. 4).

Cameras record continuously and send video to associated fog nodes, where they are stored in circular buffers. Only when an event occurs, such as inserting a USB key, does the fog-based system trigger two video streams: what happened before the event (stored in the circular buffer and what happens right after the event in real time. The reasons for not streaming continuously to the cloud, but deploying services at the edge using fog, are cost, privacy, and data storage overheads [12]. Actions taking place after the USB stick is plugged in (step 1 in Fig. 4) until the video is stored and made available correspond with steps 2–7 in Fig. 4: 2) the USB is detected, generating an event; 3) the event is captured by a SIEM agent; 4) and 5) reporting the event through the communication bus; 6) analysis of the event and triggering the appropriate response; and 7) streaming the videos to one or more predefined locations (e.g., in the cloud). Communications between the use case components occur transparently, and there is no semantic separation between fog and cloud deployed components.

An important aspect is the multi-tenant nature of the converged cloud/network/fog platform, as services supporting this use case were deployed on the same fog node used before. As in the previous use case, not all services and hardware needed for implementing the use case were managed by the same city department. The IT department manages the services running in the cabinets, while the cameras and their functionality are managed by another department. We leveraged common functions offered by the platform, including the data sharing service, various security and service assurance functions, and so on.

This use case demonstrates that, an IoT service is typically composed of multiple services. Services can be managed by different tenants or securely shared among multiple tenants (cf. the data sharing service in Fig. 4). Some services may be deployed and associated solely with an IoT service and tenant (e.g., the circular buffer service in Fig. 4). Besides service composition and reusability, the aim is to turn the deployment and management of IoT services into almost trivial tasks, which can be operated through a set of intuitive actions (performing a few clicks on a dashboard). All these aspects are at the heart of our converged architecture.

Related Work

The authors in [13] discuss how some of the MANO concepts can be exploited to deliver end-to-end network services using a description-based approach over a set of distributed resources. This work has similarities with ours, although our focus is mainly IoT and fog, whereas [13] is centered on the orchestration and deployment of network services. Note that the work discussed in this article sits at the intersection of NFV, 5G/MEC, and IoT and fog, and extends the concept beyond the data center and networking to fuse cloud and fog. While MEC focuses mainly on the edge of the network [6], our approach covers the continuum from edge to cloud.

Service configuration and life cycle management are important aspects of our platform. Several products such as Puppet, Chef, Ansible, and Salt provide configuration management and help automate deployment of services. Other products like Terraform, CloudFormation, and OpenStack provide infrastructure life cycle management capabilities (e.g., for day 0 configuration), which can be combined with tools like Puppet or Chef (for day 1 onward). However, all these products mainly target IT infrastructures. In IoT, the fundamental requirements in terms of connectivity (I/O interfaces), security, applications, and data management are significantly different from those that rule the life cycle management of IT servers. The compute resources available in a fog environment are typically much more heterogeneous, and the criticality of some applications requires special treatment.

This heterogeneity, combined with the criticality of some of the services connected to physical devices, creates new requirements for service life cycle management that go far beyond what state-of-the-art tools in the IT space currently offer. Our approach takes into account this heterogeneity natively.

Finally, many of the members of the OFC are already offering fog products. This is the case of Foghorn, Nebbiolo, and Cisco, just to name a few [4]. At the time of writing, none of the products available in the marketplace are focused on a converged NFV, 5G/MEC, fog, and cloud paradigm, with emphasis on exposing the infrastructure as a single and unified computing fabric.

Conclusion

This article describes an architecture that addresses some of the central challenges behind the convergence of NFV, 5G/MEC, IoT, and fog. By using a two-layer abstraction model, along with IoT-specific modules enriching the NFV MANO architecture, we introduce a promising paradigm to fuse cloud, network, and fog, and apply this to a project in the city of Barcelona. For now, we focus only on a small number of use cases. We expect that once we start expanding this model to different domains and cities, more end-user services will be developed, enabling the reutilization of service models and associated service catalogs.

References

[1] "NFV"; http://www.etsi.org/technologies-clusters/technologies/nfv, accessed May 10, 2017.

[2] I. Chih-Lin *et al.*, "5G: Rethink Mobile Communications for 2020+," *Phil. Trans. R. Soc. A*, vol. 374, 2016.

[3] F. Bonomi *et al.*, "Fog Computing: A Platform for Internet of Things and Analytics," *Big Data and Internet of Things: A Roadmap for Smart Environments in Series Studies in Computational Intelligence*, vol. 546, 2014, pp. 169–86.

[4] OpenFog Consortium; http://www.openfogconsortium.org/, accessed May 10, 2017.

[5] "Network Functions Virtualisation (NFV), Management and Orchestration"; http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf, 2014, accessed May 10, 2017.
[6] Y. C. Hu *et al.*, "Mobile Edge Computing A Key Technology towards 5G"; http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf, 2015, accessed May 10, 2017.
[7] "YANG — A Data Modeling Language for the Network Configuration Protocol (NETCONF)," IETF RFC 6020; http://www.rfc-editor.org/rfc/rfc6020.txt, accessed May 10, 2017.
[8] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Commun. Surveys & Tutorials*, vol 19, no. 2, 2nd qtr., 2017, pp. 855–73.
[9] "Fog Computing: Keystone of Industry 4.0, KUKA/Nebbiolo Technologies"; https://www.kuka.com/-/media/kuka-corporate/documents/press/kuka_nebbiolo_solutions.pdf, accessed May 10, 2017.
[10] M. Chiang *et al.*, *Smart Data Pricing*, Wiley, 2014.
[11] E. Lear, R. Droms, and D. Romascanu, "Manufacturer Usage Description Specification," IETF draft; https://tools.ietf.org/html/draft-ietf-opsawg-mud-05, 2017, accessed May 10, 2017.
[12] M. Yannuzzi *et al.*, "A New Era for Cities with Fog Computing," *IEEE Internet Computing Mag.*, Special Issue on Fog Computing, vol. 21, Mar./Apr. 2017, pp. 54–67.
[13] I. Cerrato *et al.*, "Toward Dynamic Virtualized Network Services in Telecom Operator Netnetworks," *J. Computer Networks*, vol. 92, 2015, pp. 380–95.

Biographies

Frank van Lingen (fvanling@cisco.com) is a technology strategist at Cisco's Corporate Strategy Office where he works on strategic innovation, emerging technologies, and customer/partner co-innovation, focusing on areas such as analytics, fog computing, AI, and the Internet of Things. He has a Ph.D. in computer science from the University of Technology Eindhoven.

Marcelo Yannuzzi (mayannuz@cisco.com) is a principal engineer at Cisco's Corporate Strategy Office, where he works on strategic innovation in the areas of fog computing, IoT, and security, and provides strategic advice on new business opportunities and technologies for Cisco. He has a Ph.D. in computer science from the Technical University of Catalonia — BarcelonaTech.

Anuj Jain (januj@cisco.com) is a director at Cisco's Corporate Strategy Office. He leads an innovation team working in the areas of fog computing, IoT, next-generation computing, artificial intelligence, and security, with a focus on disruptive technologies and strategic business opportunities for Cisco. He has an M.S. in micro-engineering from EPFL.

Rik Irons-Mclean (rironsmc@cisco.com) is a lead architect for next generation IoT platforms in Cisco's Industry Product and Technology Group. As both lead architect and technical lead, he has successfully delivered a number of emerging technology solutions for smart grid, process automation, oil and gas, building automation, and green energy. He has an M.B.A. from the Bradford University School of Management, and is currently studying for a doctorate in cyber security.

Oriol Lluch Parellada (orilluch@cisco.com) is a technology strategist at Cisco's Corporate Strategy Office where he works on strategic innovation in the field of artificial intelligence. His research interests include cloud infrastructure, fog computing, service orchestration, and artificial intelligence. He has an M.S. in telecommunications engineering from the Technical University of Catalonia — BarcelonaTech and an E.M.B.A. in management of technology from EPFL and HEC Lausanne.

David Carrera (david.carrera@bsc.es) leads the Data-Centric Computing Research Group at the Barcelona Supercomputing Center (BSC). His research interests include performance management of data-centric platforms. He has a Ph.D. in computer science from the Technical University of Catalonia — BarcelonaTech.

Juan Luis Pérez (juan.luis.perez@bsc.es) is a senior research engineer in the Data-Centric Computing Research Group at the Barcelona Supercomputing Center. His research interests include model-driven IoT. He has an M.S. in computer architecture, networks, and systems from the Technical University of Catalonia — BarcelonaTech.

Alberto Gutiérrez Torre (alberto.gutierrez@bsc.es) is a Ph.D. candidate in the Data-Centric Computing Research Group at the Barcelona Supercomputing Center. His research interests include applied machine learning, in particular, over IoT/stream data. He has an M.S. in data science from the Technical University of Catalonia — BarcelonaTech.

Diego Montero (dmontero@ac.upc.edu) is a Ph.D. candidate at the Networking and Information Technology Lab (NetITLab), where his research interests include network security, SDN, network virtualization, fog computing, and network mobility. He has an M.S. in computer architecture, networks, and systems from the Technical University of Catalonia — BarcelonaTech.

Josep Martí (jmarti@nearbysensor.com) is the managing director and R+D projects coordinator at NearbySensor, focusing on strategic cooperation with other companies and government agencies. He has an M.S. in telecom engineering from the Technical University of Catalonia — BarcelonaTech.

Ricard Masó (rmaso@nearbysensor.com) is the CTO at NearbySensor, where he is also the lead architect of its software products and solutions, devoted to the quick and simple integration of operational and information technologies. He has a degree in pedagogy from the University of Barcelona and is an associate professor for computing science at the Open University of Catalonia.

Pedro Rodriquez (jprodriguez@nearbysensor.com) is the engineering director at NearbySensors where he works on innovation in IoT, distributed systems, automation, edge computing, and embedded systems. He holds degrees in telecom engineering, electrical engineering, and economics, and an M.B.A. from the IESE Business School.

This heterogeneity, combined with the criticality of some of the services connected to physical devices, creates new requirements for service lifecycle management that go far beyond what state-of-the-art tools in the IT space currently offer. Our approach takes into account this heterogeneity natively.

TelcoFog: A Unified Flexible Fog and Cloud Computing Architecture for 5G Networks

Ricard Vilalta, Victor López, Alessio Giorgetti, Shuping Peng, Vittorio Orsini, Luis Velasco, René Serral-Graciá, Donal Morris, Silvia De Fina, Filippo Cugini, Piero Castoldi, Arturo Mayoral, Ramon Casellas, Ricardo Martínez, Christos Verikoukis, and Raul Muñoz

The authors propose the TelcoFog architecture as a novel, secure, highly distributed, and ultra-dense fog computing infrastructure, which can be allocated at the extreme edge of a wired/wireless network for a telecom operator to provide multiple unified, cost-effective, and new 5G services, such as NFV, MEC, and services for third parties (e.g., smart cities, vertical industries, and IoT).

ABSTRACT

We propose the TelcoFog architecture as a novel, secure, highly distributed, and ultra-dense fog computing infrastructure, which can be allocated at the extreme edge of a wired/wireless network for a telecom operator to provide multiple unified, cost-effective, and new 5G services, such as NFV, MEC, and services for third parties (e.g., smart cities, vertical industries, and IoT). The distributed and programmable fog technologies that are proposed in TelcoFog are expected to strengthen the position of the mobile network and cloud markets. TelcoFog, by design, is capable of integrating an ecosystem for network operators willing to provide NFV, MEC, and IoT services. TelcoFog's key benefits are the dynamic deployment of new distributed low-latency services. The novel TelcoFog architecture consists of three main building blocks: a scalable TelcoFog node, which is seamlessly integrated in the telecom infrastructure; a TelcoFog controller, focused on service assurance and based on service data modeling using YANG, which is integrated in the management and orchestration architecture of the telecom operator; and TelcoFog services, which are able to run on top of the TelcoFog and telecom infrastructure. The TelcoFog architecture is validated through a proof of concept for IoT services.

INTRODUCTION

Telecom operators require cloud computing and storage infrastructures, integrated with their heterogeneous access and transport networks, in order to provide software defined networking (SDN), network functions virtualization (NFV), mobile edge computing (MEC), and cloud radio access network (C-RAN) for future 5G services. Virtualized functions (e.g., mobile Evolved Packet Core – EPC, firewall, local cache, video analytics, video storage, central cache, virtual base station, virtualized BBU-BBU hosteling) are typically deployed in specialized and dedicated hardware. To that end, telecom operators need to dynamically allocate computing and storage resources to flexibly deploy virtualized functions in cloud infrastructures where needed. Notwithstanding, deploying a private cloud infrastructure integrated with the telecom network presents a differential set of challenges due to the industry's inherent requirements for high availability (5-nines), ultra-low latency, and complex networking (Ethernet, optical, wireless, etc.).

Given the tendency to softwarize most of the functions of a telecom network, network operators are in transition from operating the network to programming the network. In order to fulfill this vision of intelligent network resources offering NFV, MEC, or Internet of Things (IoT) services, spread through the whole network, from the core to the edge, this article proposes TelcoFog as an innovative architecture based on software defined networking (SDN), NFV, and MEC that provides distributed services.

The fog computing is a relative new cloud computing concept. The basics and objectives of Fog computing (e.g., geographical distribution, low-latency applications, mobility, end so on) have been previously explained in the literature [1]. Fog nodes, located at the network edge, are required to support a number of heterogeneous services by providing computational, storage, and networking resources. These services have their own requirements in terms of bandwidth, latency, reliability, and so on. Moreover, the adoption of fog computing brings the possibility that (cloud) resources allocated for each service may be distributed among a number of functions (generic virtualized functions), which are instantiated through selected fog nodes. Reference [2] proposes a distributed architecture that solves use cases which cannot be successfully implemented using "cloud only" solutions or independent edge devices.

The distribution of functions and the subsequent forwarding of the (control and data) traffic through those functions is referred to as service function chaining (SFC) [3]. Within TelcoFog, the SFC concept is adopted in fog computing, in order to offer added-value services in all the targeted scenarios (i.e., IoT, MEC, and NFV).

To make the above concepts reality, it will be necessary to provide a control and orchestration system (the TelcoFog controller) able to allocate cloud resources for the VNFs of a specific service along with defining its SFC. For the latter, the TelcoFog controller should also ensure the connectivity (network resources) among the different fog nodes, accommodating the virtual net-

Ricard Vilalta, Arturo Mayoral, Ramon Casellas, Ricardo Martínez, Christos Verikoukis, and Raul Muñoz are with CTTC/CERCA; Victor López is with Telefónica; Alessio Giorgetti, Filippo Cugini, and Piero Castoldi are with Scuola Superiore Sant'Anna; Shuping Peng is with Huawei; Vittorio Orsini is with Ericsson; Luis Velasco and René Serral-Gracià are with UPC; Donal Morris is with RedZinc; Silvia De Fina is with H3G.

Digital Object Identifier:
10.1109/MCOM.2017.1600838

work functions (VNFs), to enable traffic steering according to the computed SFC [4]. This provides seamless and unified control for the complete visibility, computation, and allocation of both cloud/fog and network resources through different network segments (access, aggregation, and transport) assuming heterogeneous access and transport technologies (e.g., WiFi, packet switching, optical transmission) with the goal of satisfying and ensuring (stringent) service requirements (e.g., zero-latency applications for mission-critical machine communications). To this end, a fundamental action to be done, currently not completely accomplished, is the definition of a common data model for devices and TelcoFog services that will be used by TelcoFog controller.

Besides the fog-like nature of TelcoFog and its orchestration capabilities, another critical aspect is the adoption of YANG as a data modeling language, which has been steadily growing in the IT and networking communities for the last few years, for example, in the optical networking community [5] — and consequently, its use has been increasing in multiple standards defining organizations. There is still a lot to define regarding computational resources and devices to cover the IoT landscape, from sensors to IoT gateways and related applications (e.g., IoT services and the enabled application ecosystem that better exploit the gathered knowledge) [6]. Moreover, it shall include smart and expert systems able to apply newer approaches involving the manipulation and processing of a large volume of data (e.g., big data). The architecture in [2] does not include this modeling perspective for services using YANG, and thus, it can benefit from TelcoFog innovations. This data modeling approach was introduced by UNIFY Universal Node [7].

In this context, there are many aspects to standardize including, but not limited to, information and data models for the core/main devices in a given architecture, which can be built by inheritance or composition, with a common subset, but allowing for applicable extensions. Another important aspect to standardize are application programmable interfaces (APIs) between functional elements in the encompassing frameworks and related service workflows, including, as important ones, resource, device, service exposition, and (auto)discovery. In line with this, TelcoFog architecture is expected to fulfill the requirements associated with dynamic platforms and deployments, as we demonstrate in the proof of concept (PoC) section.

The adoption of a common, flexible, and powerful data and information modeling language to express all sensors, actuators, gateway facilities, and services is a first, important step toward the standardization of IoT frameworks across multiple vendors beyond the existing ones. Moreover, a standardized IoT framework shall include the optimization of the underlying data transport network. Since this objective is known to be ambitious and mid- to long-term, an important goal is also ensuring at least a certain level of interoperability in complex deployments. The widest adoption of a common set of models, methodologies, and approaches is an enabler for further automation in the integrated control and management of IoT platforms that include, in addition to the main components in an IoT deployment, the integration of the heterogeneous transport network as a core component.

This article presents the basic components of the novel TelcoFog system architecture, and it provides a PoC for the dynamic deployment of IoT services at the network edge. In the following section, this article introduces the infrastructure challenges from an operator's perspective. Next we focus on the description of TelcoFog architecture. Then we introduce the developed TelcoFog PoC, and the final section concludes the article.

The Challenges for a Unified Flexible Fog Computing Infrastructure for Telecom Operators

Telecom operators shall accommodate a wide range of use cases with different requirements (e.g., security, latency, resiliency, and bandwidth) for fifth generation (5G) services, which will include NFV, MEC, and IoT services and applications. This opens a whole new set of significant challenges, which we present in this section.

Challenge 1: Fog Computing for Network Operators

It is clear that a distributed data center (DC) architecture is needed for network operators so as to improve the perceived quality of experience (QoE) for their users, reduce energy consumption [8], or even have high-level and fast reaction in response to events such as network failures. Such distributed cloud architecture was named the telecom cloud in [9]. Scalability also has to be considered in the telecom cloud since, in contrast to a small number of warehouse-sized DCs commonly used in public clouds, the telecom cloud must support a large number of small, distributed DCs to reduce traffic in the core network.

While both fog and cloud use networking, computing, and storage resources, and share many of the same mechanisms and attributes (virtualization, multi-tenancy), the extension is nontrivial. Fog computing enables a new breed of applications and services that goes beyond the regular telecom services, so there is a fruitful interplay between the cloud and the fog. Therefore, there is a need for a distributed intelligent platform at the edge that manages distributed computing, networking, and storage resources (see an example in [9] for video distribution).

Challenge 2: Fog and Cloud Computing Interconnection through Operator SDN-Enabled Networks

A hybrid cloud-fog computing architecture is needed, which spans from the edge (fog) to the core (cloud). Services deployed in fog nodes will interwork with cloud-located services; thus, developing a resource orchestration mechanism will be of the essence. It shall interconnect both fog and cloud domains, which will be interconnected through heterogeneous operators' networks.

A related challenge is the fact that operators are reluctant to incorporate the principles of SDN. There is work to overcome this in [10] where the authors propose the usage of a transport API for the control and management of future transport networks. Even though its detailed definition and

Fog computing enables a new breed of applications and services that goes beyond the regular telecom services, so there is a fruitful interplay between the cloud and the fog. Therefore, there is a need for a distributed intelligent platform at the edge that manages distributed computing, networking, and storage resources.

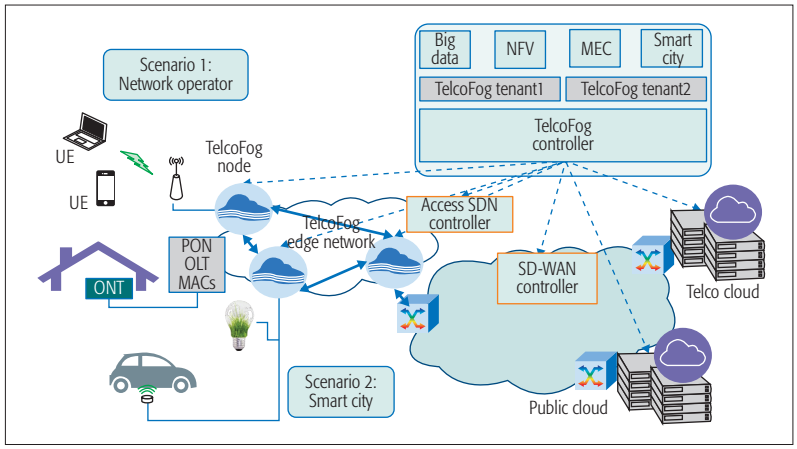


Figure 1. TelcoFog architecture.

development still remain a challenge, it might help the programmability of the operators' SDN-enabled networks. Cloud interconnection has been recently studied [11], but joint integration of fog and cloud paradigms and their network interconnection remains a research challenge. A basic network isolation mechanism at the fog node might be obtained through the introduction of per-tenant software switches; the TelcoFog network standard isolation mechanisms could be used as well (e.g., VxLAN, GRE).

Challenge 3: Decentralized NFV Services

The growth of NFV is driving the softwarization of all functions in the network that are traditionally deployed in dedicated hardware. By eliminating specialized network processors, multiple heterogeneous workloads can be consolidated onto a single architecture, thus reducing complexity and simplifying operation, which leads to reducing total cost of ownership (TCO). Therefore, NFV enables the migration into a telecom cloud and the transition of the operator network to SDN control, at the same time allowing the programmability of the network resources for fully utilizing the capacity of the deployed physical resources [4].

Challenge 4: Mobile Edge Computing and D2D Communication

Besides NFV, telecom operators are also studying the benefits and business models of addressing MEC, which provides IT and cloud-computing capabilities within the RAN in close proximity to mobile subscribers. MEC allows content, services, and applications to be accelerated, increasing responsiveness from the network edge. The user's experience can be enriched through efficient network and service operations. Using MEC, network operators can deploy fog nodes in the RAN and open the radio network edge to third-party partners, allowing them to rapidly deploy innovative applications and services toward mobile subscribers, enterprises, and other vertical segments.

Challenge 5: Smart City Services on Top of a Fog Computing Architecture

The need for data processing, analysis, and security close to the connected things at the edge of the network is leading to an explosive growth of independent gateways, repeaters, and systems with vendors' proprietary information models that do not interoperate. This results in siloed solutions that do not interoperate and increase TCO for smart city operators and vertical industries. They must have an open, flexible, and secure platform on which to consolidate siloes and services at the edge and to connect intelligently with the cloud [12].

Challenge 6: Integration with a Big Data and Analytics Framework

In recent years, the term big data has emerged to describe a new paradigm for data applications. The heart of the big data paradigm is that data is too broad, arrives too fast, changes too fast, contains too much noise, or is too diverse to be processed within a local computing structure using traditional approaches and techniques. The big data paradigm consists of the distribution of data systems across horizontally coupled independent resources to achieve the scalability needed for the efficient processing of extensive datasets. The challenge is to provide the necessary extensions to big data frameworks in order to provide the necessary TelcoFog node computational and storage resources for applications.

TelcoFog System Architecture

Figure 1 shows the proposed TelcoFog architecture and how it can be introduced at the edge of a network operator infrastructure in order to fulfill the presented challenges. We can observe that TelcoFog nodes are placed at the edge of the network. Two scenarios are envisaged: a) integrated network operator services and b) integrated smart city services. TelcoFog nodes might create an overlay network (referred to as a TelcoFog edge network) on top of the operator's access network in order to interwork, allowing different networking services (e.g., multicast or anycast services based on the emerging segment routing technology). In both scenarios, the TelcoFog node plays a significant role in providing the necessary distributed and secure computing, storage, and networking infrastructure in order to provide the targeted services. The TelcoFog controller can act in both a hierarchical (parent/child) anda peer architecture for the optimal allocation of resources across several networks and TelcoFog nodes. It also includes a mechanism for slicing such TelcoFog resources, as well as providing a standardized procedure to describe and deploy TelcoFog services. Finally, to complement these mechanisms, a big data and analytics framework is also provided.

TelcoFog nodes act as interconnected and highly distributed resources closer to the network edge. To fulfill this view, TelcoFog architecture proposes the necessary technologies to obtain highly performing, secured, and resilient TelcoFog nodes, and the necessary TelcoFog controller, which is responsible for the orchestration of TelcoFog resources, as well as their interconnection through highly programmable networks.

Figure 2 provides an overall description of the basic components in both the TelcoFog node (below) and TelcoFog controller (above).

TelcoFog Node

The TelcoFog node is the fog/network infrastructure that is responsible for provisioning the necessary computation, storage, and networking resources. Physically, a TelcoFog node might con-

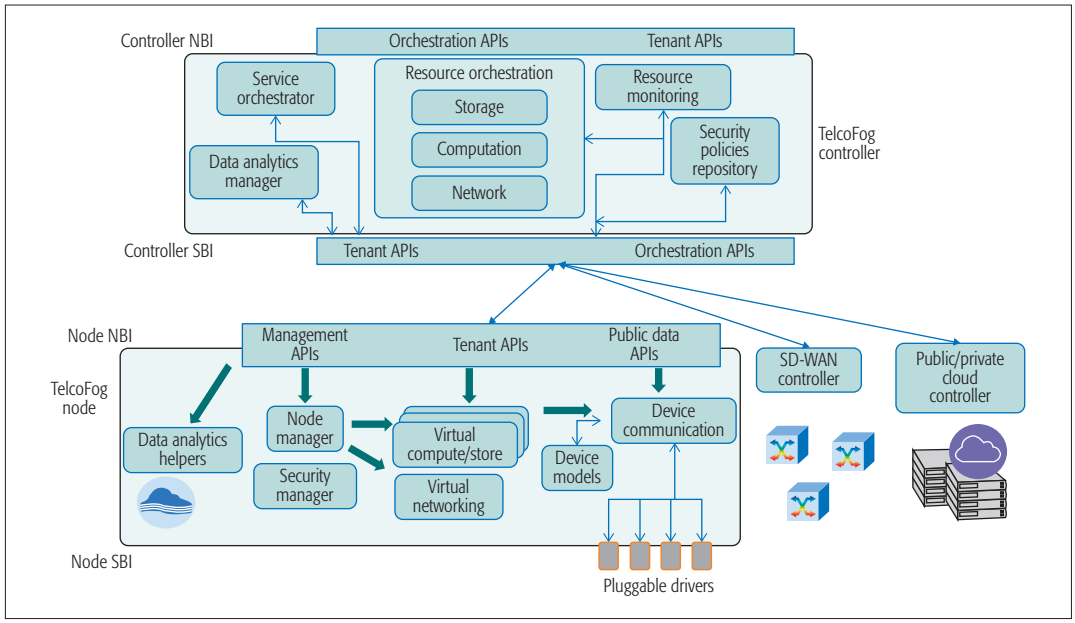


Figure 2. Detailed TelcoFog system architecture.

The TelcoFog controller can both act in a hierarchical (parent/child) or peer architecture for the optimal allocation of resources across several networks and TelcoFog nodes. It also includes a mechanism for slicing such TelcoFog resources, as well as providing a standardized procedure to describe and deploy TelcoFog services based on YANG data models..

sist of a set of (mission-critical) servers, hard disks, and network interface cards. Logically, a TelcoFog node incorporates a node manager in order to handle the offered TelcoFog virtual resources. A Security Manager is responsible for handling the device authorization, authentication, and encryption. Finally, the device communication module allows the abstraction and control of the underlying smart things and devices, through the data modeling of the devices. Devices' configuration, procedures, and notifications are modeled and can be (auto) discovered and related through services running in the TelcoFog node.

The Node Manager handles the optimal allocation of the required virtual resources onto the node physical resources, which are the pool of existing resources within the node. The virtual allocated resources might include containers or virtual machines (depending on the capabilities of the node), allocated virtual memory, virtual disk space or virtual network interface cards, and virtual switches. The TelcoFog node leverages on the existing fog node solutions focused on virtual computation resources, and it provides the necessary extensions in order to ensure a high degree of resource virtualization.

To access the particular smart things and devices, a TelcoFog node foresees the abstraction of the things' data model description by a Device Communication module. This module provides a set of Pluggable Drivers that allow uniform access to the things; these drivers are extensible and use a public interface to allow the easy integration of sensors, actuators, or any other devices by modeling their behavior in the Device Models. This allows the disaggregation of the fog resource toward the extreme edge of the network, as smart devices could also be used for processing, storage, and networking purposes. Another important component within the node is the Data Analytics Helpers, a predefined set of functionalities for data analysis and evaluation that can be provided as services running on top of allocated virtual resources.

TelcoFog services abstract the access to the different smart things and devices by means of a Device Proxy, as part of the Device Communication module, which interplays between the users, the tenants (through a privileged API allowing an enhanced set of features), and the things. The main purpose of this proxy is to provide finer granularity and a more powerful system to control the access to the things, homogenizing its access, being able to enforce the necessary Security Policies, using the Security Manager to offer the sufficient smart caching capabilities to avoid the unnecessary resource consumption of the things.

Finally, in order to allow the usage of all these functionalities, the TelcoFog node offers a common northbound interface (NBI) that can be split into three different views: i) management API, ii) tenant API, and iii) public data API. The management API is used to manage the resources within the TelcoFog node and should be only used from the TelcoFog Controller (the Security Manager enforces this). The tenant API is used as a private interface to allow the different tenants to control and manage TelcoFog services, which gather data from the allocated virtual resources. Finally, the public data API provides access to the monitored data that Security Manager policy specifies as publicly available.

TelcoFog Controller

The TelcoFog controller extends the concept of an NFV orchestrator in order to support the dynamic deployment of generic virtualized functions (hereafter referred to as TelcoFog services). Its main role is the distributed orchestration of resources and services. To this end, the core block of this unit is the Resource Orchestration; its main role is to define and enforce the resource orchestration logic, defining the particular logic that allows the system to allocate the different storage, computation, and network resources. To achieve this, the Resource Orchestrator will receive information about the status of each fog node through its Resource Monitoring module, which will have an updated view

Each component in the fog computing architecture generates detailed event records for every significant event. These event records are kept/sent to one or multiple instances of TelcoFog nodes that collate, store, and process the information in a horizontally scalable framework for distributed storage and processing of very large data sets.

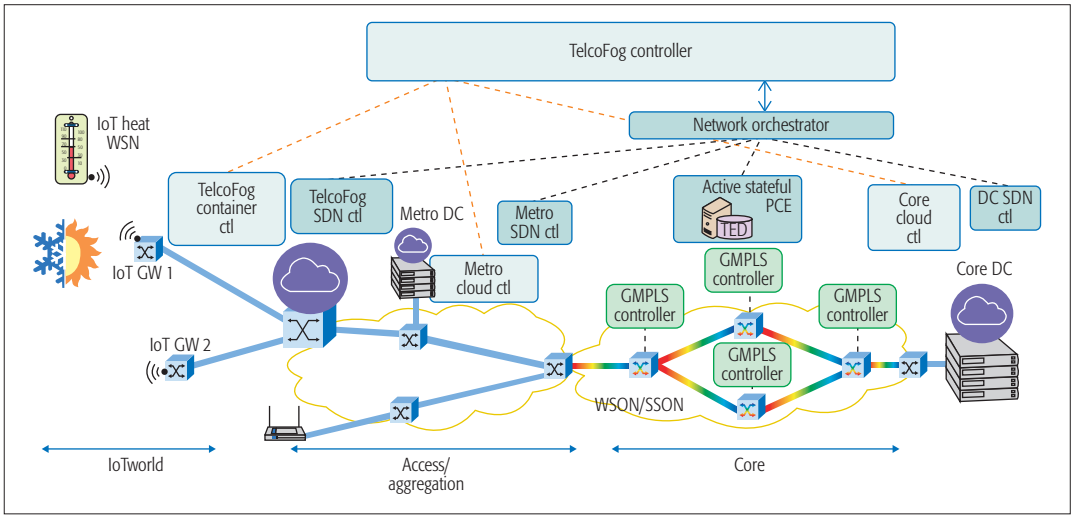


Figure 3. TelcoFog proof of concept scenario.

of the resource consumption and general status of the system. Besides the pure resource management functionalities, it is also very important to manage the deployment of the different services. This is achieved by using a Service Orchestrator, which at the same time is also in charge of guaranteeing that the service is functioning properly. Finally, to control the access to the different resources, and to define the security policies that will be enforced on each fog node, we consider a Security Policies Repository, where the policies are stored and securely pushed to the fog node.

TelcoFog services are modeled using their YANG data models, and they can be deployed on top of the allocated TelcoFog resources reserved for each tenant. The Service Orchestrator is responsible for requesting the necessary resources and deploying the requested services on top of them. It acts as generalized NFV management and orchestration (NFV MANO), while services are generic virtualized functions, which might or not be network related. It is expected to leverage the work done in NFV and align it with MEC servers, while providing access to the data obtained from the smart things and devices.

The TelcoFog Resource Orchestrator is the key element to handle the allocation of TelcoFog resources into the deployed TelcoFog nodes, or in centralized cloud DCs.

As previously explained, resource monitoring is key in providing service assurance, due to the fact that it inspects the provided TelcoFog services in order to anticipate future degradation of the QoE. Finally, data analytics management allows the triggering of a specifically configured set of functionalities for data analysis, and evaluation can be provided to services running on top of allocated virtual resources.

TelcoFog Big Data and Analytics Framework

One of the main objectives of data analytics is knowledge discovery from data (KDD) [13]. To that end, the following steps are performed in an iterative way,

- Data Pre-Processing: Basic operations include data selection (to retrieve data relevant to the KDD task from the database), data cleaning (to remove noise and inconsistent data, handle the missing data fields, etc.), and data integration (to combine data from multiple sources).
- Data Transformation: The goal is to transform data into forms appropriate for the learning and mining task, that is, to find useful features to represent the data. Feature selection and feature transformation are basic operations.
- Data Mining and Machine Learning: This is an essential process where intelligent methods are employed to make predictions and extract patterns (e.g., classification, regression, clustering).
- Pattern Evaluation and Presentation: Basic operations include identifying the truly interesting patterns that represent knowledge in an easy-to-understand fashion.

The TelcoFog allows the KDD process previously described that includes data collection, pre-processing and storage, data transformation, and data mining and presentation so as to offer knowledge as a service to TelcoFog services. The real-time capability will provide mission-critical business intelligence in support of enterprise decision making. Such a framework will allow applications to monitor and manage computation and storage resources, while protecting the privacy and integrity of data.

Each component in the fog computing architecture generates detailed event records for every significant event. These event records are kept/sent to one or multiple instances of TelcoFog nodes that collate, store, and process the information in a horizontally scalable framework for distributed storage and processing of very large data sets. The nodes include mechanisms to automatically trigger the collection of more detailed records when a certain event occurs; the goal is to be able to get to the root cause of any issue without having to reproduce it.

TelcoFog Proof of Concept for IoT Services

The IoTWorld testbed consists of a set of heating, ventilating, and air conditioning (HVAC) modules and actuators. It also includes a wireless sensor network (WSN), which forwards measurements

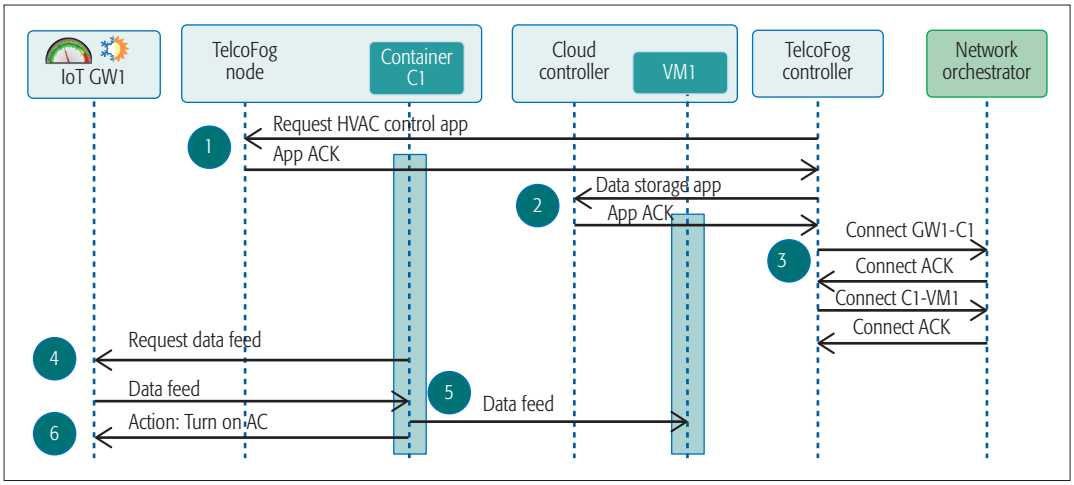


Figure 4. Message Exchange workflow for the deployment and operations of a HVAC application.

The HVAC application is running at the TelcoFog node at the network edge. The location of the application at the network edge improves the latency of the application, and reduces the necessary bandwidth with cloud resources, typically located in distant locations.

of temperature and energy consumption to an IoT gateway. The ADRENALINE testbed is a distributed cloud computing platform across access/aggregation and core networks [14].

In this PoC, shown in Fig. 3, we have deployed an SDN/NFV-enabled TelcoFog node in ADRENALINE, and we have interconnected it to IoT gateways from IoTWorld by means of an end-to-end (E2E) TelcoFog controller [14]. The network orchestrator provides network connectivity between IoT gateways and deployed containers that might be allocated in the proposed TelcoFog node or toward virtual machines which have been allocated in a DC in the core network. The TelcoFog node has been implemented using Docker containers and OpenVSwitch [15]. An agent allows the dynamic creation of containers and their attachment to the underlying virtual switch. Cloud Controller has been implemented using OpenStack Mitaka.

We have defined an HVAC application, which models HVAC services such as temperature control. The HVAC application is responsible for monitoring temperature sensors and uploading the data into a database running on the cloud. If the application detects an increase of temperature, it is able to activate the AC actuator in order to reduce the measured temperature. The YANG model used for the HVAC agent uses three containers to organize the necessary config/status data for temperature, heat, and AC. Temperature allows the monitoring of current temperature in Celsius. Heat and AC might be accessed in order to modify the status of the heat or AC systems (Stop/Run/Error).

The HVAC application runs at the TelcoFog node at the network edge. The location of the application at the network edge improves the latency of the application and reduces the necessary bandwidth with cloud resources, typically located in distant locations.

The TelcoFog Controller is responsible for handling computational and network connectivity requests, which are processed through the Cloud Controller/TelcoFog node and network orchestrator. The Cloud Controller (OpenStack) is accessed through its REST API, while the TelcoFog node and network orchestrator are handled using the YANG-based APIs.

The orchestration process for the deployment of the HVAC application consists of three different steps (steps 1 to 3), and the HVAC operations include steps 4, 5, and 6 (Fig. 4).

Step 0: The TelcoFog controller is requested to deploy an HVAC service, which will be able to control the temperature locally and store the measurements on a cloud-based database.

Step 1: The TelcoFog controller will first request of a fog node the creation of a container (C1) running the HVAC application.

Step 2: Once the container is available, the TelcoFog controller triggers the creation of a database running on a cloud DC (VM1).

Step 3: Once the computational resources have been obtained, the TelcoFog controller requests the connectivity services to the network orchestrator. Connectivity services are requested between the HVAC container and the cloud-based database, as well as between the HVAC container and the IoT gateway (GW1).

Once the HVAC service has been fully deployed, the HVAC enters operation mode.

Step 4: The HVAC application continuously monitors the temperature using a standardized HVAC YANG service.

Step 5: The data is stored toward the database running on the cloud.

Step 6: If a high temperature is detected, a YANG remote procedure call (RPC) will be triggered toward the IoT GW1 in order to turn on the AC.

Figure 5 shows the captured Wireshark traces for the TelcoFog orchestration process for HVAC service deployment, as well as the traces from the operation of the HVAC application. It can be observed that the RESTconf Protocol is usedfor the HVAC, Container, and Connectivity Service YANG data models. These Wireshark traces demonstrate the feasibility of the proposed approach in order to use YANG-based services for both IoT and NFV applications.

Table 1 shows the mean delays for 10 orchestration cycles of the proposed experimental PoC. It can be observed that container deployment delay is two orders of magnitude inferior to virtual machine deployment delay, thus allowing faster service deployment. Connectivity services delay is much influenced by the delay between network

The presented HVAC service has demonstrated the feasibility of the proposed approach of using YANG modeling language for IoT services description, as well as the basic for unifying the NFV and MEC services, allowing telecom operators to reduce their TCO.

1	TELCOFOG_CTL	FOG_NODE_1	HTTP	POST /restconf/config/container/hvac_container/ HTTP1.1 (application/json)
	FOG_NODE_1	TELCOFOG_CTL	HTTP	HTTP/1.0 200 OK (application/json)
2	TELCOFOG_CTL	CLOUD_CTL	HTTP	POST /v2.1/e9102671a6004a209f8ccec14cadf2fd/servers HTTP/1.1 (application/json)
	CLOUD_CTL	TELCOFOG_CTL	HTTP	HTTP/1.1 202 Accepted (application/json)
	TELCOFOG_CTL	CLOUD_CTL	HTTP	GET / v2.1/e9102671a6004a209f8ccec14cadf2fd/servers/45244ef2-8a9a-448b-bd38-62c31f8edd2a HTTP/1.1
	CLOUD_CTL	TELCOFOG_CTL	HTTP	HTTP/1.1 200 OK (application/json)
3	TELCOFOG_CTL	NET_ORCH	HTTP	POST /restconf/config/Context/_connectivityService/gw1_c1/ HTTP/1.1 (application/json)
	NET_ORCH	TELCOFOG_CTL	HTTP	HTTP/1.0 200 OK (application/json)
	TELCOFOG_CTL	NET_ORCH	HTTP	POST /restconf/config/Context/_connectivityService/c1_vm1/ HTTP/1.1 (application/json)
	NET_ORCH	TELCOFOG_CTL	HTTP	HTTP/1.0 200 OK (application/json)
4	HVAC_CONTAINER	IOT_GW1	HTTP	GET /restconf/config/HVAC/Temperature/ HTTP/1.1
	IOT_GW1	HVAC_CONTAINER	HTTP	HTTP/1.0 200 OK (application/json)
5	HVAC_CONTAINER	MYSQL_CLOUD_VM	MySQL	Request Query
	MYSQL_CLOUD_VM	HVAC_CONTAINER	MySQL	Response OK
6	HVAC_CONTAINER	IOT_GW1	HTTP	PUT /restconf/config/HVAC/Ac/ HTTP/1.1 (application/json)
	IOT_GW1	HVAC_CONTAINER	HTTP	HTTP/1.0 200 OK (application/json)

Figure 5. Wireshark capture of the HVAC service deployment and operation.

Container deployment delay	399 ms
Connectivity service setup delay (GW1 – C1)	736 ms
HVAC command delay	186 ms
VM deployment delay	16.17 s
Connectivity service setup delay (C1 – VM1)	2.86 s
Edge orchestration delay	1.32 s
Total orchestration delay	20.35 s

Table 1. Experimental result for TelcoFog orchestration.

elements and network orchestrator, as well as the need for establishment of dynamic optical paths, which significantly increases the setup delay. In case only edge services are deployed, orchestration delay is reduced to 1.32 s.

Conclusions

In this article we have presented a novel architecture for providing unified cloud and fog resources for deploying NFV, MEC, and IoT service on top of a telecom operator's network.

A proof of concept for the TelcoFog architecture has been introduced, which focuses on distributed and programmable fog technologies. TelcoFog, by design, is capable of integrating an ecosystem for network operators willing to provide NFV, MEC, and IoT services.

The presented HVAC service has demonstrated the feasibility of the proposed approach of using YANG modeling language for IoT services description, as well as the basis for unifying the NFV and MEC services, allowing telecom operators to reduce their TCO.

Acknowledgments

This work was partially supported by Spanish MINECO projects DESTELLO (TEC2015-69256-R), SYNERGY (TEC2014-59995-R), CellFive (TEC2014-60130-P), and AGAUR (2014 SGR 1551).

References

[1] F. Bonomi *et al.*, "Fog Computing and Its Role in the Internet of Things," *Proc. MCC Wksp. Mobile Cloud Computing*, 2012, pp. 13–16.
[2] OpenFog Consortium Architecture WG, "OpenFog Architecture Overview," white paper, Feb. 2016.
[3] J. Halpern and C. Pignataro, "Service Function Chaining (SFC) Architecture," IETF RFC 7665, Oct 2015.
[4] R. Vilalta *et al.*, "Transport Network Function Virtualization," *J. Lightwave Technology*, vol. 33, no. 5, Apr. 2015, pp. 1–8.
[5] M. Dallaglio *et al.*, "YANG Model and NETCONF Protocol for Control and Management of Elastic Optical Networks," *OFC*, 2016, pages 1–3.
[6] B. Claise, "YANG as the Data Modeling Language in the IoT Space," *Proc. IoT Semantic Interoperability Wksp.*, 2016; https://www.iab.org/activities/workshops/iotsi/, accessed Feb. 5, 2017.
[7] UNIFY Project, "D5.1: Universal Node Functional Specification and Use Case Requirements on Data Plane," 2014; http://www.fp7-unify.eu/files/fp7-unify-eu-docs/Results/Deliverables/UNIFY-WP5-D5.1-Universal_node_functional_specification.pdf, accessed Dec. 22, 2016.
[8] L. Velasco *et al.*, "Elastic Operations in Federated Datacenters for Performance and Cost Optimization," *Elsevier Computer Commun.*, vol. 50, 2014, pp. 142–51.
[9] L. Velasco *et al.*, "A Service-Oriented Hybrid Access Network and Cloud Architecture," *IEEE Commun. Mag.*, vol. 53, 2015, pp. 159–65.
[10] V. López *et al.*, "Transport API: A Solution for SDN in Carriers Networks," *Proc. 42nd Euro. Conf. Optical Commun.*, Düsseldorf, Germany.
[11] R. Muñoz *et al.*, "Integrated SDN/NFV Management and Orchestration Architecture for Dynamic Deployment of Virtual SDN Control Instances for Virtual Tenant Networks," *J. Optical Commun. Networking*, vol. 7, no. 11, 2015.
[12] "Building Scalable, Sustainable, Smart+Connected Communities with Fog Computing"; http://blogs.cisco.com/innovation/barcelona-fog-computing-poc, 2015, accessed Dec. 22, 2016.
[13] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "From Data Mining to Knowledge Discovery in Databases," *AI Mag.*, 17:3, vol. 37, 1996.
[14] R. Vilalta *et al.*, "End-to-End SDN Orchestration of IoT Services Using an SDN/NFV-Enabled Edge Node," *Proc. OFC*, 20–24 Mar. 2016, Anaheim, CA.
[15] https://github.com/rvilalta/iotworld, accessed Dec. 12, 2016.

Biographies

Ricard Vilalta [SM'17] has a telecommunications engineering degree (2007) and Ph.D. degree (2013) from the Polytechnic University of Catalunya (UPC), Spain. Since 2010, he has been a researcher at CTTC in the Communication Networks Division. He is currently a research associate at the Open Networking Foundation. His research is focused on SDN/NFV, network virtualization, and network orchestration. He has been involved in international, EU, national, and industrial research projects, and published more than 100 journals, conference papers, and invited talks.

Victor López received his M.Sc. from the Universidad de Alcal de Henares in 2005 and his Ph.D. from UAM in 2009. In 2006 he joined the High-Performance Computing and Networking Research Group, UAM. He worked as an assistant professor at UAM. In 2011 he joined Telefonica I+D as a technology specialist. He has co-authored more than 150 publications and contributed to IETF. His research interests include IP/MPLS, optical networks, and control plane (PCE, SDN, GMPLS).

Alessio Giorgetti received his Ph.D. in 2006 from Scuola Superiore Sant'Anna (SSSA). During 2007 he was a visiting scholar at the University of Cambridge, United Kingdom. Since 2011 he hasa been an assistant professor at SSSA. His main research interests include planning, fault tolerance, and GMPLS/PCE control plane for optical networks; SDN control plane for optical and IP/MPLS networks; and industrial Ethernet networks. He is a co-author of two international patents, one IETF RFC, and more than 100 IEEE publications.

Shuping Peng worked as a senior researcher at the Fujitsu Laboratories of Europe — Fujitsu UK. She has been involved in multiple national (U.K.) and international proposals and projects such as 5GPPP Horizon2020 SESAME. Her research interests are 5G,

mobile edge computing/fog computing, NFV, network virtualization, and data cdnters. She has published over 90 technical papers and served as a TPC member and Session Chair for IEEE/ACM/OSA conferences.

VITTORIO ORSINI joined Ericsson through a Managed Service contract signed between Ericsson and H3G Italy in 2005. During 1997–2005 he was head of core network planning and engineering, strongly contributing to the Wind Fixed & 2G mobile services startup in 1998 and H3G Italy 3G service launch in 2003. We was head of network planning on the North West area at Vodafone from 1995 to 1997.

LUIS VELASCO received his degree in telecommunications engineering from UPM in 1989, and his Ph.D. degree from UPC in 2009. In 2004 he joined UPC, where currently he is an associate professor in the Department of Computers Architecture and a senior researcher at the Advanced Broadband Communications Center (CCABA). He has co-authored more than 150 papers in peer-reviewed international journals and conferences. He has participated in various IST FP-6, FP-7, and H2020 European research projects.

RENÉ SERRAL-GRACIÀ received his degree in computer science (2003) and Ph.D. (2009) from the Technical University of Catalunya (UPC). Currently he is associate professor at UPC, where his research is focused on topics such as Internet of Things, Fog Computing, Off-loaded Security, and Software Defined Networks. He has co-authored more than 75 papers in high impact magazines and conferences, while actively participating in european projects such as SECURED (FP7), EuQoS (FP5).

DONAL MORRIS is CEO of RedZinc. He has played a leadership role in the business of packet networks for 16 years, leading development teams and raising development finance. In 2004 he established the Eu QoS consortium for the development of an end-to-end quality of service system across heterogeneous networks. He served as chairman of the EuQoS consortium board (2004–2007). Between 1998 and 2004, he served as CEO of Sherkin Communications.

SILVIA DE FINA received both a Master's degree in telecommunications engineering and a doctorate in information engineering from Sapienza Universita di Roma (1986 and 1992, respectively). Since 2012, she has been head of technology strategy and development at H3G, providing leadership and experience in strategic and operational management of product and process innovation, with focus on the mobile broadband ecosystem.

FILIPPO CUGINI is head of research at CNIT, Pisa, Italy. His main research interests include theoretical and experimental studies in the field of packet and optical communications, including SDN control plane, management and monitoring architecture for optical networks, segment routing, and service chaining. He is a co-author of 15 patents and more than 200 international publications.

PIERO CASTOLDI [SM] has been an associate professor in telecommunications and responsible for the "Networks and Services" area of the TeCIP Institute at SSSA since 2001. His most recent research interests cover optical interconnection networks for data centers, cloud and fog computing, and software defined networks. He is an author of more than 400 technical papers published in international journals and international conference proceedings.

ARTURO MAYORAL graduated in telecommunications engineering by the Universidad Autónoma de Madrid in 2013, and is now a Ph.D. student at UPC. In 2012, he joined Telefonica I+D where he developed his Final Career's Project awarded by the Spanish College of Telecommunications Engineers. He joined CTTC in 2013, where he has participated in several R&D projects (FP7 STRAUSS and H2020 5G-Crosshaul, etc.). His research interests include SDN, NFV, and cloud computing.

RAMON CASELLAS [SM'12] graduated in telecommunications in 1999 from UPC and ENST. He worked as an undergraduate researcher at France Telecom and BT Labs, completed a Ph.D. in 2002, and worked as an associate professor (ENST) until joining CTTC in 2006. He is a senior researcher, involved in research and technology transfer projects. His research interests include network control, GMPLS/PCE, and SDN/NFV. He has co-authored over 150 papers, 4 book chapters, and 4 IETF RFCs.

RICARDO MARTÍNEZ [SM'14] graduated and received a Ph.D. in telecommunications engineering from UPC-BarcelonaTech University in 2002 and 2007, respectively. He has been actively involved in several publicly funded (national and EU) R&D as well as industrial technology transfer projects. Since 2013 he has been a senior researcher in the Communication Networks Division (CND) at CTTC. His research interests include control and network management, protocols, and traffic engineering mechanisms for packet and optical transport networks within aggregation and core segments.

CHRISTOS VERIKOUKIS [S'95, M'04,SM'07] got his Ph.D. from UPC in 2000. He is currently a fellow researcher at CTTC, head of the SMARTECH department, and an adjunct associate professor at the University of Barcelona. He has published 108 journal papers and over 170 conference papers. He is also a co-author of three books, 14 chapters in other books, and two patents. He is the Chair of the IEEE ComSoc CSIM Technical Committee.

RAUL MUÑOZ [SM'12] graduated and received a Ph.D. in telecommunications engineering in 2001 and 2005, respectively, from UPC. He joined CTTC in 2002, where is a senior researcher and head of the Optical Networks and System Department. Since 2000 he has participated in several publicly funded R&D and technology transfer projects. He has led several Spanish R&D projects and the EU-Japan STRAUSS project. His research interests include control and management architectures, protocols, and traffic engineering algorithms for future transport networks.

A Fog Operating System for User-Oriented IoT Services: Challenges and Research Directions

Nakjung Choi, Daewoo Kim, Sung-Ju Lee, and Yung Yi

Fog computing brings computing, storage, and networking even closer to end users and devices for services with better QoS. We introduce FogOS, a fog computing architecture for IoT services. The authors take the perspective of designing an operating system, practicing the architectural lessons from the long history of operating systems.

ABSTRACT

As the proliferation of mobile devices has ignited cloud computing, it is expected that increasing development and deployment of IoT services will expedite the era of fog computing. Fog computing brings computing, storage, and networking even closer to end users and devices for services with better QoS. We introduce FogOS, a fog computing architecture for IoT services. We take the perspective of designing an operating system, practicing the architectural lessons from the long history of operating systems. We focus on addressing the challenges raised by the diversity and heterogeneity of IoT services and edge devices that are owned by individuals and different owners, and presenting how FogOS is designed to effectively and efficiently provide and manage such IoT services. We provide a city-scale surveillance use case to demonstrate FogOS in action.

INTRODUCTION

The Internet of Things (IoT) is no longer a vision, but a reality. We are already witnessing and experiencing many interesting IoT applications. Gartner predicts that about 21 billion "things" across industry sections will be connected to the network by 2020 [1]. These devices generate and transmit data that have diverse requirements in terms of not only volume, but also variety and velocity.

With the ever increasing number of devices and data generated from the edge, the classical cloud-based computing paradigm is faced with challenges, as IDC estimates that the amount of data analyzed on the IoT that are physically at or near the devices is approaching 40 percent [2]. To address these networking and computing trends, *fog computing* brings the cloud closer to the "things" that produce and act on IoT data as depicted in Fig. 1. It is an architectural paradigm that is more appropriate for the fast-growing IoT as it brings computing, storage, and networking closer and faster to the edge devices. We propose Fog Operating System (FogOS), a fog computing architecture for IoT services. We view the whole IoT ecosystem as a computer, and take the perspective of an operating system for our FogOS architecture. The role of traditional operating systems in computers is managing computer hardware and software resources and providing common services for computer programs. FogOS, on the other hand, regards IoT applications (that correspond to programs in OS) as X-as-a-service (X-aaS, e.g., lighting-as-a-service, temperature-sensing-as-a-service) for which common interfaces are provided. The set of resources managed by FogOS include all fog and cloud (e.g., nano/edge cloud) and edge devices (e.g., sensors/actuators). They can also be connected to any level of cloud (e.g., central/regional/metro) when FogOS has an appropriate peering contract.

We particularly consider the case where edge devices are possibly owned by different individuals and providers. Many current IoT devices are deployed by infrastructure providers, but we argue that many more sensors/actuators will be increasingly individually owned and shared in the future when they are appropriately incentivized. In that scenario, there is a complex economic interplay between different players (e.g., IoT users, IoT application providers, infrastructure providers, and edge device owners). Hence, FogOS can function as a distributed operating system that manages the cloud and the resources at the edge, and a platform of incentivizing and connecting individually owned edge devices.[1]

An OS for network resource management, such as Open Network Operating System (ONOS) [3], is a seemingly similar concept to FogOS. For example, ONOS has been proposed as a control platform of software defined networking (SDN) for carrier and cloud provider networks, with scalability, availability, and performance in mind. However, there are two main differences between FogOS and ONOS.

First, ONOS operators directly own and control all network devices that are fixed with relatively stable operating conditions, while FogOS needs to control significantly diverse edge devices that are highly dynamic and owned by different parties. Thus, FogOS needs to play the role of a broker of pooling/slicing edge devices' resources and coordinating all the players with self-interest. Second, ONOS participates in standardizing device interfacing (e.g., OpenFlow [4]). However, in IoT, diversity in devices, services, and protocols is inevitable, resulting in a more challenging environment. A cloud computing OS, such as OpenStack [5], also aims to orchestrate the large-scale computing resources in a shared infrastructure built on top of standard and commodity hardware under the same administrative domain. Hence, FogOS has similar major differences compared to the traditional cloud computing OS.

There are three groups actively designing

[1] Fog: typically means both clouds at edge and user devices in theliterature, but throughout this article, we use the terms "fog cloud" and "edge device."

Digital Object Identifier:
10.1109/MCOM.2017.1600908

Nakjung Choi is with Bell Labs, Nokia; Daewoo Kim, Sung-Ju Lee, and Yung Yi are with KAIST; Yung Yi is the corresponding author.

architectures for fog computing: the Open Fog Consortium [6], the European Telecommunications Standards Institute's (ETSI's) mobile edge computing (MEC) [7], and cloudlets [8], each with slightly different visions and emphasis (see [9] for comparison). We believe that FogOS can be applied to or even merged with any of these architectures, as our focus is on handling the diversity and heterogeneity of user-oriented IoT services and edge devices that are owned by individuals and different owners using fog computing.

Fog Operating System: Architecture

Key Challenges

We describe the challenges of fog computing architecture for highly diverse IoT applications with heterogeneous edge devices owned by different individuals and providers (see Table 1 for a summary and existing solutions).

Scalability: Being at exponential growth, there would be a significant number of IoT devices, which in turn run various IoT applications and generate a sheer amount of data.

Complex Inter-Networking: Due to the large scale and diversity, IoT devices will be physically connected in various forms and under diverse conditions, for example, wireless multihop connectivity using heterogeneous radio access technologies, often with mobility.

Dynamics and Adaptation: With wireless connectivity and mobility, IoT devices experience frequent environmental changes in topology and communication conditions. In addition, IoT applications may have diverse lifetimes and quality of service (QoS) requirements, requiring prompt allocation of edge resources and re-embedding of IoT applications.

Diversity and Heterogeneity: Edge devices have various capabilities in communication radios, sensors, computing powers, storage, and so on. This requires seamless interfacing and interoperability, often incurring non-negligible overhead and yielding implementation/operation complexity.

In FogOS, we tackle the above challenges using a reference architecture. as depicted in Fig. 2, consisting of the following four main components:

- Service and device abstraction
- Resource management
- Application management
- Edge resource: registration, ID/addressing, and control interface

The challenges due to diversity and heterogeneity are resolved by an abstraction layer for services and devices (see the following subsection). The application and resource managers work closely together to provide complex internetworking services and adaptively allocate edge/fog resources to accommodate the dynamics of applications and resources (see "Resource Management" and "Application Management" below). In the "Edge Resource: Registration, Identification, and ControlInterface" section, we describe ways of improving network and service scalability.

Service and Device Abstraction

In the fog computing environment where FogOS operates, there is a common property in IoT applications and edge devices: diversity. This diversity complicates the process of developing an IoT application and the control of edge devices. It is therefore necessary to provide flexible but consistent abstraction as application programming interfaces (APIs), both from FogOS to applications (service abstraction or service API) and from FogOS to edge devices (device API). These APIs are designed and categorized by the degree of generalization and exposure, where generalization refers to how concrete abstraction should be, and exposure deals with how controllable we should make service and device through the designed APIs.

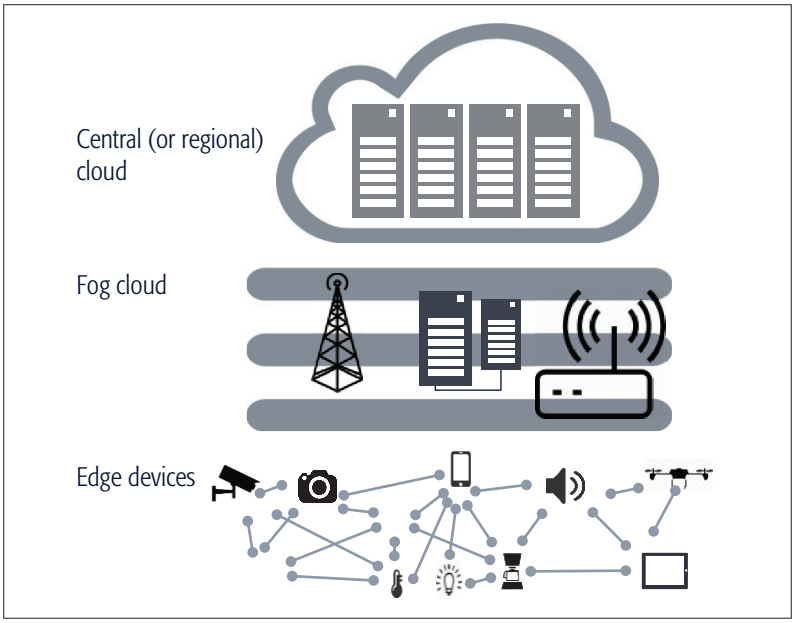


Figure 1. Fog cloud and edge devices.

Service Abstraction

Generalization: In operating systems, users can directly access OS resources by invoking low-level system calls or using a high-level programming language dependent standard library. FogOS defines the following three hierarchical service APIs from low to high level:

- *Level 1:* Resource service API: This API resides at the lowest level, providing services that can control each individual edge device resource such as computing, storage, sensing, actuating, and radio access (or link) to applications. For example, a service call of "read the temperature from sensor X" can be invoked by an application.
- *Level 2:* Network service API: Using a collection of resource service APIs, this API provides the service of creating a networked slice that consists of some set of edge device resources. For example, to create a video surveillance service, a service call of "form a wireless video sensor network with video sensors X, Y, Z and an edge cloud C, where all wireless sensor nodes are connected to C with statistical bandwidth guarantee of 1 Mb/s." Note that there can be a multihop path from X to C, where the resource matching module of the service manager determines the "optimal" path (see "Application Management" later in the article).

Components (FogOS)	Task	Example func. in general OS	Challenges	Existing solutions
Service and device abstraction	Providing a device data model	File as a universal resource identification	Diversity in devices	Device data model in [10, 11]
	Providing service APIs	System calls and standard libraries	Diversity in services	IoT service APIs (e.g., IoBridge, Evrythng)
Resource management	Pooling resources	Distributed system (e.g., Hadoop distributed file system)	Spatially separated resources, heterogeneous devices	Network controller for SDN (e.g., ONOS [3])
	Slicing resources	Virtual memory	Lightweight slicing	Hypervisor for compute resource
Application management	Matching services with resources	CPU scheduling	Adaptation to dynamics environments (e.g., diverse service lifetime, devices' mobility)	Virtual network embedding and adaptation
Edge resource control	Registration and identification	Device manager	Diversity and large scale	AllJoyn and IoTvity's administration system [10, 11]
	Control interface	System bus	Heterogeneous network interfaces	Openflow, CoAP, MQTT

Table 1. Challenges and solutions: fog computing.

- *Level 3:* Application service API: This API is at the highest abstraction and allows application developers to easily create a service that is defined as a typical service a priori. An example could be a call of "create a video surveillance service at hotspots with high-definition TV quality."

Note that there could be more levels in this hierarchy. Application developers are allowed to utilize any level of service APIs with different controllability and programming proficiency.

Exposure: A FogOS designer may choose different exposure degrees even in each service API, based on programming friendliness and security level. For example, a video surveillance service can be created with the service requirement description {3 cameras} or {1 camera near *gps-1*, 2 cameras near *gps-2*} at the level 3 resource API. Also, everything cannot be open to application developers. For example, network link resources in the resource API at level 1 cannot be accessible because arbitrary change of link resources may negatively affect other applications; even the entire resource API at level 1 can be blocked to allow only high-level access.

Device Abstraction

Generalization: UNIX-like operating systems treat everything as a file, for example, /dev/sda1 for a hard disk, /tmp/mongodb-27017.sock for a socket, and /proc filesystem (procfs) for a process or other system information. FogOS could enjoy a similar level of generalization, but has more diversity to interface with various existing and emerging edge devices, which are possibly manufactured by different vendors. To this end, multiple device data models are defined and exposed to FogOS, for example, "sensor device data model," which is different from a single device data model in operating systems (i.e., a file). Note that device data models might have inheritance relation as in the object oriented programming language; for example, a temperature sensor device data model inherits a sensor device data model, or some device data models might be grouped. This generalized abstraction of edge devices enables emerging IoT devices to easily be incorporated without affecting existing applications.

Exposure: Typical OSs provide different control granularity to each managed resource. For example, a default WiFi device driver provides the interface to configure WiFi behaviors. However, a vendor-provided device driver can be activated to expose vendor-specific features with finer control granularity. Similarly, edge devices that are in the same device category might have their own specific features that can be differentiated from other edge devices. Hence, FogOS still requires vendor-specific/owner-specific device drivers to control devices' details or new features, in addition to general and abstract IoT device data model-based control.

Resource Management

FogOS manages the resources of edge devices and fog clouds that are spatially separated and often need to be controlled in a distributed manner. We assume that the list of available resources are registered at the resource management module for the process of edge resource registration. As in traditional OS, FogOS pools or slices the available resources whenever needed, but there are many challenges to be handled, as elaborated next.

Resource Pooling: The concept of resource pooling is used in a variety of contexts across different domains. In this article, we define resource pooling as a mechanism to collect the resources of the same "class." A good example in a general OS is the notion of virtual memory in the hierarchical memory system, which enables the main memory and hard disk to be pooled, transparently seen as runtime storage by running processes.

In fog computing, similar resource pooling would be useful in furnishing IoT applications with larger service options and freedom. The unique challenges of resource pooling in fog computing are:

- Pooling occurs among edge devices that might be placed in spatially different locations.

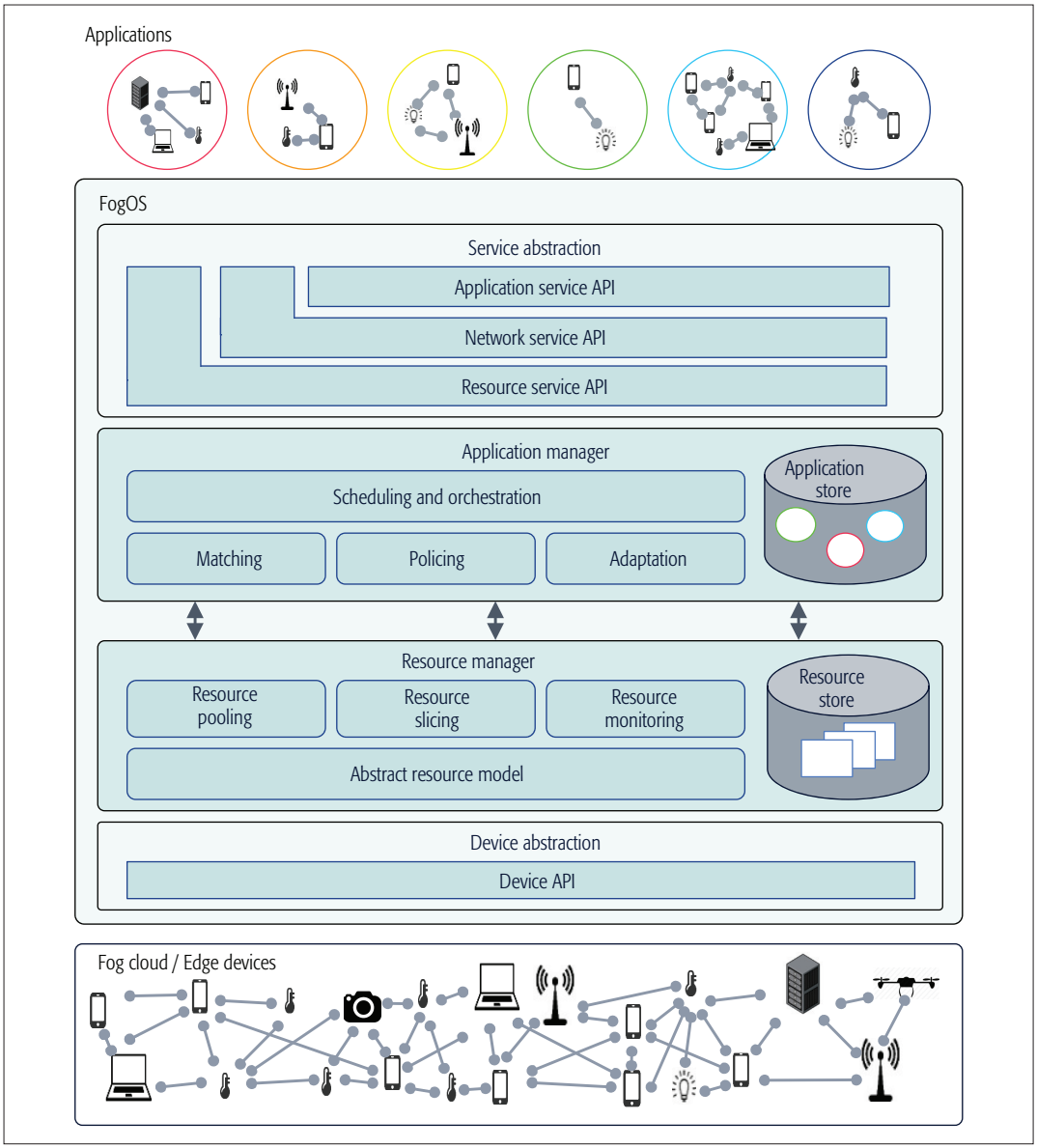


Figure 2. FogOS (Fog Operating System) reference model.

We assume that the list of available resources are registered at the resource management module for the process of edge resource registration. As in traditional OS, FogOS pools or slices the available resources, whenever needed, but there exist many challenges to be handled, as elaborated next.

- The resources to be pooled are highly heterogeneous.
- Limited resources of edge devices often require large-scale pooling.

These unique features act as technical challenges that should be tackled by FogOS. A candidate list of resource pooling is as follows.

Computing/Storage Pooling: The processing power of an edge device is likely limited. For intense data processing that requires fast response, we can use multiple edge devices in a distributed manner. Similarly, limited storage can be compensated by a distributed collection of storage of other devices.

Sensor/Actuator Pooling: Many IoT applications relying on data from sensors might increase information accuracy by exploiting similar data from multiple sensors. Also, different kinds of sensors lead to more complete information on the monitoring status, for example, pooling and fusion of the data from a combination of gyroscopes, magnetometers, and accelerometers. In actuator pooling, a good example is multiple drones flying in a group, performing environmental sensing in a collaborative manner.

Network Link Pooling: IoT applications that generate large data or require low latency need high-speed access links. To that end, an edge device with multiple communication radios can pool them to create a thick communication pipe. Also, a device that is not directly connected to a fog cloud could use other edge nodes as relays.

Resource Slicing: As opposed to resource pooling, resource slicing corresponds to a mechanism that enables sharing of physical resources by multiple IoT applications. For example, in an OS, storage can be sliced through the concept of virtual memory space so that multiple processes can regard the entire (virtual) memory as if it is exclusively allocated to each single process. Multicore CPU allocating each core independently to each process is another example.

Slicing of the resources of edge devices can provide differential granularity and help use the resources efficiently. Sensor/actuator and processing resources can be sliced temporally, and stor-

Different IoT applications need different types and amount of edge resources, depending on their QoS requirements. One of key functions of the application manager is to compute a matching solution from such requirements to the edge resources, where the available resources are obtained by querying to the resource manager.

age resource can be sliced spatially. The network link resource can also be sliced temporally as well as spatially (e.g., subdivision of the communication channel). Synchronization and scheduling among the distributed resources is a key challenge, as poor execution would result in serious resource waste.

Application Management

As the resource manger manages all the edge device resources, the application manager manages everything on the running IoT applications by matching the service requests to the edge resources, monitoring the running application's resource usage status and enforcing service level agreements (SLAs), orchestrating the registered and available edge resources among multiple ones (e.g., prioritization), concurrent applications, and adapting to the changes of edge resource and application status.

Application-Edge Resource Matching: Different IoT applications need different types and amounts of edge resources, depending on their QoS requirements. One of the key functions of the application manager is to compute a matching solution from such requirements to the edge resources, where the available resources are obtained by querying the resource manager. In a typical OS, such a matching is trivial as the device resources are directly controllable and small scale. However, in IoT, there are many and diverse devices, often placed in spatially different locations, requiring networked control. Diversity requires the matching module to match the required resource "optimally" from many candidates. Depending on how effective this matching is, the number of IoT applications that can be accepted and run is determined, which has large impact on the revenue of IoT service providers and other economic players. Theoretical understanding of this matching problem must be made, and practically implementable algorithms with low complexity are of significant importance, which in turn depends on the type of applications provided as IoT application service APIs.

Policing, Scheduling, and Orchestration: Once edge resources are appropriately allocated to incoming IoT applications, the application manager keeps track of their resource usage and monitors whether SLAs are violated. SLA violation of an application might degrade QoS of other applications, for which a certain level of resource partitioning often becomes of some value. The key challenge comes from the large scale of edge devices, where monitoring and policing for each would incur significant overhead even for a small edge device.

Dynamic creation and termination of IoT applications fluctuates available edge resources over time, often leading to the resource competition among them. In addition, each application would be assigned a different priority based on, for instance, security and pricing. All these motivate FogOS to employ a smart scheduler of running applications, similar to the job scheduler of an OS.

Adaptation to Resource and Service Changes: After the applications are matched to a set of edge resources, this matching result might not remain valid due to the change of application status and the change/fault of edge resources. Whenever applications with higher priority arrive or existing applications terminate, the application manager might need to re-match the resource among the running applications for better resource management. This adaptation is also necessary when the edge resource topology changes as edge devices move or experience fault (e.g., battery shortage). In this case, the application manager must support continuous reconfiguration of the application and edge resources in collaboration with the resource manager. However, we must consider the trade-off between operation cost efficiency of reconfiguration and performance.

Edge Resource: Registration, Identification, and Control Interface

Identification and Addressing: In fog computing, high dynamics and diversity of edge networks force FogOS to interact with edge resources frequently to keep an up-to-date snapshot of th resource store of the resource manager (Fig. 2), and pool/negotiate a proper set of resources to embed various IoT applications, where an efficient identification of edge resources via IDing and addressing is essential. We propose to use both syntactic and semantic IDs in FogOS. Syntactic IDs refer to the ones that directly identify the edge resource (e.g., a 5th sensor of room 2 of building 2 of the Korea Advanced Institute of Science and Technology, KAIST), whereas semantic IDs support the context of what a service want to utilize (e.g., any temperature sensor sensing 10°C of room 2 of building 2). Each ID might use a different binding with its network address, for example, static binding for syntactic IDs and dynamic binding for semantic IDs.

One can refer to IoTivity's identification specification [10], AllJoyn [11], geocasting [12], or Named Data Networking (NDN) for IoT [13]. For example, AllJoyn requires each IoT device to know the minimum information (i.e., name) of destinations, and each device can find the destination device with this information by using mDNS (multicast). However, while AllJoyn is suited for a small-scale IoT network, FogOS targets networks with a large number of edge devices with high dynamics and diversity, and hence requires scalable solutions.

Resource Discovery, Registration, and Management: FogOS must discover edge devices and their resources, manage the list, and monitor their status. Two schemes are possible: proactive and reactive. In a proactive scheme, when an edge device enters our FogOS-administered network, it notifies FogOS of its intention to join with its list of available resources. FogOS then updates its resource store database to keep track of this new edge resource. In order to keep the information up to date, the available resource status must be periodically rteported to the resource manager of FogOS. In a reactive scheme, edge resources are queried on demand, whenever new edge resources are needed as new applications are about to be created. Proactive schemes provide faster response to resource lookup and matching for new applications, but at the cost of larger overhead stemming from keeping track of the resource-related information. On the other hand, reactive schemes provide fresher information but

with slower response time. AllJoyn follows this reactive scheme, mainly because it is designed for home-scale one-hop IoT applications. We envision FogOS operating on a larger scale; thus, we believe that a scheme with a certain degree of proactivity is necessary for a possible hybrid approach.

Heterogeneous Control and Network Protocols: As discussed earlier, FogOS uses device APIs to control each individual edge device and fog cloud. We argue that to control fog clouds, the current approach to SDN (i.e., OpenFlow) is a good option. However, to control diverse resource-constrained edge devices, the classical SDN approach might be too heavy and inflexible. Thus, a lightweight version of SDN could be a candidate solution for separating data and control planes. Many of the challenges are due to high heterogeneity in control, communication, and networking protocols of edge devices. The control plane should leverage existing IoT control protocols such as Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT), and also emerging architectures such as information-centric networking (ICN). Similarly, the data plane should support diverse wireless technologies, for example, WiFi, LTE, Low Power WAN (LPWAN) [14], and ZigBee, which is necessary to deliver data as well as control information. There are different proposals for this, where one is to employ a gateway that can understand such heterogeneity, but such an approach of only a single hop at the last mile might restrict the service coverage, and thus limiting the scope of possible IoT applications that FogOS supports. To extend the reach of FogOS, seamless multihop communication over a large-scale wireless nodes would be highly valuable.

FogOS-Driven IoT Ecosystem

In the fog computing market, there are four key economic players that compete and cooperate to increase their revenues. This is depicted in Fig. 3. We do not claim that the ecosystem mentioned in this article is the only one that would emerge. Rather, we believe that it might be one of the most basic and intuitive patterns where players interact.

End Service[2] Users (SUs): These are end users who are ready to enjoy IoT applications. They pay the application service fee to service providers under a variety of tariffs.

Edge Resource Owners (EROs): These are individuals or large companies (e.g., mobile network operators that have large-scale communication and sensor infrastructures) who own edge resources or fog clouds. In particular, individual edge resource owners share their resources and partially or entirely sell the resources to an infrastructure provider (InP). They act similarly to Uber drivers. They need to be appropriately incentivized to share the resources, where the incentive mechanism would be given by InPs.

Service Providers (SPs): SPs create diverse IoT applications that attract SUs as over-the-top (OTT) providers. Logically, they do not own the resources of fog clouds or edge devices, but rent them. Thus, they make a contract with InPs that manage the edge resources. Note that it is possible that SPs and InPs are run by a single company. Application development is made based on the service APIs opened by FogOS.

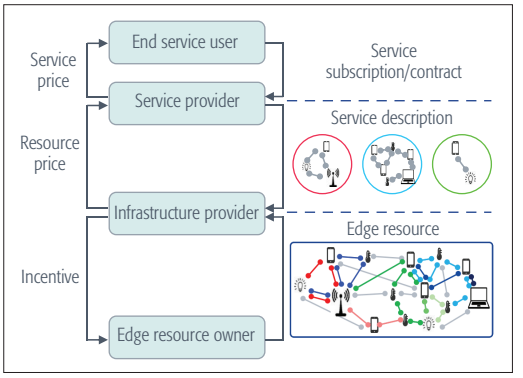


Figure 3. Major economic players in fog computing and their interaction patterns.

Infrastructure Providers: They are the ones who run FogOS. InPs have infrastructure of edge devices and fog clouds, and might rely on individual EROs for a large portion of IoT infrastructure. They are required to develop a nice incentive mechanism to attract as many EROs as possible at low cost. Their resources interface with FogOS via device APIs, and they sell their owned and leased resources to SPs. They make profit through business with SPs and EROs.

Note that this market is open to many diverse competition and cooperation scenarios. Edge device owners may act selfishly to maximize their individual revenue, or cooperate with InPs under fair revenue sharing mechanisms. As mentioned earlier, some big player might behave as multiple players. For example, an InP such as a mobile network operator that already has a large-scale cellular and WiFi infrastructure minimally relies on edge device owners by deploying city-scale or even nation-wide sensor/actuator platforms; in such cases, big players are highly likely to provide IoT applications as well to make a large profit from the IoT industry. Non-cooperative and cooperative game theory helps understand the complex interplay in this market and predict the business landscape.

Use Case and Demonstrator: City-Scale Surveillance Service

We now present the use case of FogOS, a large-scale surveillance service, where Fig. 4 shows our preliminary proof-of-concept implementation of FogOS for a drone-based surveillance service.

Scenario Overview

This is an example of sensing-as-a-service that deploys city-scale surveillance, originally starting with a set of sensing of some target regions, and extends to the service coverage change with drone-driven moving sensors. In this case, an SP can be an IoT sensor service provider, and SUs may include a public safety agency.

Original Service:

- An SP requests a surveillance service to an InP (running FogOS) with a service requirement description {*K* regions, *M* videos, *N* audios, *P* sensors} through a level 3 applica-

Proactive schemes provide faster response to resource look-up and matching for new applications, but at the cost of larger overhead stemming from keeping track of the resource-related information. On the other hand, reactive schemes provide fresher information but with slower response time.

[2] In earlier sections, we used the term "IoT applications" rather than "IoT service" as "service" is also used as the service provided by FogOS to applications. However, in this section, we use service to mean IoT application service, unless otherwise noted.

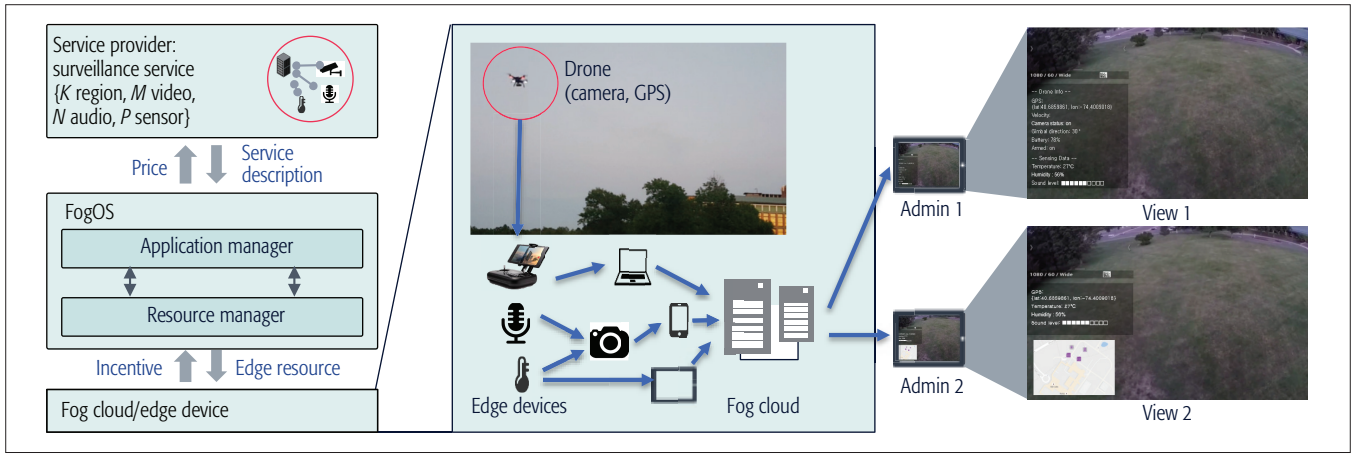


Figure 4. Example implementation of surveillance service on FogOS: extension of drone-based moving video sensing.

tion service API.

- FogOS searches available edge resources owned by itself as well as those owned by EROs (possibly with different priorities), and let the application manager allocate the required resources to embed this application (i.e., matching). These resources might be ready in advance through a proactive resource discovery mechanism, or be searched through a reactive mechanism as discussed earlier.
- The application manager's matching algorithm produces an embedding solution, allocates the computed resource by communicating with the resource manager to retrieve existing/available fog/edge resource information, and commands the resource manager to perform the allocation action.
- SUs enjoy this surveillance service.
- The resource manager periodically monitors the resource usage at associated edge devices, and collaborates with the service manager whenever there is any change or fault of the existing edge resources.

Service Extension

- The SP intends to observe more details of a specific region, say *R* due to an expected crime, for instance. It requests to add a drone-based video sensing of region *R* with the modified service description {region *R*, 1 video sensing with drone, `AVAILABLE` sensors through level 1 and 2 resource and network service APIs. This service corresponds to live video streaming at the edge cloud in region *R* to a single or multiple SUs.
- FogOS searches its resource pool, and finds a fog cloud as well as a group of WiFi APs by the InP, but failed to find a drone. It broadcasts a request to find a drone with a video sensor to the EROs in *R*.
- The video scenes captured by drones and sensing data from the original service reach the allocated fog cloud in region R, which performs augmented reality (AR) functions to generate a richer content of the scene view. This post-processed video stream is delivered to multiple SUs.

Proof-of-Concept Implementation of FogOS

To see the feasibility of FogOS, we implement a prototype, where FogOS plays the following two roles: controller and platform for IoT ecosystem. In our implementation, the economic interaction between key players is simplified, that is, when EROs register their resources to FogOS, EROs' resources are shared through InP. In this article, we mainly focus on the control function of FogOS, as follows:

- Drones and sensors are controlled by an application running on the FogOS through service and device abstraction layers. Thus, we are able to control flying drones and SDN IoT sensors through FogOS.
- Computing, sensing, and networking resources are pooled together and matched to this service by the resource and service managers of FogOS.
- A video from drones and sensing data is processed/merged by the allocated computing resources, and then multiple views for different SUs are created, as shown in Fig. 4.

Conclusion

We introduce a fog computing and networking architecture for IoT services, termed FogOS, practicing architectural lessons from operating systems. FogOS is composed of four major components: service/resource abstraction, resource manager, application manager, and edge resource identification/registration, whose challenges and main research directions are discussed. We hope that our vision in FogOS will be shared by other groups in academia and industry working on IoT and fog computing, and more constructive discussions will continue to follow, inspired by FogOS. These future directions include the extension of FogOS to support the key scenarios in the fifth generation, that is, enhanced mobile broadband, ultra-reliable and low-latency communications, and massive machine type communications.

Acknowledgment

This work was partially supported by the Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.B0717-17-0034,Versatile Network System Architecture for Multi-Dimensional Diversity).

References

[1] Gartner, "Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent from 2015"; http://www.gartner.com/newsroom/id/3165317, accessed 4 May 2017.
[2] V. Turner *et al.*, "IDC FutureScape: Worldwide Internet of Things 2015 Predictions," Int'l. Data Corp., 2014.
[3] ON.LAB. "ONOS — A New Carrier-Grade SDN Network Operating System Designed for High Availability, Performance, Scale-out"; http://onosproject.org, accessed 4 May 2017.
[4] ONF, OpenFlow Switch Specificatio, v. 1.5.1, 2015.
[5] "OpenStack: Open Source Software for Creating Private and Public Clouds"; https://www.openstack.org/, accessed 4 May 2017.
[6] Open Fog Consortium; https://www.openfog consortium.org/, accessed 4 May 2017.
[7] M. Patel *et al.*, "Mobile-Edge Computing Introductory Technical White Paper," MEC Industry Initiative, 2014.
[8] M. Satyanarayanan *et al.*, "Cloudlets: At the Leading Edge Of Mobile-Cloud Convergence," *Proc. IEEE Mobile Computing, Applications and Services*, 2014.
[9] G. I. Klas, "Fog Computing and Mobile Edge Cloud Gain Momentum Open Fog Consortium, ETSI MEC and Cloudlets," 2015.
[10] OCF, "OIC Core Candidate Specification," 2016.
[11] A. Alliance, "AllJoyn Framework," 2016; https://allseenalliance.org/framework, accessed 4 May 2017.
[12] Y.-B. Ko and N. H. Vaidya, "Geotora: A Protocol for Geocasting in Mobile Ad Hoc Networks," *Proc. IEEE Int'l. Conf. Network Protocols*, 2000.
[13] E. Baccelli *et al.*, "Information Centric Networking in the IoT: Experiments with NDN in the Wild," *Proc. ACM Information-Centric Networking*, 2014.
[14] Nokia Networks, "LTE-M - Optimizing LTE for the Internet of Things," white paper, Aug. 2015.

Biographies

NAKJUNG CHOI (nakjung.choi@nokia-bell-labs.com) is a member of technical staff at Nokia Bell Labs, Murray Hill, New Jersey, since April 2010. He received his B.S. (magna cum laude) and Ph.D. at the School of Computer Science and Engineering, Seoul National University in 2002 and 2009, respectively. Also, he has received several awards such as Best Paper Awards and Awards of Excellence. His research is focused on SDN/NFV/cloud, 4G/5G/IoT, and future converged services.

DAEWOO KIM (daewookim@kaist.ac.kr) received his B.S. from the Department of Electrical Engineering, Yonsei University, South Korea, in 2013. He is a doctoral student at the School of Electrical Engineering, KAIST, since 2013. His research interests include sensor networks, network economics, fog computing, and machine learning in networking.

SUNG-JU LEE (profsj@kaist.ac.kr) is an associate professor and KAIST Endowed Chair Professor at KAIST. He received his Ph.D. in computer science from the University of California, Los Angeles in 2000, and spent 15 years in the industry in Silicon Valley before joining KAIST. His research interests include computer networks, mobile computing, network security, and HCI. He is the winner of the HP CEO Innovation Award, the Best Paper Award at IEEE ICDCS 2016, and the Test-of-Time Paper Award at ACM WINTECH 2016.

YUNG YI (yiyung@kaist.ac.kr) is an associate professor at the Department of Electrical Engineering at KAIST. He received his Ph.D. from the Department of Electrical and Computer Engineering, University of Texas at Austin in 2006. His research interests include computer networks and machine learning. He received the best paper awards at IEEE SECON and ACM Mobihoc in 2013, and he was the winner of the IEEE William R. Bennet Prize in 2016.

A Hierarchical Game Framework for Resource Management in Fog Computing

Huaqing Zhang, Yanru Zhang, Yunan Gu, Dusit Niyato, and Zhu Han

The authors propose a three-layer hierarchical game framework to solve the challenges in fog computing networks. In the proposed framework, they apply the Stackelberg sub-game for the interaction between DSOs and ADSSs, moral hazard modeling for the interaction between DSOs and FNs, and the student project allocation matching sub-game for the interaction between FNs and ADSSs.

ABSTRACT

Supporting real-time and mobile data services, fog computing has been considered as a promising technology to overcome long and unpredicted delay in cloud computing. However, as resources in FNs are owned by independent users or infrastructure providers, the ADSSs cannot connect and access data services from the FNs directly, but can only request data service from the DSOs in the cloud. Accordingly, in fog computing, the DSOs are required to communicate with FNs and allocate resources from the FNs to the ADSSs. The DSOs provide virtualized data services to the ADSSs, and the FNs, motivated by the DSOs, provide data services in the physical network. Nevertheless, with fog computing added as the intermediate layer between the cloud and users, there are challenges such as the resource allocation in the virtualized network between the DSOs and ADSSs, the asymmetric information problem between DSOs and ADSSs, and the resource matching from the FNs to the ADSSs in the physical network. In this article, we propose a three-layer hierarchical game framework to solve the challenges in fog computing networks. In the proposed framework, we apply the Stackelberg sub-game for the interaction between DSOs and ADSSs, moral hazard modeling for the interaction between DSOs and FNs, and the student project allocation matching sub-game for the interaction between FNs and ADSSs. The purpose is to obtain stable and optimal utilities for each DSO, FN, and ADSS in a distributed fashion.

INTRODUCTION

Ever since the digital revolution half a century ago, the scale of digital data has grown exponentially. Nowadays, with the high demand of data storage and computing requests, various data services and applications have been proposed to facilitate businesses and our daily lives. However, the traditional rigid deployment of data centers by data service operators (DSOs) is unable to fulfill the requirements of various data services and applications. To improve the flexibility and efficiency of resource allocation, the concept of cloud computing is advocated, where all the resources can be organized as a sharing pool, and authorized data service subscribers (ADSSs) can access the resource pool on demand.

Nevertheless, for some emerging data services and applications, such as vehicle-to-vehicle communication, augmented reality, and smart grid, not only the volume of resources, but the service delay and delay jitter determine the quality of service (QoS) [1]. Moreover, most resources in cloud are physically located far from ADSSs, failing to support the requirements of mobility and real-time interactions during the data services. Accordingly, in order to improve QoS for ADSSs, it is necessary to pull the computing resources closer to ADSSs [2].

In 2014, the idea of fog computing was first proposed by Cisco [3]. Fog computing, similar to cloudlet edge computing proposed by other companies, is composed of geo-distributed fog nodes (FNs), which can be any fixed or mobile collaborative devices with built-in data storage, computing, and communication devices. Benefiting from small scale, low cost, and mobility, the FNs located around ADSSs are able to offload data traffic from the cloud, reduce the communication cost in the networks, and provide real-time, location-aware data services [4].

For the system architecture shown in Fig. 1, there are multiple DSOs serving multiple ADSSs at the same time. In order to improve QoS of the ADSSs, fog computing is introduced in addition to cloud computing. However, as the resources in FNs are owned by independent users or infrastructure providers (InPs), the ADSSs cannot connect to and access data services from the FNs directly. Currently, the ADSSs can only request data service from the data service operators (DSOs) in the cloud, such as Amazon S3, Google Cloud, and IBM Cloud. Therefore, the DSOs are required to communicate with the FNs and allocate resources from the FNs to the ADSSs. Accordingly, in fog computing, the DSOs provide virtualized data services to the ADSSs, and the FNs, after the communication with the DSOs, provide data services in the physical network [5].

With the introduction of fog computing, the resource allocation problem becomes complicated and challenging since there are multiple distributed and autonomous entities in the network. In order to solve the problem, various optimization methods have been adopted in the literature. In [6], the joint radio and computing resource allocation in fog computing was studied by solving the formulated optimization problem in a dis-

Digital Object Identifier:
10.1109/MCOM.2017.1600896

Huaqing Zhang and Zhu Han are with the University of Houston; Yanru Zhang is with the Chinese University of Hong Kong; Yunan Gu is with Huawei; Dusit Niyato is with Nanyang Technological University.

tributed fashion. Furthermore, being aware of the ADSSs' locations with fog computing, dynamic adaptation of computing resources was proposed by [7].

However, the fog computing architecture considered in prior work is based on a single DSO scenario, which simplifies the system architecture and lacks generality. Following the sequential decision making behaviors for the DSOs, FNs, and ADSSs, we propose a three-layer hierarchical game framework with the following three sub-games:

- We first introduce the Stackelberg sub-game for the interaction between the DSOs and the ADSSs to solve the virtualized resource allocation problem. The key problem is the pricing mechanism.
- Then, according to the amount of requested virtualized resources, in order to motivate the FNs to offer the optimal amount of virtualized resources, the moral hazard model in contract theory is utilized to model the interaction between the DSOs and the FNs. The key problem is the incentive mechanism design between the DSOs and the FNs.
- Based on the physical resources offered and virtualized resources provided, the student project allocation matching sub-game from matching theory is adopted to achieve a stable resource allocation solution. The key problem is resource matching in a distributed way that is combinatorial in nature.

The rest of this work is organized as follows. In the following section, we discuss the challenges in fog computing. Based on the challenges, we propose a hierarchical game framework to model the three-layer architecture, where the interactions between different parties, which are the FNs and ADSSs, the DSOs and ADSSs, and the DSOs and ADSSs are then analyzed. Finally, the article is concluded.

Resource Allocation Challenges in Fog Computing

In cloud computing, only DSOs and ADSSs exist in the network. Thus, the resource allocation problem between the DSOs and ADSSs is a straight two-layer structure, where there is a market for all DSOs to compete for ADSSs. In [8], the authors introduced an in-depth game theoretic study of the market and provided pricing strategies for DSOs to achieve Nash equilibrium solutions. However, when the intermediate fog layer is introduced, the relation among DSOs, FNs, and ADSSs becomes complicated. In this section, based on the general system shown in Fig. 1, we classify and discuss challenges of resource allocation in fog computing.

The Interactions between DSOs and ADSSs

The interaction between DSOs and ADSSs in fog computing is similar to the interaction in cloud computing. When there is one DSO serving ADSSs in the network, the DSO is able to adjust its price to motivate all ADSSs to purchase its virtualized resources. In fact, there is a trade-off when the DSO sets the price. On one hand, if the DSO sets a high price, the DSO is able to receive high revenue from the unit amount of resource, while the ADSSs may choose to purchase less resources considering the high unit price. On the other hand, if the DSO sets low prices, although a large amount of resources are purchased by ADSSs, the revenue gained from the ADSSs may decrease.

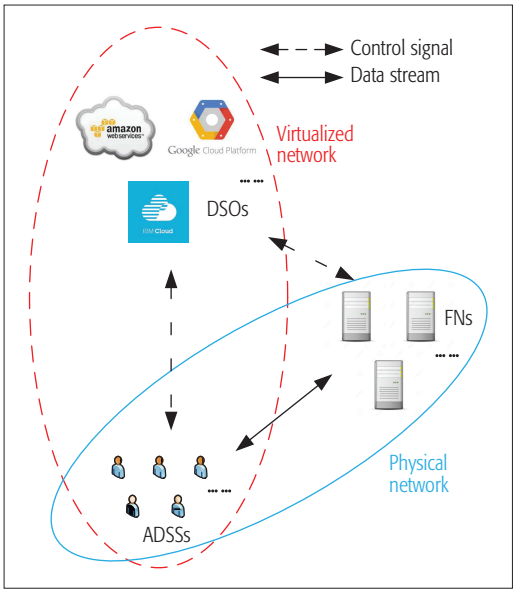


Figure 1. System architecture.

When there are multiple DSOs serving at the same time, competition among DSOs exists in the fog computing market. Thus, there is also a trade-off when DSOs compete for the ADSSs. On one hand, if one DSO increases its price, the revenue from serving one single ADSS may increase, while the ADSS may refuse its service and switch to other DSOs with lower prices. On the other hand, if one DSO reduces the price, more ADSSs will be attracted, but the revenue received from each ADSS decreases. Therefore, it is important for each DSO to set an optimal service price to achieve the highest total revenue.

The Interactions between DSOs and FNs

As most of the FNs are deployed and maintained by private users or independent InPs, the FNs will not directly provide services to ADSSs to help relieve the computation load at DSOs. Therefore, the DSOs need to motivate the FNs to help serve the ADSSs by paying a certain amount of monetary rewards to the FNs. The DSO aims to maximize its revenue by purchasing the exact amount of computing resources needed by the FNs. On one hand, if not enough resources are purchased, even though less payment is required, such insufficient resources will cause poor QoS to ADSSs and result in poor revenue in the future. On the other hand, if physical resources are over-supplied, even though high QoS will attract more ADSSs, the high payment will decrease the DSO's revenue. Thus, it is challenging for the DSO to determine an optimal amount of resources to purchase from each FN. In order to maximize the revenue while minimizing the payment, each DSO needs to design an efficient incentive mechanism so that the DSO's objective revenue maximization can be achieved, and the FNs still have the incentive to participate in such an activity.

As most of the FNs are deployed and maintained by private users or independent InPs, the FNs will not directly provide services to ADSSs to help relieve the computation load at DSOs. Therefore, the DSOs need to motivate the FNs to help serve the ADSSs by paying a certain amount of monetary rewards to the FNs.

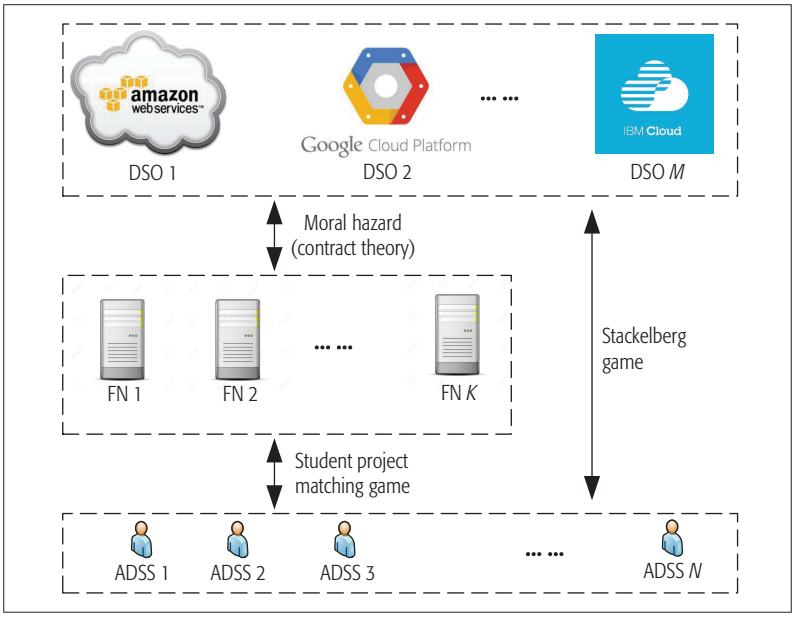


Figure 2. Hierarchical game framework.

The Interactions between FNs and ADSSs

When the ADSSs have determined the amount of virtualized resources needed to purchase, and the FNs have been motivated to supply physical resources, the next step is to efficiently map the physical resources offered by the FNs to the virtualized resources required by the ADSSs. Since the FNs compete with each other for serving ADSSs, and the ADSSs compete with each other for better services. The ultimate goal is to find an optimal matching between the physical resources offered by the FNs and the virtualized resources requested by the ADSSs so that the network can achieve maximum efficiency. Given the large numbers of ADSSs and FNs, the optimal mapping will be hard to solve, or even unsolvable using traditional centralized methods. It is essential to find a sub-optimal stable mapping by a distributed method so that the computation complexity can be reduced, and none of the FNs or ADSSs can deviate from its current mapping to achieve a higher revenue.

The Hierarchical Game Framework

Considering the aforementioned challenges of resource allocation in fog computing, each DSO, FN, or ADSS can be regarded as a rational individual that aims to maximize its own revenue based on the behaviors of all other DSOs, FNs, and ADSSs. Therefore, game theory can be adopted as a suitable mathematical tool to analyze the competition and coordination among all DSOs, FNs, and ADSSs [9, 10].

In fog computing, all DSOs, FNs, and ADSSs form a three-layer architecture and make decisions sequentially. Thus, we model the network as a hierarchical game as shown in Fig. 2, which consists of three sub-games corresponding to the interactions between DSOs and ADSSs, between DSOs and FNs, and between FNs and ADSSs in a sequential manner.

In the following, adopting the backward induction, we sequentially analyze the interactions between different parties, which are the FNs and ADSSs, the DSOs and FNs, and the DSOs and ADSSs, so as to obtain optimal strategies for the DSOs, FNs, and ADSSs with stable and optimal payoffs.

Student Project Allocation Matching Game Analysis for the Interactions between FNs and ADSSs

In this step, we suppose the initial values of the offered resource from each FN and requested resources from each ADSS are given. We consider the resource to be composed of both computation/storage resources and radio resources from different FNs, which are combined as a resource pair and mapped to requested ADSSs.

The mapping between the resource pairs from FNs and ADSSs can be suitably modeled as a student project allocation problem [11], which is a many-to-many stable matching problem and can be described as follows. In many departments of universities, students are required to undertake a series of projects from classes or research by lecturers. The students have preferences among the offered projects. Considering the purpose of training students, for different projects, the lecturers may have preferences over (student, project) pairs according to their suitability. In addition, not only each lecturer but also each project has restrictions on the maximum number of students to accommodate, which are called their capacities. In order to find a stable matching between the students and projects, the SPA-(S,P) algorithm can be utilized.

In this article, we assume the DSOs, resource pairs, and ADSSs act as lecturers, projects, and students, respectively. The preference list of each ADSS is built based on the total revenues gained from the data transmission minus the penalty of service latency as well as the payment to the DSO for the services. On the other hand, the preference list of the DSOs is the mandatory revenue collected from the ADSS minus the cost of service delay using a certain resource pair. If the ADSS requires high QoS, the ADSSs are willing to offer high payment for better resources. At the same time, the DSOs give higher priorities to those ADSSs that offer higher prices by allocating better resources for them. Thus, each DSO establishes its preference list as the ratio of price collected from an ADSS over its service delay.

With the preference lists set up, the SPA-(S,P) algorithm can be adopted to find a stable matching between FNs and ADSSs [12]. In the algorithm, ADSSs first propose to their currently most preferred resource pair in their preference lists. For each resource pair, if the requested proposal from the ADSSs exceeds its capacity, the DSO will find the worst combination of FNs and ADSSs in its preference list and reject this ADSS. Receiving the rejected notification, the ADSS will continue to engage with the next favorite resource pair in its preference list. The procedure terminates when all ADSSs are either matched with a resource pair or have proposed to every resource pair in their preference lists. By the sequential proposing and rejecting actions of ADSSs and DSOs, the convergence of the algorithm is guaranteed, and a stable matching result exists.

In Fig. 3, we evaluate the performance of transmission delay with the proposed SPA-(S,P)

algorithm. When the number of ADSSs increases, due to the limited amount of computing resource blocks (CRBs), the ratio of ADSSs satisfying delay requirement generally decreases. However, compared to the random matching result, the algorithm that matches SPA-(S,P) is able to maintain the high ratio, where most of the ADSSs are able to achieve low transmission delay and high utility.

Moral Hazard Game Analysis for the Interactions between DSOs and FNs

According to the possible matching results between the physical resources provided by FNs and the virtualized resource requested by the ADSSs, given the total amount of virtualized resource, each DSO is required to consider the motivation strategy for each FN to provide the optimal amount of physical resource and achieve a high utility.

The motivation problem from DSOs to FNs can be modeled as a moral hazard in contract theory [13]. The problem arises when both parties have incomplete information about each other. For example, the employees' actions are hidden from the employers [14]. As the DSOs do not know the resource usage information within different FNs, if one DSO offloads its data services to FNs with limited available resource, the ADSSs will suffer poor QoS and will switch to other DSOs. Therefore, such an asymmetric information situation between DSOs and FNs will severely reduce the utility of both DSOs and ADSSs.

In order to avoid such a situation, considering the amount of physical resource provided from one FN to one DSO and the payment from the DSO to the FN, we propose a resource-payment bundle in the contract between DSOs and FNs. In order to motivate the FNs to provide larger amounts of physical resource, the DSO is required to pay more to the FNs correspondingly. Furthermore, according to different requirements of its serving ADSSs and different transmission delay between the FN and serving ADSSs, the relations between the amount of provided physical resource and the payment for different DSO and FN pairs may be different.

In [14], we evaluate the motivation strategy from each DSO to FN with contract theory. In order to motivate FNs to serve ADSSs, when one FN agrees to provide resources for ADSSs, the DSO will pay a fixed amount of money to the FN. Furthermore, if the ADSS is able to provide more resource to improve the QoS of the ADSSs during the service, the DSO will offer an additional bonus. Accordingly, the rent from each DSO to FN can be defined as a combination of the fixed payment plus bonus for providing ADSSs with higher QoS. The utility of each FN is the total rent paid by the DSOs minus the operation and measurement costs. The utility of each DSO is denoted as the revenues from ADSSs minus the rent to FNs. Aiming to maximize the utility of each DSO based on the selfish behaviors of FNs, we obtain the optimal value of rent for each FN in a contract.

In the simulation, we compare our proposed payment plan with four other plans. In the single bonus plan, we assume each FN can offer at most one CRB to the DSO. In the stochastic independent plan, we assume the measurement error from the DSOs to all FNs is zero. For the technologically independent plan, we consider the cost for adopting each CRB within each FN is independent of each other. The independent plan combines both stochastic independent and technologically independent plans. As shown in Fig. 4, when the cost coefficients of CRB within FNs increase, as the DSO is required to pay more to motivate FNs, the utility of the DSO generally decreases for all plans. Moreover, with the amount of asymmetric information between DSOs and FNs increasing, the utility of DSO decreases. Thus, the utility of the DSO in the independent payment plan is the highest, followed by the utilities in the stochastic independent plan, technologically independent plan, and our proposed plan. The single bonus plan has the lowest utility due to the limited amount of offered CRBs in each FN.

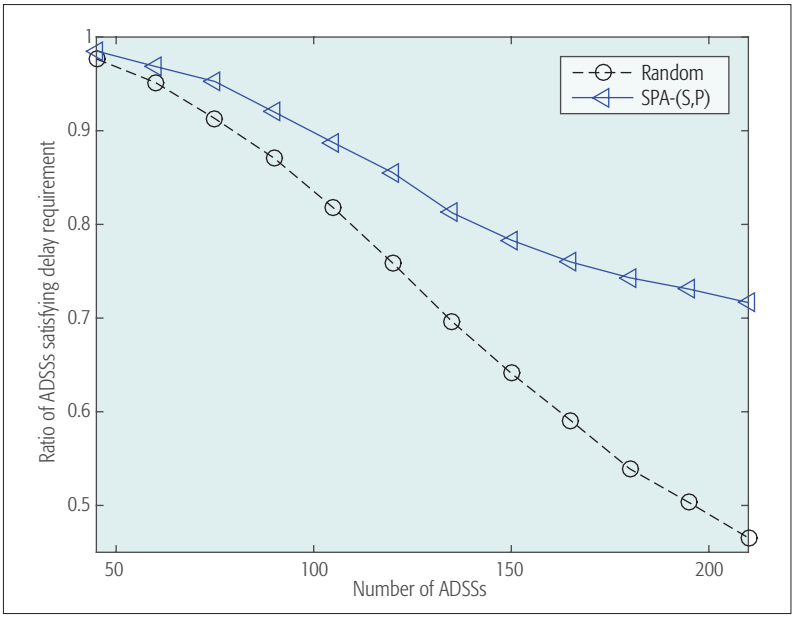


Figure 3. The performance evaluation of SPA-(S,P).

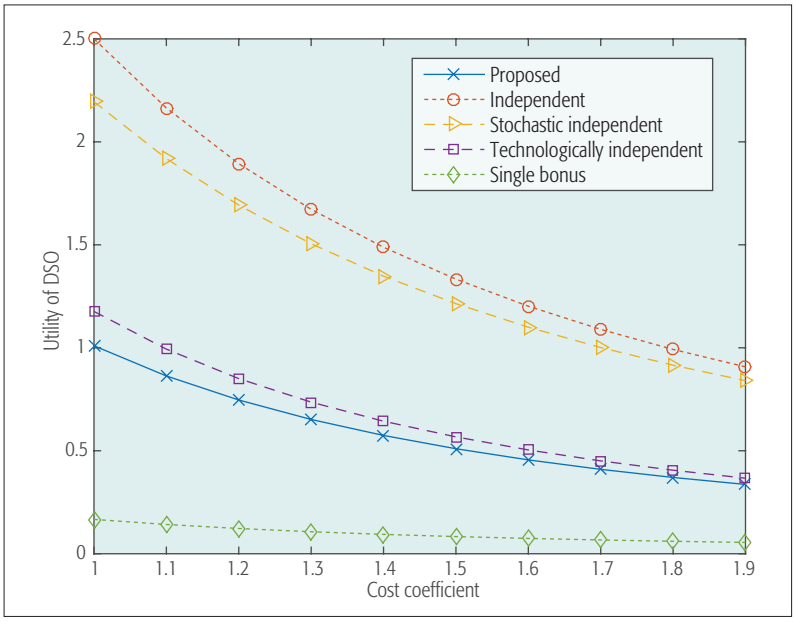


Figure 4. The performance in moral hazard between DSOs and FNs.

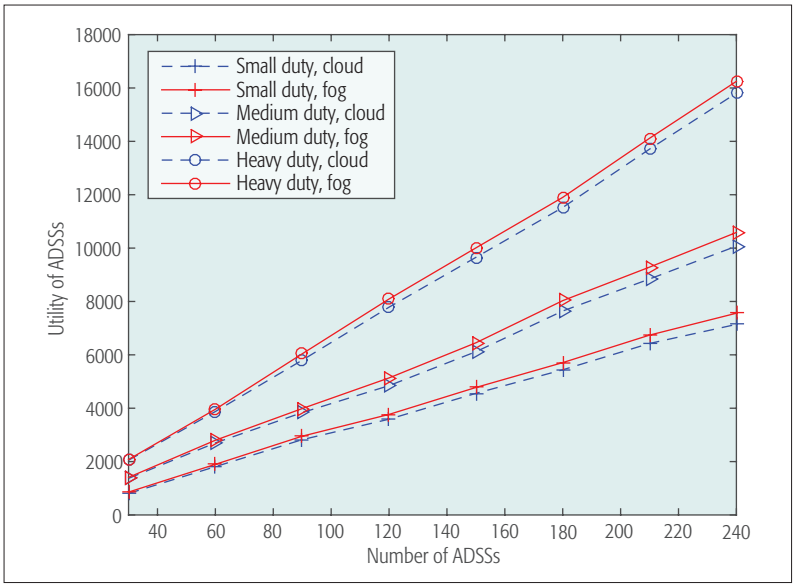


Figure 5. The utility of all ADSSs vs. the number of ADSSs.

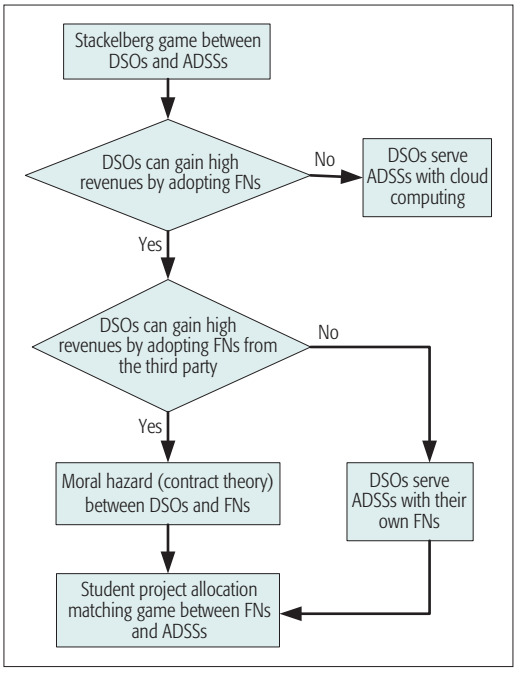


Figure 6. The flowchart for the three-layer hierarchical game.

Stackelberg Game Analysis for the Interactions between DSOs and ADSSs

Predicting the payment for motivating the FNs and the matching results between the provided physical resources and the requested virtualized resource, each DSO determines its optimal service price charging to its serving ADSSs.

As in the virtualized data market, all DSOs first announce their prices for their virtualized services. Based on the announced prices, each ADSS chooses its preferred DSO and determines the optimal amount of resources to purchase. The interaction between DSOs and ADSSs can be modeled as a Stackelberg game, where the DSOs act as the leaders, and the ADSSs act as the followers. In the game, because of the first-mover advantage, each DSO is able to predict the reactions of its serving ADSSs and determine its optimal price for the highest utility. Thus, the Stackelberg equilibrium exists between DSOs and ADSSs [5, 15].

Moreover, the competition also exists among DSOs. If one DSO sets its price too high, the ADSSs may switch to other DSOs for high utility. Therefore, there is also a non-cooperative game among all DSOs. In order to attract more ADSSs and maintain high utility for each DSO, following the proposals in [5], a sub-gradient algorithm can be adopted. In the algorithm, each DSO does not know the existence of other DSOs at the beginning and sets its initial service price at a high value. Then each DSO predicts the utility that it can achieve by adjusting its price with a small value $\pm\Delta$. If adjusting the price is able to improve the utility, the DSO will follow the adjustment in the next round. Otherwise, in the next round, the DSO keeps the current price unchanged. The game continues with reduced value of Δ until no DSO is able to adjust prices to achieve a higher utility.

According to the proposed hierarchical game framework, we evaluate the performances of ADSSs in fog computing, given the cost of motivating the FNs and the matching results between FNs and ADSSs. As shown in Fig. 5 [15], with the number of ADSSs increasing, regardless of the computing data size for each ADSS, the total utility of ADSSs generally increases. Furthermore, considering the fixed service price of the DSO and the same computing data size, because of the low transmission delay, the utility of the ADSS in fog computing can be better than the utility in cloud computing. However, in fog computing, the DSOs are able to set high prices in the virtualized network to gain high revenues. With our proposed algorithm, we guarantee that the utility of the ADSS in fog computing is always higher than that in cloud computing, and the improvement gap of the ADSSs' utility from fog computing to cloud computing is small.

The Three-Layer Hierarchical Game for Fog Computing

From the interaction analyses between DSOs and FNs, between DSOs and ADSSs, and between FNs and ADSSs, a general data service with the proposed three-layer hierarchical game can be summarized as in Fig. 6. In the flowchart, the DSOs first play the Stackelberg game with all ADSSs, and the DSOs are required to make decisions based on the investigation of all the FNs' and ADSSs' information. If the DSOs cannot gain higher revenues by adopting the FNs, the cloud computing will be adopted where FNs will not be included in the data services. If the fog computing is able to bring high profits (i.e., revenue minus costs) for the DSOs, the DSOs then consider whether or not renting the FNs from the third party is beneficial. If the DSO is able to achieve higher utility by renting the FNs from the third party, moral hazard can be applied to motivate the FNs. Otherwise, the DSOs will apply their own FNs for the data services. Finally, with the provided resources from the FNs and the requirements from the ADSSs, the student project allocation matching game is employed to achieve stable results.

Conclusions

In this article, we have proposed a three-layer hierarchical game framework for resource management in the multi-DSO, multi-FN, and multi-ADSS scenario. In the proposed framework, we have first introduced a Stackelberg game between DSOs and ADSSs, where DSOs act as the leaders, providing virtualized services to ADSSs, the followers. Second, based on the total amount of requested virtualized resources, a moral hazard model in contract theory is adopted between the DSOs and FNs to motivate the FNs to offer efficient physical resources. Third, based on the offered physical resources and provided virtualized resources, a student project matching game has been proposed for resource allocation. Finally, based on the hierarchical game framework, we have summarized our work and shown it in the flowchart in Fig. 6.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation Nos. CPS-1646607, ECCS-1547201, CCF-1456921, CNS-1443917, ECCS-1405121, NSFC61428101, and ECCS-1554576.

References

[1] S. Yi, C. Li, and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," *Proc. 2015 Wksp. Mobile Big Data*, Hangzhou, China, pp. 37–42.

[2] Y. Mao *et al.*, "Mobile Edge Computing: Survey and Research Outlook," arXiv preprint arXiv:1701.01090, 2017.

[3] CISCO, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are," white paper; https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf, accessed Apr. 2015.

[4] I. Goiri et al., "Intelligent Placement of Datacenters for Internet Services," *Proc. IEEE ICDCS*, Minneapolis, MI, June 2011, pp. 131–42.

[5] H. Zhang *et al.*, "Fog Computing in Multi-Tier Data Center Networks: A Hierarchical Game Approach," *Proc. IEEE ICC*, Kuala Lumpur, Malaysia, May 2016.

[6] G. S. S. Sardellitti and S. Barbarossa, "Joint Optimization of Radio and Computational Resources for Multicell Mobile-Edge Computing," *IEEE Trans. Signal Info. Processing over Networks*, vol. 1, no. 2, June 2015, pp. 89–103.

[7] Z. Jiang *et al.*, "Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture," *Proc. 2013 IEEE 7th Int'l. Symp. Service Oriented System Engineering* Redwood City, CA, Mar. 2013, pp. 320–23.

[8] Y. Feng, B. Li, and B. Li, "Price Competition in an Oligopoly Market with Multiple IaaS Cloud Providers," *IEEE Trans. Computers*, vol. 63, no. 1, Jan. 2014, pp. 59–73.

[9] J. C. Harsanyi and R. Selten, *A General Theory of Equilibrium Selection in Games*, MIT Press, 1988.

[10] Z. Han *et al.*, *Game Theory in Wireless and Communication Networks: Theory, Models and Applications*, Cambridge Univ. Press, 2011.

[11] A. H. A. El-Atta, and M. I. Moussa, "Student Project Allocation with Preference Lists over (student, project) Pairs," *Proc. Second Int'l. Conf. Computer and Electrical Engineering*, Dubai, UAE, Dec. 2009.

[12] D. J. Abraham, R. W. Irving, and D. F. Manlove, "The Student-Project Allocation Problem," *Proc. 14th Int'l. Symp. ISAAC*, Kyoto, Japan, Dec. 2003, pp. 474–84.

[13] P. Bolton, and M. Dewatripont, *Contract Theory*, MIT Press, 2004.

[14] Y. Zhang *et al.*, "Multi-Dimensional Payment Plan in Fog Computing with Moral Hazard," arXiv preprint arXiv:1701.07877, 2017.

[15] H. Zhang *et al.*, "Computing Resource Allocation in Three-Tier IoT Fog Networks: A Joint Optimization Approach Combining Stackelberg Game and Matching," arXiv preprint arXiv:1701.03922, 2017.

Biographies

Huaqing Zhang [S'14] received his B.S. degree from Huazhong University of Science and Technology, Wuhan, China, in June 2013. He is now pursuing a Ph.D. degree in the Department of Electronic and Computer Egineering at University of Houston, Texas. He has been a reviewer for TWC, TCCN, TBC, and JWCN. His research interests include wireless communications and networking, zero-determinant strategy, and hierarchical game.

Yanru Zhang [S'13, M'16] received her B.S. degree in electronic engineering from the University of Electronic Science and Technology of China in 2012, and her Ph.D. degree from the Department of Electrical and Computer Engineering, University of Houston in 2016. She is now working as a postdoctral fellow at the Network Communications and Economics Lab, Chinese University of Hong Kong. Her current research involves the contract theory and matching theory in network economics, Internet and applications, and wireless communications and networking. She received the best paper award at IEEE ICCS 2016.

Yunan Gu received her M.S. in computer science from Texas Southern University in 2013 and her Ph.D. degree in electrical and computer engineering from the University of Houston in 2016. Now, she is in an R&D engineer in the IP Technology Research Division of Huawei. Her research interests include matching theory, LTE-Unlicensed, D2D, V2X, and so on.

Dusit Niyato [M'09, SM'15, F'17] is currently an associate professor in the School of Computer Science and Engineering, Nanyang Technological University, Singapore. He received his B.Eng. from King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999 and his Ph.D. in electrical and computer engineering from the University of Manitoba, Canada, in 2008. His research interests are in the area of energy harvesting for wireless communication, the Internet of Things (IoT), and sensor networks.

Zhu Han [S'01, M'04, SM'09,F'14] received his B.S. degree in electronic engineering from Tsinghua University in 1997, and his M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively. From 2000 to 2002, he was an R&D engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a research associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the *Journal on Advances in Signal Processing* in 2015, the IEEE Leonard G. Abraham Prize in the Field of Communications Systems (best paper award in *IEEE JSAC*) in 2016, and several best paper awards at IEEE conferences. Currently, he is an IEEE Communications Society Distinguished Lecturer.

With our proposed algorithm, we guarantee that the utility of the ADSS in fog computing is always higher than that in cloud computing, and the improvement gap of the ADSSs' utility from fog computing to the cloud computing is small.

SOFTWARE-DEFINED VEHICULAR NETWORKS: ARCHITECTURE, ALGORITHMS, AND APPLICATIONS: PART 2

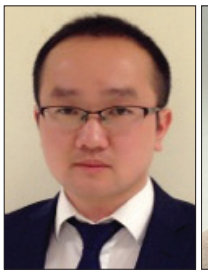

Guangjie Han


Mohsen Guizani


Yuanguo Bi


Tom H. Luan


Kaoru Ota


Haibo Zhou


Wael Guibene


Ammar Rayes

Due to the random vehicle mobility and varying communication environment, an integrated vehicular network comprising heterogeneous access technologies (DSRC, WiFi, 4G/LTE, 5G, etc.) will be indispensable to provide ubiquitous mobile coverage. Although heterogeneous networking has been extensively studied in different contexts, the salient features of vehicular communications (e.g., varying road density, fast mobility) have brought new challenges and led to fundamental and interesting research issues, such as how to flexibly configure and efficiently conduct resource allocation, how to enable interoperation among multiple coexisting networks, and how to effectively accommodate a large number of traveling users with various kinds of smart devices.

In addition to the advances in the underlying access technologies, cloud computing as a centralized control and management solution has become mature, representing an indispensable component of large scale vehicular networks. In particular, software-defined networking (SDN) has emerged as a promising paradigm to control the network in a systematic way, gaining attention from both academia and industry. The flexibility and programmability of SDN not only make it attractive to satisfy the quality of service (QoS) requirements of vehicular services, but also greatly simplify resource management in heterogeneous vehicular networks.

In this Feature Topic (FT), we invited authors from the industry and academic research communities to discuss the architecture, applications, challenges, and standardization efforts on enabling software-defined vehicular networking (SDVN). We received a large number of submissions and conducted a rigorous review process. This is Part 2 of the FT.

To deliver content to remote vehicles, path establishment, maintenance, and identity assignment in dynamic vehicular networks generate much overhead. S. H. Ahmed *et al.*, in ''Named Data Networking for Software Defined Vehicular Networks," present an architecture that utilizes SDN in vehicular networks to support content retrieval by named data networking. Furthermore, a number of current research challenges are discussed, and a precise roadmap to address these issues is provided.

The high user mobility in vehicular networks usually results in long handover delay among eNodeBs (eNBs) in 5G communications. C. F. Lai *et al.*, in "A Buffer-Aware QoS Streaming Approach for SDN-Enabled 5G Vehicular Networks," propose a buffer-aware QoS streaming approach over SDN-enabled 5G vehicular networks, which provides various priority levels of streaming services to mobile users. Experimental results show that the proposed approach can adjust the priority of streaming content segments and avoid the delay of streaming content transmissions for 5G vehicular networks.

In order to support software updates in vehicles, M. Azizian *et al.* propose an SDN-based vehicular cloud architecture (SVC) that leverages vehicle-to-vehicle (V2V) communications in ''Vehicle Software Updates Distribution with SDN and Cloud Computing." In SVC, solutions on how vehicular networks can be modeled as connectivity graphs are proposed, and an SDN-based scheme that assigns different frequency bands to graph edges is presented to improve network performance.

The highly coupled design of traditional networks cannot satisfy various QoS requirements in vehicular networks. W.

Quan *et al.*, in ''Enhancing Crowd Collaborations for Software Defined Vehicular Networks," propose a customized smart identifier networking (SINET)-based solution to enable crowd collaboration for SDVN. It utilizes crowd sensing to flexibly select virtualized function slices, and enables crowd collaboration to dynamically adapt to various vehicular scenarios and applications.

In edge networks, a network may suffer from potential interference, resource congestion, or underutilization in the absence of joint resource optimization. D. J. Deng *et al.*, in ''Latency Control in Software Defined Mobile Edge Vehicular Networking," point out a complete series of latency control mechanisms and principles for edge-up software-defined cloud/edge vehicular networking. The proposal thus creates a paradigm shift to enable SDVN.

Drivers' fatigue and their mood shifts may lead to traffic accidents. Y. Zhang *et al.*, in ''SOVCAN: Safety-Oriented Vehicular Controller Area Network," propose an SDN-based approach to develop a safety-oriented vehicular controller area network (SOVCAN), which can improve traffic safety by detecting drivers' fatigue and recognize their emotions.

In order to offload the data to centralized servers or other devices, an intelligent controller is indispensable to make decisions. G. S. Aujla *et al.*, in ''Data Offloading in 5G-Enabled Software-Defined Vehicular Networks: A Stackelberg-Game-Based Approach," propose a novel data offloading scheme for 5G-enabled SDN-based vehicular networks. The SDN-based controller makes decisions for data offloading by using the priority manager and load balancer. In addition, a single leader multi-follower Stackelberg game is designed for network selection. The performance evaluations of the proposed scheme demonstrate the superiority of the scheme to other existing proposals.

In closing, we would like to thank all of those who have made significant contributions to this FT, including the contributing authors, the anonymous reviewers, and the *IEEE Communications Magazine* publications staff, in particular the Editor-in-Chief. We believe that the research results presented in this FT will further stimulate research and development ideas in vehicular networks.

BIOGRAPHIES

GUANGJIE HAN [S'01, M'05] is currently a professor with the Department of Information and Communication Systems, Hohai University, China. His current research interests include sensor networks, computer communications, mobile cloud computing, and multimedia communication and security. He has served on the Editorial Boards of up to 14 international journals, including *IEEE Access* and *Telecommunication Systems*. He has been a Guest Editor for a number of Special Issues in IEEE journals and magazines. He is a member of ACM.

MOHSEN GUIZANI [S'85, M'89, SM'99, F'09] received his B.S, M.S., and Ph.D. from Syracuse University. He is currently a professor and the ECE Department Chair at the University of Idaho. His research interests include wireless communications/mobile cloud computing, computer networks, security, and smart grid. He is the author of nine books and more 450 publications. He was Chair of the IEEE Communications Society Wireless Technical Committee. He served as an IEEE Computer Society Distinguished Speaker.

YUANGUO BI received his Ph.D. degree from Northeastern University, Shenyang, China, in 2010. He joined the School of Computer Science and Engineering, Northeastern University, as an associate professor in 2010. His current research interests focus on medium access control, QoS routing, multihop broadcast, mobility management in vehicular networks, as well as SDN-enabled vehicular networks.

TOM H. LUAN received his Ph.D. degree from the University of Waterloo, Ontario, Canada, in 2012. Since December 2013, he has been a lecturer in mobile and apps with the School of Information Technology, Deakin University, Melbourne, Australia. His research mainly focuses on vehicular networking, wireless content distribution, peer-to peer networking, and mobile cloud computing.

KAORU OTA received Ph.D. degrees in computer science and engineering from the University of Aizu, Japan, in 2012. She is currently an assistant professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. She was a research scientist with the A3 Foresight Program (2011–2016) funded by the Japan Society for the Promotion of Sci-ences (JSPS), NSFC of China, and NRF of Korea.

HAIBO ZHOU received his Ph.D. degree in information and communication engineering from Shanghai Jiao Tong University, China, in 2014. From 2014 to 2016, he was a postdoctoral research fellow with the Broadband Communications Research (BBCR) Group, University of Waterloo. He is currently a research associate in the BBCR Group. His current research interests include resource management and protocol design in cognitive radio networks and vehicular networks.

AMMAR RAYES [S'85, M'91, SM'15] is a Distinguished Engineer focusing on the technology strategy for Cisco Services. His research interests include IoT, network management NMS/OSS, machine learning, analytics, and security. He has authored three books, over 100 publications in refereed journals and conferences on advances in software and networking related technologies, and over 25 patents. He received B.S. and M.S. degrees from the University of Illinois at Urbana and a D.Sc. degree from Washington University, all in electrical engineering.

WAEL GUIBENE is a research scientist at Intel Labs since June 2015. He was awarded his Ph.D. from Telecom ParisTech in July 2013. He also holds an M.Eng. and a Master's degree in telecommunications obtained in 2009 and 2010, respectively. He worked at Eurecom as a research engineer from 2010 to November 2013, and then joined Semtech to work on LoRa systems from 2013 to June 2015. His research activities include IoT, 5G, and wireless communications.

Named Data Networking for Software Defined Vehicular Networks

Syed Hassan Ahmed, Safdar Hussain Bouk, Dongkyun Kim, Danda B. Rawat, and Houbing Song

The authors discuss both SDN and NDN enabled VNs, and present an architecture that combines SDN functionalities within VNs to retrieve the required content using NDN. They also discuss a number of current research challenges and provide a precise roadmap that can be considered to jointly address such challenges by the research community.

ABSTRACT

Named data networking and software defined networking share mutual courage in changing legacy networking architectures. In the case of NDN, IP-based communication has been tackled by naming the data or content itself, while SDN proposes to decouple the control and data planes to make various services manageable without physical interference with switches and routers. Both NDN and SDN also support communication via heterogeneous interfaces and have been recently investigated for vehicular networks. Naïve VNs are based on the IP-based legacy, which is prone to several issues due to the dynamic network topology among other factors. In this article, we first see both SDN and NDN enabled VNs from a bird's eye view, and for the very first time, we present an architecture that combines SDN functionalities within VNs to retrieve the required content using NDN. Moreover, we discuss a number of current research challenges and provide a precise roadmap that can be considered for the research community to jointly address such challenges.

INTRODUCTION

The rapid growth in Internet traffic has triggered a plethora of research and development projects in the wide domain of communications. Today, we prefer to use high bandwidth and expect a great quality of experience (QoE) in the communication technologies ranging from cellular, Wi-Fi, WiMAX, and Bluetooth to the Internet of Things (IoT) [1]. Similarly, the past two decades have brought tremendous advancements in the transportation and automation industries, where the assurance of safety and security have become the baseline of what we are perceiving today; for example, autonomous cars, safety/non-safety information dissemination between vehicles (V2V), infrastructure-based vehicle communications (V2I), and heterogeneous vehicular networks (VNs) [2].

The key applications for VNs include, but are not limited to, traffic conditions, accident warnings, pedestrian collision warning systems, smart parking, auto-braking systems, live video streaming, and live gaming. However, the main technical challenges in VNs are related to the high volatility and dynamicity of vehicles' mobility. Even though the Dedicated Short-Range Communication (DSRC) and Wireless Access Vehicular Environment (WAVE) protocol suites have been playing a sophisticated role in the initial stages of VN implementation, it is hard to ensure low latency, high quality, and secured content or data[1] retrieval in a robust manner. Moreover, the DSRC and WAVE protocols are based on the conventional TCP/IP originally designed for a single conversation between two end-to-end entities widely known as *client* and *host*.

Regardless of the applications' motivation (i.e., safety or non-safety), the main purpose of connecting vehicles is to share the content to fulfill the applications' requirements. However, dynamic mobility makes it difficult to have reliable communication of the content between connected vehicles. The main reason is that the current standards were originally proposed for static and quasi-static environments. Despite the fact that these standards tend to support mobility and fast content delivery in VNs, the applications still require a destination address to deliver the content. Hence, the communication is contingent on the vehicle's identity (IP and/or medium access control, MAC, address). Hence, the path establishment, maintenance, and identity assignment in VNs are challenging and generate much overhead. From a non-safety application's point of view, it requires content irrespective of the identity and location of the actual provider or producer.

Meanwhile, named data networking (NDN) [3] as an extension of content-centric networks (CCNs) [4] has been merged into VNs (VNDN) as a future networking architecture [5]. VNDN basically assigns a *name* to the content rather than the device (i.e., vehicles), and that name is used to retrieve the required content. In VNDN, we consider a simplified pull-based communication, where a content requesting vehicle (the *consumer*) sends an Interest message, and the infrastructure or vehicle with the required content (the *provider*) sends back the Data message. Interest contains the required content name and unique NONCE value to identify the Interest message and avoid its duplicate transmission. On the other hand, the Data message contains the same content name and the embedded security information (e.g., digital signature) within it. Therefore, instead of securing the connection between consumer-provider node pairs, the security is inherently augmented with the Data. Additionally, VNDN supports multiple interfaces for reliable and quick fetching of the required content. Every NDN enabled vehicle maintains the following basic data structures:

[1] In the context of this article, the terms *data* and *content* are interchangeable.

Digital Object Identifier:
10.1109/MCOM.2017.1601137

Syed Hassan Ahmed, Safdar Hussain Bouk, and Dongkyun Kim are with Kyungpook National University; Danda B. Rawat is with Howard University; Houbing Song is with Embry-Riddle Aeronautical University.

0163-6804/17/$25.00 © 2017 IEEE

- Content store (CS): This caches data or contents either generated or received by the vehicle.
- Forwarding information base (FIB): It stores the outgoing interface(s) associated with the name prefixes to forward the Interests.
- Pending Interest Table (PIT): This keeps track of the names or name prefixes, NONCEs, and incoming interfaces of the received Interest(s). The entries are kept for a certain period and removed when the Interests are satisfied or their lifetime in the PIT expires.
- NONCE List: It records the NONCEs of all the pending entries of the satisfied Interests from the PIT to prevent an Interest loop. All entries are timestamped and purged after a certain time period.

An Interest is uniquely identified by the NONCE plus content Name. A node receiving an Interest first checks the NONCE list, to check whether the Interest has been recently satisfied or not. If no entry is found in the NONCE list, a record of the received Interest is scanned in the PIT to verify whether the Interest is still pending or not. The entry in the PIT shows that the Interest has already been forwarded. On the contrary, the NONCE and Name are stored in the PIT along with the Interface from where the Interest was received (called *InFace*). The PIT entry is purged once the Interest is satisfied. If a node receives multiple copies of the pending Interest, the InFace(s) and other information are aggregated in the PIT record with the same Name. In a scenario where a node receives a Data message, it first checks the PIT record. Based on the PIT search result, the Data message is either forwarded, if there is an entry in the PIT, or dropped otherwise. The satisfied Interest's record is removed from the PIT, and NONCE(s) information is stored in the NONCE list. An Interest loop occurs when a node receives another copy of the satisfied Interest from the path with large delay and can be avoided by checking the Interest's record in the NONCE list. This operational mechanism of Interest and Data messages is summarized in Fig. 1.

Benefits of applying NDN in VNs are discussed thoroughly in our recent works [6–8]. To be precise, the VNDN separates the functions that assist in locating and supplying the required content from the underlying communication technologies used by the VNs. The preparation nature of the data retrieval process brings in the discussion of software defined networking (SDN) [9]. We have known SDN as an alternative and emerging way to look at the networking architecture [10]. Here it is worth mentioning that any networking system is based on the control plane, the data plane, and the management plane. The control and management plane serve the data plane, which bears the traffic that the network exists to carry. The management plane, which is responsible for administrative traffic, is considered a subset of the control plane. In the conventional networks, all three planes are implemented in the firmware of routers, switches, and related network elements. SDN decouples the data and control planes by removing the control plane from network hardware and implements it in software using OpenDayLight, which enables software-based access and, as a result, makes network administration much more flexible. Moving the control plane to software allows dynamic access and administration. Similarly, the administrator can change any network switch's rules when necessary, including prioritizing, de-prioritizing, or even blocking specific types of packets with a very granular level of control. Explicitly, both VNDN and SDN share the concept of core architectural changes from their own perspectives.

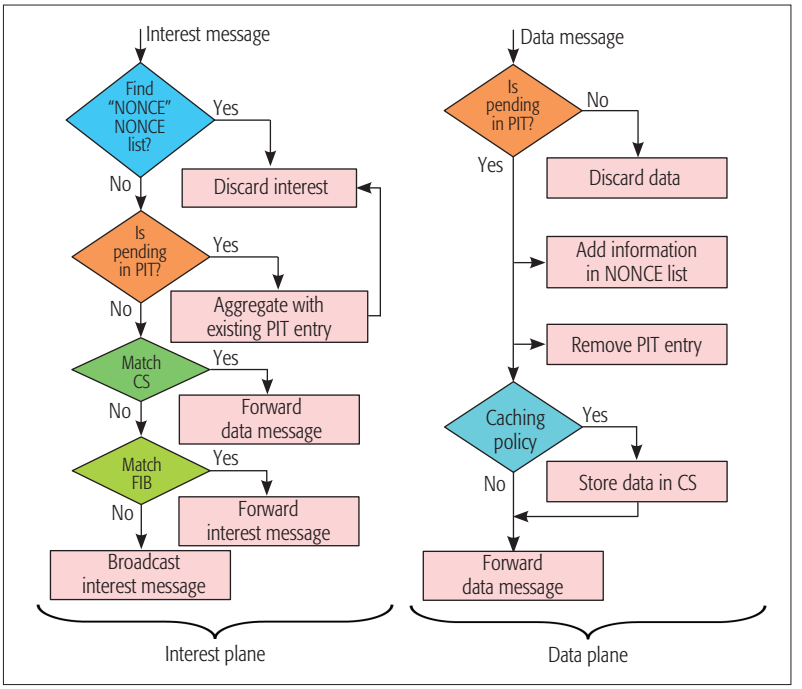


Figure 1. *Interest* and *data* message processing in VNDN.

This article discusses the possible cohesion of VNDN and SDN to support robustness in content retrieval. Although there are recent efforts being carried out for combining the future Internet architectures with SDN features, to the best of our knowledge, we will be leading the research community in bridging both technologies for VNs. In the following section, a basic overview of SDN-based VNs and NDN-enabled VNs is presented. Furthermore, a novel architecture for retrieving the named data in VNs using SDN features, followed by the open research issues, is presented.

Bird's Eye View of Software Defined-Named Data Vehicular Networks

The cultivation of VNs through conventional technologies, such as the IEEE 802.11x family and third/fourth generation (3G/4G) cellular infrastructures, while utilizing the existing switches and routers has led us to several issues and challenges such as frequent disconnection due to fast mobility, short-range communication, and so on. In order to address these issues, several concepts such as intelligent transportation systems (ITS), V2V, and V2I have been proposed [11]. However, the tremendous increase in the number of vehicles and the different requirements of users cannot be addressed through conventional switching and routing techniques. SDN presents intelligent mechanisms and solutions to switch and route the vehicular data by incorporating several parameters including traffic density, multiple

The unification of the interfaces of various technologies can be made possible by decoupling the control and data planes in SDVN. This will allow us to make centralized decisions by designing flow table entries at the data plane side. However, the approach of decoupling planes is not straightforward and can lead to several issues and challenges.

network interface, and so on. In addition to communication in a heterogeneous wireless environment, a unified abstraction model is needed to link the communication of different technologies on a single platform.

SDVN: SDN Transition to Vehicular Networks

The unification of the interfaces of various technologies can be made possible by decoupling the control and data planes in the software defined vehicular network (SDVN) [12]. This will allow us to make centralized decisions by designing flow table entries at the data plane side. However, the approach of decoupling planes is not straightforward and can lead to several issues and challenges.

In a typical SDVN, the communication of the Data messages is logically controlled by the centralized control plane. However, such centralization of the control plane mainly dependeds on the vehicles' trajectory predictions. In a naïve wired SDN, the communication between the data and control planes is carried out by high-speed optical fiber; however, in the case of SDVN, the communication is mainly performed via wireless links. Thus, the cost of communication and the dynamic topology have great impact on SDVN deployment and configuration. Nevertheless, intelligent techniques are needed to tackle the topology variations by using various techniques such as self-configuration and self-healing. Moreover, SDVN is highly dependent on fast and efficient virtual routing and switching of the Data messages; therefore, the modeling of single-hop and multihop communication can be revised and remodeled to meet the requirements of vehicular applications in a scalable manner. Likewise, the introduction of 5G will somehow solve the data forwarding capability by high-speed networking, but again the linking of SDVN with 5G will bring several challenges. To be precise, designing a communication model for SDVN becomes more challenging due to the limited coverage and short-range communication technologies such as Wi-Fi that cannot address the connectivity of vehicles. More or less, fetching important information from the cloud [13] and the rest of communication can be achieved through Wi-Fi technology.

SDN-NDN Mutuality

Nevertheless, there are similarities in the concept of SDN and NDN; for example, a tentative change to conventional switches and routers in the form of decoupled planes and retrieving the required content by naming the content instead of devices (end-to-end devices, NDN).

Similarly, the previously scanned literature considers NDN to exchange Interest/Data messages over a single wireless interface (i.e., 802.11 in the case of VNs). However, it is foreseen that vehicles will be equipped with a variety of wireless communication interfaces thanks to the NDN forwarding strategy, which is natively able to deal with multiple network interfaces [14]. Likewise, SDN also tends to support multiple interfaces by allowing the control plane to make decisions based on the packet's requirements. Moreover, NDN can decide, for each incoming Interest, which outgoing face to use (e.g., the best-performing face, one of a subset of possible faces, or any available face). On the other hand, in SDN, the decision depends on the implemented forwarding strategy, which may take as input the face cost, determined by the routing protocol, and the face rank, maintained by the flow tables. In the following section, we present an architecture for combining SDN-NDN for VNs and discuss the tentative working principles of our proposed architecture.

When SDVN Meets VNDN: An Architecture

The main objective of the proposed architecture is to provide SDN services and benefits to efficiently communicate named contents over VNs with better network resource utilization. SDN-based named data VNs consist of mobile vehicles, fixed infrastructure points — roadside units (RSUs), base stations (BSs), and so on — and the SDN controller. The proposed software defined vehicular named data networking (SDVNDN) architecture can be deployed as a clean slate or an overlay architecture on the current IP. For the control and data planes, any of the wireless interfaces in the network can be used by the VNs. All these VN elements run our proposed SDN architecture. The working principle of each component of the proposed architecture is discussed below.

Components of the Proposed Architecture

SDN Controller: The SDN controller is a network entity that has an overall network view to effectively orchestrate the network elements to efficiently perform the NDN operations including content caching, intelligent Interest and Data message forwarding, broadcast control, push-base services, and so on. Upon reception of an Interest with a specific content name prefix, it can easily delegate the forwarding, caching, and other strategies to the SDN-enabled nodes to avoid network congestion and provide quality of service (QoS)-based content communication between the provider and consumer nodes. The controller also forwards the prefix(es) (name or IP prefix depending upon the clean slate or overlay implementation, respectively,) to the network elements to receive Interests no forwarding rules of which are defined in the FIB table.

Caching: In NDN, per packet caching is performed by the nodes involved in the content forwarding process. The caching policies include cache all, probability-based caching, popularity-based caching, and no caching. Other than the caching policies, the cache location and caching pattern are also important in NDN. Cache location and caching pattern determine where the content should be cached and in what format (either whole or chunk-based content caching), respectively. Due to the dynamic nature of the network, the fixed elements at the edge of the VNs or potential nodes (maybe parked vehicles or vehicles with low mobility) may play a vital role in caching contents. It is worth investigating the network performance when RSUs, BSs, access points (APs), or potential nodes are selected as caching anchors. The SDN controller must select the feasible caching location(s) to avoid unnecessary copies of the content to balance the CS capacity and search overhead in the network. In the case of a large content, each Data message commu-

nicates a fragment or chunk of the content. Each content chunk in a separate Data message is forwarded through dynamic multiple paths, where each node along a path may be different when content chunks are forwarded to the consumer node. In this situation, the whole content may not be forwarded through the same set of vehicles. However, the question arises of whether it will be feasible to cache random fragments of the content and for how long those fragments should be cached. Because of the dynamic topology, the vehicles may receive unsolicited fragments of a content, and the network must describe the caching policies for unsolicited content fragments.

Content Naming: In NDN, either the whole content or a chunk of the content is identified and accessed using the name. The well-known NDN implementation of integrated computing networking (ICN) uses the hierarchical name structure consisting of several components in the name, each separated by /. In the VN scenario, each name component defines the relationship between content or content chunks and its spatial and/or temporal information where the content belongs. As the content searching and forwarding decisions depend on its name, the name must contain necessary components to precisely and efficiently receive the content from the network.

Intelligent Forwarding: The FIB table plays a pivotal role in content communication in the NDN. It contains name prefix, outgoing face ID(s), and some key parameters including the rank of the face(s). Every time an Interest is satisfied through a specific face, its rank is increased, which makes it more suitable for Interest forwarding in the future. Conversely, the successive data retrieval failures reduce the face's rank. This rank value is used to prioritize the face and its preference to forward Interests. If the rank value exceeds the threshold, it may be purged from the FIB. Therefore, the Interest satisfaction success probability depends on the updated FIB information.

If no entry is found in the FIB table, the Interest is forwarded to the controller, and based on the global network view and provider information, it defines the FIB entries plus their corresponding outgoing faces. These entries are delegated to the intermediate nodes between the consumer and provider nodes. The controller should include faces in FIB entries that satisfy the Interest's QoS requirements (e.g., minimum delay, low cost, high bandwidth). Once the Interest is successfully forwarded to the provider (either through single path or multiple path, or in a broadcast manner) and PIT entries are maintained at intermediate nodes, the content communication back to the consumer is a relatively straightforward operation.

Push-Based Forwarding: Push-based communication is one of the fundamental requirements of safety-based vehicular applications (accident or crash warning, emergency vehicle approaching, blind spot warning, etc.). However, there is no standard communication mechanism specified in the name data communication architectures to forward time-critical warning messages in a push-based manner. Most push-based communication requires location and heading formation of the vehicles. In an accident warning scenario, a warning message generated by the vehicle should be forwarded in time to all the following vehicles behind the warning issuing vehicle(s). Conversely, in the emergency vehicle approaching scenario, the warning message should be forwarded to the vehicles before the warning message generating vehicle. This module formulates the rules based on the warning type and spatio-temporal traffic information from the topology indicator. The rules include warning dissemination area, time-critical QoS requirements, and warning dissemination direction. Those rules are periodically advertised in the network to keep all network elements ready in advance to efficiently communicate warnings.

Intrinsic Data Security: In named data architecture, the content security is intrinsic in the content itself. Every content chunk and its corresponding name in the Data message are digitally signed to prove the binding between them. Signatures are mandatory in each Data message. The provider information along with the public key evidence verifies the provenance of the data. Keys along with their digital certificates are communicated as a Data message in the NDN. However, the consumer and producer vehicles must use agreed upon security policies (public key verification and signing policies) to imply the content or content chunk verification. Every vehicle shares its security and access control policies for accessing the cached contents from the CS with the controller through fixed infrastructure nodes. Having a global view of the network, the security block of the SDN controller disseminates the security and access control policies to the nodes involved in the Interest and Data message propagation.

Congestion Control: There may be a case in VNs where Interest-Data traffic may accumulate at any node in the network depending on the events or popularity of contents in a specific network region. Due to a large number of Interests and contents' flow through a node, the Interests may not be satisfied because there is specific out face link congestion, or the CS may be full or getting larger (depending on the caching policy), which may increase the cache miss ratio. To alleviate the congestion at any network point, the nodes keep traffic status of every face, and this information is shared with the controller. In view of the network traffic information, the controller selects different faces as well as the caching points in the network to evenly distribute the network traffic.

Topology Indicator: In the case of a mobile producer, the location, heading, speed, and content prefix can be used by the SDN controller to predict availability of the providers and the consumers. Every vehicle shares this information to the fixed infrastructure network elements and the information of its neighboring nodes. Information provided by the topology indicator, content prefix manager, and state information modules are used to devise and disseminate the forwarding rules to the intermediate nodes between consumer and producer.

Content Prefix Manager: Every network element publishes its CS prefix list along with the respective expiration time and vehicle identification information to the SDN controller. If a content is cached at multiple providers, a single prefix along with the multiple provider IDs are stored in the list. When the controller receives an Interest,

The proposed SDVNDN architecture can be deployed as a clean slate or an overlay architecture on the current IP. For the control and data planes, any of the wireless interfaces in the network can be used by the VNs. All these VN elements run our proposed SDN architecture.

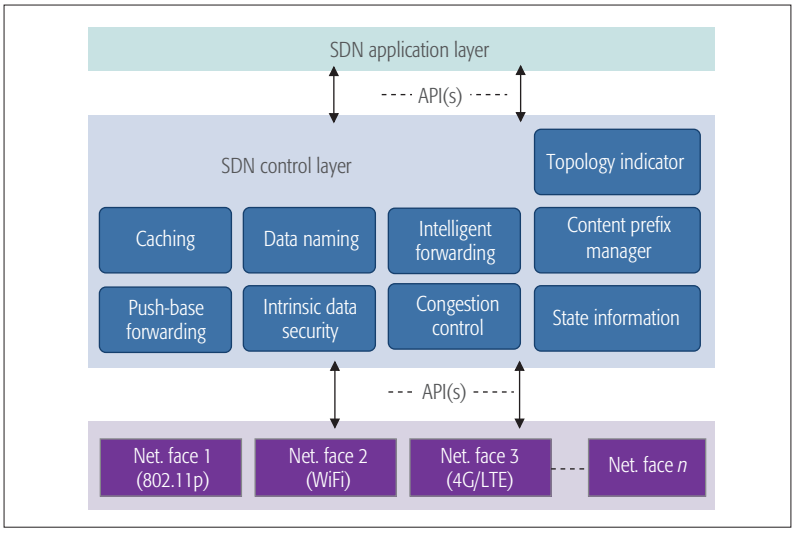


Figure 2. Proposed architecture for SDN-NDN-enabled VNs.

it performs prefix search in the content prefix list and finds the potential producer(s).

State Information: Every node monitors the Interest-Data traffic over each face (incoming and outgoing faces), per prefix traffic, and CS information (content replacement, hit or miss ratio, storage utilization, etc.). Every VN element shares its state information with the controller, and the controller manages this information in the state information table. This information helps the controller formulate better congestion control and caching policies.

Working Principles

In NDN architecture, the FIB serves an essential role to forward Interest messages in the network. Similarly, the availability of a content or chunk(s) of contents in CS depends on the popularity of the content, caching policy, and the timestamp until which that content is available in the CS. Once the timestamp expires, the entry in CS becomes stale and is purged accordingly. Additionally, the VN has a highly dynamic network topology due to high mobility of vehicles, and each vehicle may be equipped with more than one wireless interface. Therefore, the Interest messages may not be forwarded through the same set of interfaces and forwarding rules where they were satisfied previously.

Pull-Based Communication and Forwarding: Consider the example of a simple named data communication scenario in software defined VNs, as shown in Fig. 2. A consumer vehicle generates an Interest message including the content name and the unique Identifier (e.g., NONCE in NDN architecture). In a clean slate implementation, when an Interest message is received by the RSU or BS, it is simply forwarded to the controller through a predefined prefix in the FIB table. Intermediate network elements (switches, routers, etc.) between the controller and the RSU/BS forward the Interest using a vanilla NDN/CCN forwarding mechanism by maintaining the PIT entries. Once the controller receives an Interest, it searches the requested content's name prefix in the name prefix database to locate the potential content provider. After locating the content, the controller sets the forwarding, caching, and other policies based on the QoS requirements from the metadata provided in the Interest as well as the current network state. These policies are forwarded to all the VN elements involved in the Interest satisfaction process through the control plane. When network elements receive forwarding policies related to the Interest, which includes the name prefix and the outgoing face IDs of all the intermediate network elements between the consumer and provider nodes, they update their FIB entries. Subject to these policies, the Interest is forwarded to the provider node in a unicast or broadcast manner involving either the static network components or the vehicles. Refer to both cases in Fig. 3, where the Interest is forwarded in an ad hoc manner to provider A or through fixed infrastructure network elements to provider B.

In the case of an overlay architecture, the content name and related information from an Interest message is forwarded as an option in the IP packet to the controller through the controller advertised IP prefix and port information. Once the content provider is located by the controller, its address and forwarding rules are passed on to the network elements between the consumer and provider nodes. Upon reception of this information, the Interest is forwarded to the provider node. Due to the intermittent behavior of

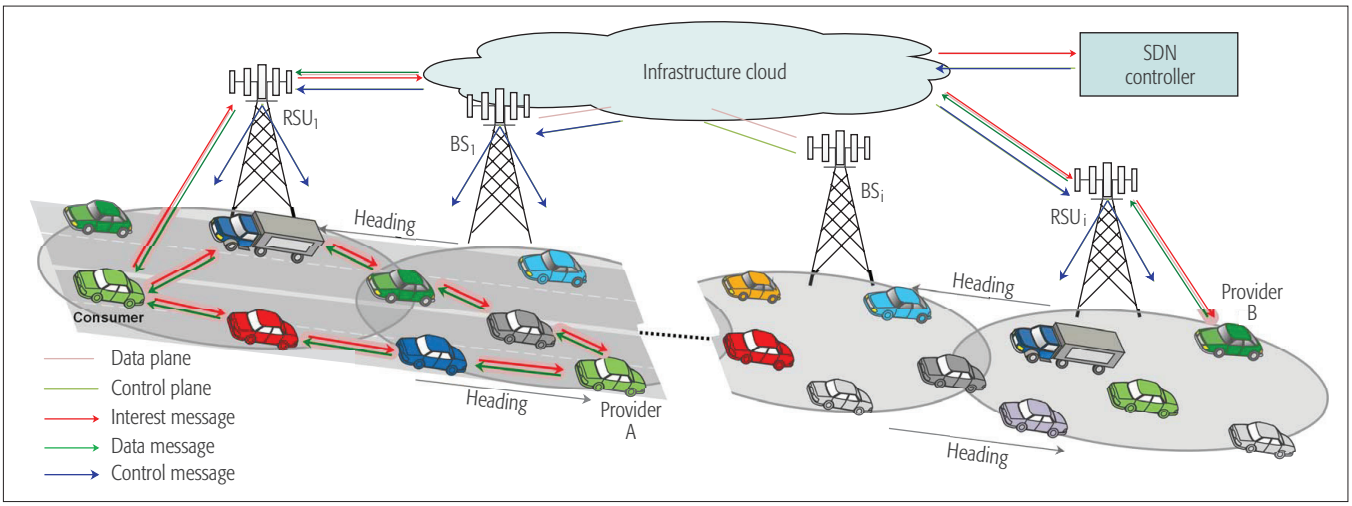


Figure 3. Pull-based named data retrieval in SDN-NDN-based VNs.

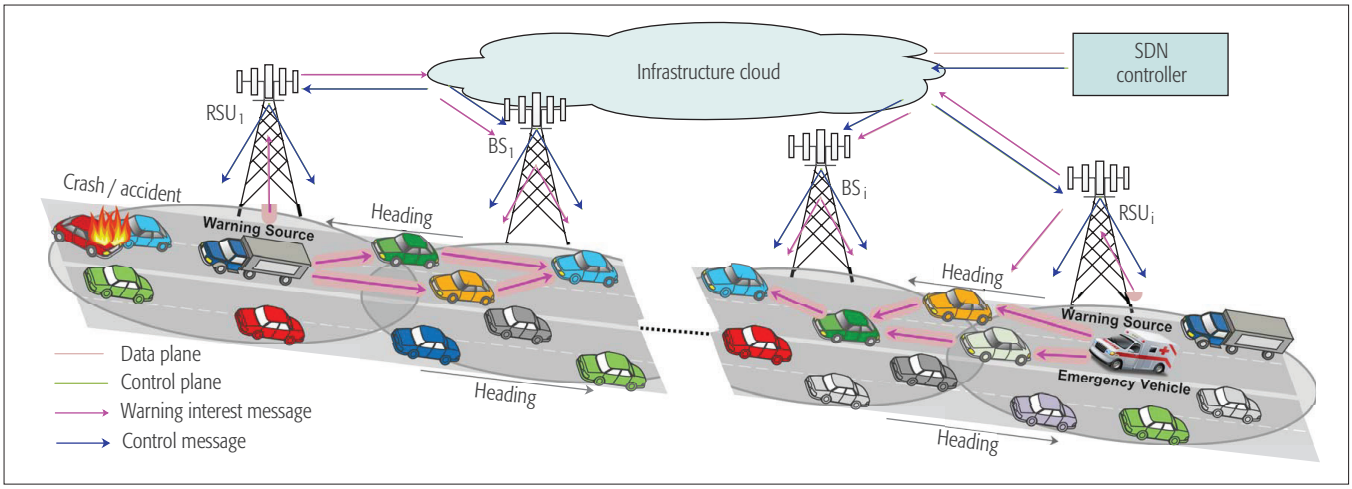


Figure 4. Push-based emergency message forwarding in SDN-NDN-based VNs.

VNs, the controller may define rules to forward Interests through multiple paths or in a broadcast manner. In VNs, there may be several consumers that generate Interests with similar name prefixes; therefore, the controller may define rules to combine Interests to collectively satisfy them.

Push-Based Communication and Forwarding: In our proposed architecture, the warning information is embedded as an extension in an Interest message with a flag to distinguish it from the pull-based Interest message. This special warning Interest message also includes the warning type, forwarding direction, PIT lifetime, and the warning generating vehicle's heading and location information. The warning Interest message is not forwarded to the controller; instead, the forwarding rules are periodically disseminated by the SDN controller in the network to avoid warning dissemination delay. Based on the heading direction of the warning message generating vehicle and the type of warning message, the VN's elements disseminate the warning in the specific region of the network accordingly. A push-based warning Interest for emergency vehicle approaching and crash scenarios are shown in Fig. 4. In case of a crash, the warning Interest is generated by a vehicle near the emergency scene. When RSU_1 and the trailing vehicles of the warning message source receive the message, they extract the warning information and forward to the application faces as well as the specified outgoing faces to inform the trailing vehicles and/or infrastructure elements. The trailing vehicles may receive the warning Interest from the RSUs, BSs, or the vehicles ahead of them. Warning Interests may be generated by the vehicles involved in the accident as well.

Open Issues and Research Roadmap

Our discussions above show that the cohesion of SDN and NDN in VNs can be beneficial in many ways. However, the proposed architecture is the first attempt and in its early stages, still far from the seamless transition. A few of the key open issues are:

•DN has been studied for wireless mobile networks to easily disseminate new services in the network. Along with the rapid increase in devices and services, more data is being generated, and thus we need to have sophisticated algorithms to search the required content. For such massive searching, NDN hierarchical naming of the content will be sufficient. Still, some real-time check using Hadoop and Dataset is missing from studies of SDN and NDN for wireless interfaces.

•In the joint venture of SDN, NDN, and VNs, forwarding tables play a vital role in making systems more efficient. Based on the current literature, it is hard to find research work focused on the active participation of forwarding rules tables. Mostly, we extract the content from tables and run algorithms on the upper layers; however, it could be more flexible to make intelligent tables' structures to enable them to take decisions.

•Similarly, communicating the content over a VN via SDN to cellular networks brings several issues and challenges [15]. For example, an abstract level of representation is needed to bridge SDN with VNs and cellular technologies. However, designing a generic platform for SDVN incorporating heterogeneous technologies can lead us to inappropriate network resources, network fragmentation, and interoperability between these networks.

•Finally, the existing trajectory prediction schemes need further modification to address the localization of vehicles over the SDN-NDN. Moreover, the decoupling of the data and control planes is not straightforward; therefore, high-speed Internet is required for intercommunication between both planes at two separate locations and devices.

Conclusion

We have foreseen the emergence of software defined networking and named data networking to retrieve the content in vehicular networks. The preliminary discussions highlighted the rationale behind SDN-based VNs, NDN-enabled VNs, and their similarities. Furthermore, the transition of future VNs has been discussed, and a contemporary detailed architecture of the SDN-NDN-based VNs has been proposed. Although SDN and NDN research is rapidly growing and approaching maturity, there is still the need for more attention from the research community to pave the foundation and guarantee effectiveness in the context of wireless and dynamic mobile networks such as VNs.

Although, SDN and NDN research is rapidly growing and approaching maturity, there is still the need for more attention from the research community to pave the foundation and guarantee effectiveness in the context of wireless and dynamic mobile networks such as VNs.

Acknowledgments

This study was supported by the BK21 Plus project (SW Human Resource Development Program for Supporting Smart Life) funded by the Ministry of Education, School of Computer Science and Engineering, Kyungpook National University, Korea (21A20131600005). Furthermore, the work of Danda B. Rawat is supported in part by the U.S. National Science Foundation (NSF) under Grants CNS-1658972 and CNS-1650831.

References

[1] J. Chen *et al.*, "Software Defined Internet of Vehicles: Architecture, Challenges and Solutions," *J. Commun. and Information Networks*, Vol. 1, no. 1, 2016, pp. 14–26.

[2] K. Zheng *et al.*, "Soft-Defined Heterogeneous Vehicular Network: Architecture and Challenges," *IEEE Network*, vol. 30, no. 4, July–Aug. 2016, pp. 72–80.

[3] L. Zhang *et al.*, "Named Data Networking," *SIGCOMM Comp. Commun. Review*, vol. 44, no. 3, July 2014, pp. 66–73.

[4] V. Jacobson *et al.*, "Networking Named Content," *Proc. 5th Int'l' Conf. Emerging Networking Experiments and Technologies*, Dec. 2009, pp. 1–12.

[5] S. H. Bouk *et al.*, "Named-Data-Networking-Based ITS for Smart Cities," *IEEE Commun. Mag.*, vol. 55, no. 1, Jan. 2017, pp. 105–11.

[6] S. H. Bouk *et al.*, "DPEL: Dynamic PIT Entry Lifetime in Vehicular Named Data Networks," *IEEE Commun. Letters*, vol. 20, no. 2, Feb. 2016, pp. 336–39.

[7] S. H. Ahmed, S. H. Bouk, and D. Kim, "RUFS: RobUst Forwarder Selection in Vehicular Content-Centric Networks," *IEEE Commun. Letters*, vol. 19, no. 9, Sept., 2015, pp. 1616–19.

[8] S. H. Ahmed *et al.*, "CODIE: Controlled Data and Interest Evaluation in Vehicular Named Data Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 6, June 2016, pp. 3954–63.

[9] R. Soua *et al.*, "SDN Coordination for CCN and FC Content Dissemination in VANETs," *Ad Hoc Networks*, Springer Int'l. Publishing, 2017, pp. 221–33.

[10] K. Xu *et al.*, "Toward Software Defined Smart Home," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 116–22.

[11] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 4th qtr. 2015, pp. 2347–76.

[12] I. Ku *et al.*, "Towards Software-Defined VANET: Architecture and Services," *13th Annual Mediterranean Ad Hoc Networking Wksp.*, Piran, 2014, pp. 103–10.

[13] M. Shojafar, N. Cordeschi, and E. Baccarelli, "Energy-Efficient Adaptive Resource Management for Real-Time Vehicular Cloud Services," *IEEE Trans. Cloud Computing*, no. 99, 2016, pp. 1–1.

[14] M. Amadeo, C. Campolo, and A. Molinaro, "Priority-Based Content Delivery in the Internet of Vehicles through Named Data Networking," *J. Sensor and Actuator Networks*, vol. 5, no. 4, 2016, p. 17.

[15] F. Modesto and A. Boukerche, "A Novel Service-Oriented Architecture for Information-Centric Vehicular Networks," 19*th ACM Int'l. Conf. Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2016, pp. 136–39.

Biographies

Syed Hassan Ahmed [S'13, M'17] (s.h.ahmed@ieee.org) received his B.S. in computer science from Kohat University of Science and Technology, Pakistan. Later, he completed his combined Master's and Ph.D. in computer engineering from the School of Computer Science and Engineering, Kyungpook National University (KNU), Korea, in 2017. In 2015, he was a visiting researcher at the Georgia Institute of Technology, Atlanta. So far, he has published over 70 international journal and conference articles in addition to two Springer brief books. From 2014 to 2016, he won the Best Research Contributor award in the Workshop on Future Researches of Computer Science and Engineering, KNU. In 2016, he also won the Qualcomm Innovation Award at KNU. He is also an ACM member while serving several well reputed conferences and journals as a TPC member and reviewer, respectively. His research interests include sensor and ad hoc networks, cyber-physical systems, vehicular communications, and future Internet.

Safdar Hussain Bouk [SM'16] (bouk@knu.ac.kr) received his B.E. degree in computer systems from Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2001. He received his M.S. and Ph.D. in engineering from the Department of Information and Computer Science, Keio University, Yokohama, Japan, in 2007 and 2010, respectively. He worked as an assistant professor in the Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan, from 2010 to 2014. Currently, he is working as a research professor at KNU. His research interests include wireless ad hoc, sensor networks, underwater sensor networks, vehicular networks, and information-centric networks.

Dongkyun Kim [M'16] (dongkyun@knu.ac.kr) received his BS degree from the Department of Computer Engineering, KNU. He also received his M.S. and Ph.D. degrees from the School of Computer Science and Engineering, Seoul National University, Korea. He was a visiting researcher at the Georgia Institute of Technology, Atlanta, in 1999. He also performed a postdoctoral program in the Computer Engineering Department, University of California at Santa Cruz, in 2002. He has been on the Organizing Committees and Technical Program Committees of many IEEE or ACM conferences. He received the Best Paper Award from the Korean Federation of Science and Technology Societies, 2002. He has been involved in many editorial activities in several well-reputed international journals. Currently, he is a professor in the School of Computer Science and Engineering, KNU. His current research interests include connected cars, vehicular ad hoc networks, Internet of Things (M2M/D2D), Wi-Fi networks (including Wi-Fi Direct), wireless mesh networks, wireless sensor networks, and future Internet. He is the corresponding author for this article.

Danda B. Rawat [M'10, SM'13] (db.rawat@ieee.org) is an associate professor in the Department of Electrical Engineering & Computer Science and Founding Director of CWiNs Research Lab at Howard University, Washington, DC. His research focuses on wireless networks, cybersecurity, cyber-physical systems, Internet of Things, big data analytics, wireless virtualization, software-defined networks, and vehicular/wireless ad hoc networks. He is a recipient of an NSF Faculty Early Career Development (CAREER) Award. He has served as an Editor/Guest Editor for over 15 international journals, and has served on the Organizing Committees of several international conferences including IEEE INFOCOM 2015, 2016, 2017, and 2018, IEEE CCNC 2016, 2017, and 2018, and IEEE AINA 2015.

Houbing Song [M'12, SM'14] (Houbing.Song@mail.wvu.edu) received his Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, in August 2012. In 2017, he joined the Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently an assistant professor and the founding director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). In 2017 he began serving as an Associate Technical Editor for *IEEE Communications Magazine*. He was the very first recipient of the Golden Bear Scholar Award, the highest faculty research award at West Virginia University Institute of Technology in 2016.

IEEE Access®

The **journal** for rapid **open access** publishing

Become a published author in 4 to 6 weeks.

Get on the fast track to publication with the multidisciplinary open access journal worthy of the IEEE.

IEEE journals are trusted, respected, and rank among the most highly cited publications in the industry. IEEE *Access* is no exception with a typical **one-third** acceptance rate. Even though it provides authors faster publication time, every submitted article still undergoes extensive peer review to ensure originality, technical correctness, and interest among readers.

Published only online, IEEE *Access* is ideal for authors who want to quickly announce recent developments, methods, or new products to a global audience.

Publishing in IEEE *Access* allows you to:

- Submit multidisciplinary articles that do not fit neatly in traditional journals
- Reach millions of global users through the IEEE *Xplore*® digital library with free access to all
- Integrate multimedia with articles
- Connect with your readers through commenting
- Track usage and citation data for each published article
- Publish without a page limit for **only $1,750** per article

Learn more about this award-winning journal at:
www.ieee.org/ieee-access

IEEE
Advancing Technology for Humanity

14-PUB-196 11/15

A Buffer-Aware QoS Streaming Approach for SDN-Enabled 5G Vehicular Networks

Chin-Feng Lai, Yao-Chung Chang, Han-Chieh Chao, M. Shamim Hossain, and Ahmed Ghoneim

It is difficult to achieve quality of service and efficiency for multimedia streaming over vehicular networks because of the high mobility feature. It is also difficult to achieve quality of service and efficiency for multimedia streaming over vehicular networks because of the high mobility feature. The authors propose a buffer-aware streaming approach to allow users to play multimedia streaming over vehicular 5G networks.

ABSTRACT

With the progress of network technology in recent years, multimedia streaming applications have become increasingly popular. However, it is difficult to achieve quality of service and efficiency for multimedia streaming over vehicular networks because of the high mobility feature. Over the existing network architecture, it is difficult to immediately analyze the status of the entire network, and then establish the rules of allocation and management. However, the novel network architecture, software-defined networking, offers other options for making network management more efficient, especially for the 5G network environment. Hence, a buffer-aware streaming approach is proposed to allow users to play multimedia streaming over vehicular 5G networks, in the case of handover between different eNodeBs, to achieve minimum delay and have better quality of service. According to the user's mobility information, the status of the player buffer, and the current strength of the network signal, the proposed approach can provide the transmission strategy of multimedia streaming to the SDN controller. Finally, the experimental results proved that the proposed approach is able to not only adjust the priority of streaming content segments with the buffer and mobility status of user equipment to effectively retain overall streaming services quality, but also avoid the delay of streaming content transmission for 5G vehicular networks.

MOTIVATION

Many vehicle streaming services are based on the technologies of dynamic networking routing planning and preloading media content to regional servers [1, 2]. Vehicle streaming services may adopt the appropriate algorithm to evaluate multimedia content that should be preloaded by each regional server according to the user's mobility information. When users connect to the regional network, the reloaded content will be delivered from the regional servers for continued playback. In other words, the content is not required to be downloaded from the Internet to avoid the risk of network congestion. However, these methods require extra bandwidth and costs.

Fifth generation (5G) mobile communication is the next major phase of mobile telecommunications standards. Although there is currently no standard for 5G deployments, two common features can be found from the 5G white paper provided by many organizations:

1. Bandwidth improvement
2. High capacity for a large number of networking devices [3, 4]

In order to achieve the above two features, 5G communication use high-frequency signals to provide higher transmission speed, which makes the previous vehicle network streaming service no longer limited by the regional server architecture. Mobile devices are able to receive streaming content from cloud servers anytime and anywhere with 5G communication technology in order to save the cost of deploying the regional servers [5, 6]. However, the high-frequency signal transmission distance of 5G is short, which means that more eNodeBs (eNBs) will build to increase the communication signal coverage. This makes the scenario possible for mobile devices to pass through several eNBs while playing multimedia streams. When the user equipment performs handover between the eNBs, the base station must re-establish the connection for the user equipment, which causes extra latency to streaming services. The latency caused by such action depends on the network deployment scale and the current status of the network [7]. It also results in the delay time of switching eNBs being too long and degrades the quality of service (QoS). Therefore, to switch the eNB while ensuring QoS and maintain the overall network performance at the same time, it must have a different priority for different users or different services. But traditional switches do not guarantee the performance of data transmission at a certain level. For this reason, we adopt software defined networking (SDN), which separates the control plane and data plane from the switch to prevent the latency. Through SDN, the network manager can use the central control mode to plan the network dynamically without changing the hardware devices. SDN can also provide the corresponding quality of service for various applications.

Therefore, a buffer-aware QoS streaming approach over SDN-enabled 5G vehicular networks is proposed. By evaluating the direction and speed of user mobility, the strength of 5G network signals, and the amount of media content stored in the buffer to provide various priority levels of streaming service to users. In order to achieve this goal, the problem of

Digital Object Identifier:
10.1109/MCOM.2017.1601142

Chin-Feng Lai is with National Cheng Kung University; Yao-Chung Chang is with National Taitung University; Han-Chieh Chao is with National Dong Hwa University; M. Shamim Hossain is with King Saud University; Ahmed Ghoneim is with Menoufia University.

temporary disruption of the network caused by handover needs to be solved. As for the interruption caused by the handover, an adaptive handover mechanism is designed to allow the content to be buffered before the handover process so that the user does not need to receive the streaming content continuously during handover. Excepting the streaming priority adjustment, the prediction mechanism is also included to judge whether the user equipment may do the handover according to the current mobility information of the user and avoid misjudgment of unnecessary handovers.

Multimedia Streaming for SDN-Enabled 5G Wireless Networks

With increasing interest in the concept of next generation networks, mobile operators have been deploying heterogeneous networks to boost network capacity and coverage, allowing users to enjoy ubiquitous network services. Furthermore, in order to achieve better transmission efficiency, potential technologies for reconfigurable networks have been investigated, such as 5G wireless communication network and SDN, to build efficient network infrastructures [8, 9]. SDN is regarded as a revolutionary technology to virtualize networks for configuring and maintaining servers and routers easily that will likely play a critical role for designing 5G wireless communication networks [10–12]. As the concept for network virtualization, SDN presents a software layer to make network device adjustments through SDN defined interfaces instead of configuring hardware network devices manually [13–15]. Therefore, there are two planes in SDN network devices: the control plane, which determines where network packages are sent, and the data plane, which forwards network packages based on the control plane instructions.

This separation means that the network administrators no longer execute all the control rules on the physical network devices individually. In other words, the traditional network device is only designated to network package transmission in the data plane. The novel deployment of network services is not limited to the original network devices, and enables the switching/routing mechanism, traffic engineering, network optimization engineering virtualization, network functions virtualization, and other functions to achieve the networking advantages, such as agility and flexibility. SDN also establishes service level agreements (SLAs) for satisfying different service requirements. However, multimedia streaming, which is one of the most bandwidth-consuming services, is an emerging challenge, and researchers have been designing new architectures and mechanisms for providing a multimedia streaming mechanism on SDN-enabled 5G wireless networks. Therefore, a buffer-aware QoS streaming approach is proposed in this study for SDN-enabled 5G vehicular networks. It follows the previously proposed traffic engineering of SDN, and further discussion is presented on how to dynamically adjust the streaming mechanism by the SDN controller according to the buffer status of user equipment (UE) and 5G network traffic conditions.

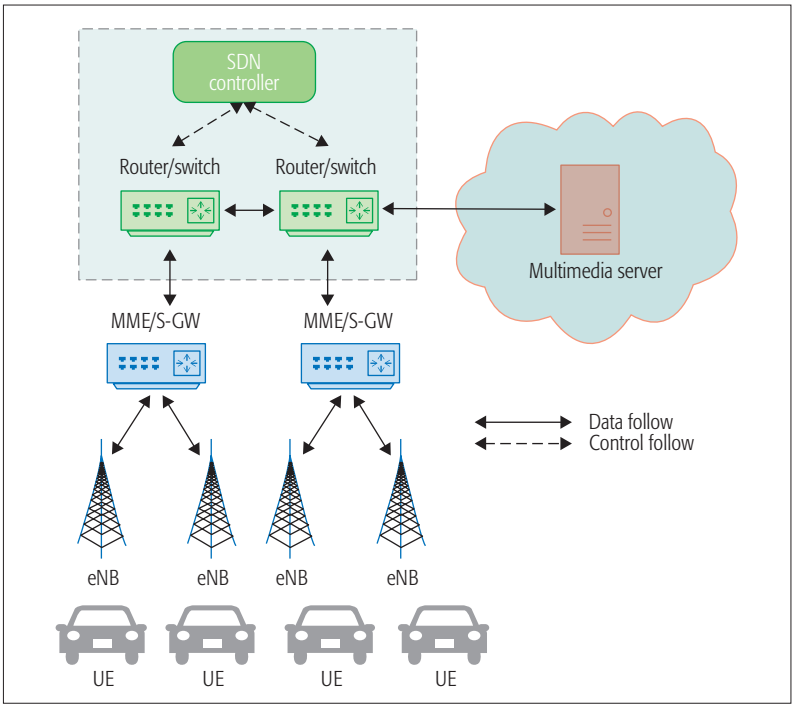


Figure 1. Proposed architecture.

A Buffer-Aware QoS Streaming Approach for SDN-Enabled 5G Vehicular Networks

In order to provide a streaming service on SDN-enabled 5G vehicular networks, a QoS dynamic multimedia streaming mechanism is designed. The main purpose is to solve the UE's handover latency caused by the problem of network connection delay and the quality of streaming services decreasing; the architecture is shown in Fig. 1. SDN is adopted to configure the network connection between the core network (e.g., the 5G core network) and the wireless base stations (e.g., eNBs). The SDN controller not only collects the real-time loading information of each eNB and the QoS requirements of the UE connected to each eNB, but also controls the network connection of each SDN switch for the wireless access configuration and bandwidth allocation. However, because the UE does not proactively report its status to the SDN controller, in order to achieve the approach proposed in this article, a network status report (NSR) module is installed on the UE. NSR will assess the direction of UE in the vehicle network and estimate the time UE will hand over after evaluating the application service packet received by UE and the connection signal strength of the eNB. The NSR communicates with the priority control function (PCF) of the SDN controller to get the necessary information of switching the network connection and transporting the prioritized data.

In the SDN architecture, in order to complete the eNB connection and network packet transmission of the UE, the PCF, which can be the application or bundle of the SDN controller, is used to control the SDN controller to send the command or obtain information from the SDN switches. The previously mentioned NSR and PCF

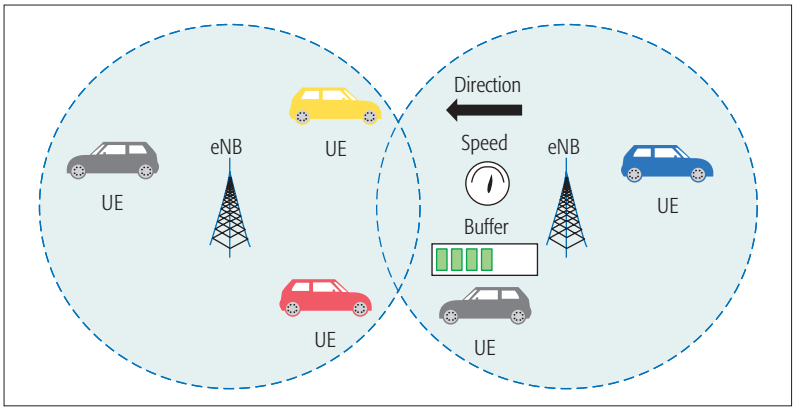


Figure 2. Vehicular handover scenario.

are installed on the UE side and the SDN network side to handle the access priority of wireless network bandwidth. With our proposed mechanism, the UE only needs to be an installed NSR module, and there no change should be made to the applications implemented on the UE originally. In other words, the applications can be used directly. When the UE initiates handover between the eNBs, the network connection latency will not meet the QoS requirement of multimedia streaming to UE. The proposed approach in this study provides the network handover time point and decision of transmission path configuration for an SDN to optimize the transmission efficiency according to the current network transmission performance and the service flow characteristics. When the eNB receives the request for multimedia streaming service from the UEs, the SDN controller will divide the UEs into several levels according to the current UEs' mobility status. The levels are used to allocate the priority of bandwidth usage and resource to the UEs through the network bandwidth evaluation by referring to the current UE priority level to allocate the appropriate bandwidth to each UE.

When the streaming content is transmitted to the user, the appropriate handover timing will be calculated using the parameters of the overlap range between eNBs, traveling speed, and so on, if the handover is about to be initiated on the UE, as shown in Fig. 2. The main purpose is to avoid the interruption caused by UE that initiates handover between eNBs. Therefore, two key factors are considered. One is the time of handover, evaluated by using the range of overlapping coverage of signals between eNBs; the other is the priority of streaming multimedia content evaluated by the buffer storage status of UE. Even with UEs able to have streaming services pre-download content in the buffer, even the network connection can be temporarily interrupted. At the same time, the SDN controller raises the content transmission priority to finally achieve streaming service QoS.

Control Plane

The control plane in SDN is mainly responsible for delivering information on mobility, identity authentication, and security. Therefore, the network control packets of the 5G architecture that go through the backhaul are the following: eNBs, the information of establishing a packet data transmission by a mobility management entity (MME), the heartbeat confirming the network link health status, and the attach procedure of initiating an attachment requirement to the eNB by the UE.

Data Plane

The data plane in SDN is used to transfer data packets for UEs. When UE is connected to the eNB, it is necessary to carry out identity authentication, key agreement, and other actions. After completing the actions, the home subscriber server assigns the corresponding QoS class identifier (QCI) to the data packets of different users or different application services of the same user. The value of QCI defines the transmission requirements, including the forwarding priority, the maximum delay, the acceptable number of lost packets, the guaranteed rate requirement, and so on. Therefore, the value of QCI can be identified to give the corresponding QoS when these data packets are transmitted in the backhaul.

Network Status Report Module

In the NSR, two parameters, time to trigger (TTT) and handover margin (HOM), are often used to evaluate the signal strength between the eNBs. TTT represents a time interval after the proposed approach archives the HOM condition, which is used to constrain the handover number within a specific time interval. HOM is a constant that represents a threshold for the difference in signal strength between the target eNB and the original eNB. Through HOM, the proposed approach can ensure that the UE can initiate handover to the appropriate target eNB. Therefore, the proposed approach can simultaneously use TTT and HOM to avoid the situation in which the UE initiates handover to the target eNB, then immediately back to the original eNB in a short time. When this above situation occurs, the proposed approach will additionally generate unnecessary operations while causing extra latency in the data transmission. When the UE is away from the eUB that is providing services, the reference signal received power (RSRP) value of the original eNB will begin to deteriorate, and the UE will be close to the target eNB at the same time, so the signal strength received from the target eNB will gradually become stronger.

$RSRP_T$ and $RSRP_O$ denote the received signal strength of the reference signal received by the UE from the target eNB and the original eNB, respectively. $Time_l$ denotes the time after the calculation begins to satisfy the first formula. The difference value of signal strength received by the target eNB and the original eNB can be divided into three parts. The first is the calculation of RSRP difference value, the second is the calculation of RSRP difference value filtered by the first formula, and the third is the handover decision made by the proposed approach. The RSRP difference value is calculated as follows:

$$Diff_{eNB}(t) = RSRP_T(t) - RSRP_O(t) \quad \text{where } RSRP_T > HOM + RSRP_O \tag{1}$$

$RSRP_T(t)$ and $RSRP_O(t)$ denote the received signal strength from the target eNB and the original eNB at time t, respectively. $Diff_{eNB}(t)$ denotes the received signal strength difference value of UE

served by the eNB. The RSRP difference value is calculated as follows:

$$FDiff_{eNB}(t) = \alpha * Diff_{eNB}(t) + (1 - \alpha) * Diff_{eNB}(t-1) \quad (2)$$
where $FDiff_{eNB}(t) > Diff_{Threshold}$

The α value is the forgetting factor. $FDiff_{eNB}(t)$, which denotes the received signal strength difference value after filtering by the second formula. The received signal strength difference value is determined by α, the ratio between the current received signal strength difference value and the received signal strength difference value at the last time point. When the value of α becomes closer to 1, it represents that the current signal intensity difference value has a higher specific gravity. On the other hand, when the value of α becomes closer to 0, it indicates that the received signal intensity difference value filtered by the second formula at the last time has a higher specific gravity. Finally, the condition in the proposed approach that decides whether to initiate handover is calculated as the following inequalities. Where $Diff_{Threshold}$ is a constant, the property is the same as HOM. When the received signal strength difference value is larger than $Diff_{Threshold}$ at time t, the proposed approach immediately determines to initiate handover.

Mobility Parameters

Regarding the calculation of mobility parameters, the moving state indicator (MSI) can be used to represent the mobile behavior between the eNB and the UE, which may be expressed by the following equation:

$$MSI_T = \frac{k_1}{(T-1)\Delta t}\left[10\frac{R(k_T)-R(k_1)}{10\alpha} - 10\frac{R(k_{T-1})-R(k_1)}{10\alpha}\right] \quad (3)$$

where Δt represents the sampling interval, and $R(k_1)$ is the value obtained at the past time point. As time passes, the received signal strength indicator (RSSI) will be continuously updated by $R(k_1)$, $R(k_{T-1})$, and $R(k_T)$. The MSI value may be provided to the UE regarding the relative motion direction and proximity ratio between the eNB and the UE. The relationship between the UE and the base station can be divided into two parts with the shortest distance (SD) if the mobility state of the UE is regarded as a straight line. When the UE moves in the direction of the SD point, the intensity of the received signal becomes stronger, and the MSI value will be negative.

On the contrary, when the UE is away from the SD point, the received signal strength will become weak, and the MSI value will be positive. For the same UE, if considering the SDs of two eNBs on this path route are different, the MSI value of the eNB with the shorter distance is relatively larger than the others.

Streaming Buffer Evolution

In order to effectively evaluate the connection condition between the UE and multimedia server, the UE buffer and overall transmission time are updated frequently. If the buffer is full, the transmission priority will be reduced; otherwise, the total streaming content is divided by the transmission time as the bandwidth information. Therefore, the SDN controller will contain the latest connection information between the UE and eNB.

When the SDN controller obtains the connection status of 5G vehicular networks, it is easy for the SDN controller to analyze the network condition, then prepare the appropriate bandwidth for further streaming transmissions. However, when the network condition may become unstable, the three modes are proposed to the UE for the various network conditions. The three buffer modes are normal mode, positive mode, and megative mode. The strategies of the buffer modes are described below:

- Normal mode: In this mode, the streaming content is received by the UE steadily and consistently. The streaming content in the UE buffer is often above the threshold, which makes the UE receive the streaming content with the connection bandwidth, and no connection information is updated to the SDN controller.
- Positive mode: The UE buffer is almost empty, and the UE compares the last bandwidth condition evaluated with the bandwidth condition currently evaluated to determine the trend of bandwidth variation in the next content transmission. If the trend is negative, the NSR will send the request of increasing the bandwidth to the PCF with time until the mode switches to normal mode, and the slope of change trend is multiplied by the remaining time, plus current average bandwidth.
- Negative mode: In this mode, the UE buffer is almost full. The NSR will send a request to decreasing the bandwidth to the PCF.

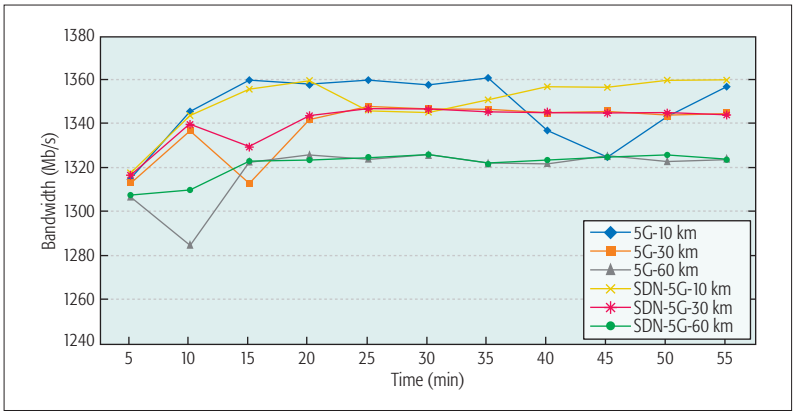


Figure 3. Bandwidth variation of UE in 5G Vehicular networks.

Evaluation

In order to implement experimental analysis of the overall 5G vehicular networks, eNB channel gains of 15 dBi are assumed static during a one-hop frame transmission, the bandwidth is limited as 1500 Mb/s, the media resolution is 1920 * 1080, and frames per second (FPS) is 30. In terms of the decision mechanism, this article carries out the bandwidth transmission rate and peak signal-to-noise ratio (PSNR) analyses for SDN-enabled 5G vehicular networks. Figure 3 shows the bandwidth variation of UE with fixed speed between the two eNBs at all time points; the blue, orange, and gray lines represent the bandwidth status of UE in 5G vehicular networks; and the yellow, red,

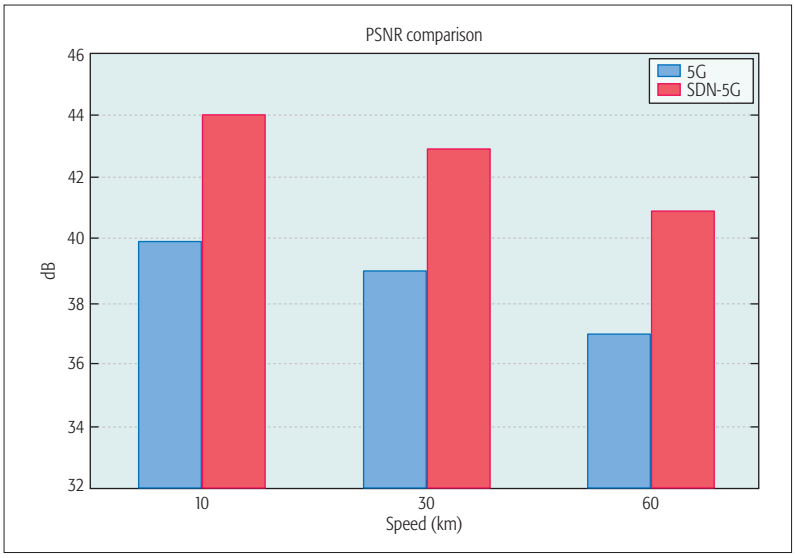


Figure 4. PSNR comparison in 5G vehicular networks.

and green lines represent the bandwidth status in SDN-enabled 5G vehicular networks. In the first 10-minute initialization phase, the handover of UE at 60 km/h is executed at the 10th second, and the bandwidth is dropped at the same time. A similar situation also occurs at the 15th and 45th seconds, meaning that streaming media cannot be completely downloaded, resulting in frame loss.

In terms of testing, this article analyzes PSNR streaming quality for vehicular networks testing scenario environments, and two decision mechanisms, including 5G vehicular networks and SDN-enabled 5G vehicular networks, as shown in Fig. 4. Since the streaming media cannot be completely downloaded within the handover, it results the frame loss and PSNR value decrease. In the result, we can find that the PSNR value in SDN-enabled 5G vehicular networks is higher than PSNR in 5G vehicular networks because the UE will send the handover message to the SDN controller that leads the SDN controller to immediately prepare the bandwidth from the connecting eNB for the UE.

Figure 5 shows the bandwidth variation and buffer size of UE with speeds of 10, 30, and 60 km/h, the blue, orange, and gray lines represent the bandwidth variation of UE in SDN-enabled 5G vehicular networks, and yellow, blue, and green bars represent the buffer size status. The bandwidth variation of UE is the same as in Fig. 3. Regarding buffer size, at the beginning of streaming, 2 is set as the buffer size threshold of the mode transition state machine, and the network behavior maintains the mode transition state machine in positive mode. After the streaming content achieves the buffer size threshold, the mode transition state machine is in normal mode. When the negative mode is entered as the bandwidth decreases, the behavior is consistent with the original behavior, and uses the maximum bandwidth configured by the SDN controller to choose the next media content; normal only uses the measured average bandwidth as the target bit rate.

In Fig. 6, the PSNR of the aforesaid scenarios is shown. We find that the PSNR value in SDN-enabled 5G vehicular networks is higher than PSNR in SDN-enabled 5G vehicular networks because the UE will send the handover message to the SDN controller, which leads the SDN controller to immediately prepare the bandwidth from the connecting eNB for the UE. It is observed that PSNR value with buffer in SDN-enabled 5G vehicular networks is higher than without buffer; that is, the media quality viewed by the user is on average better than the original mechanism.

Conclusions

In a 5G vehicular communication network, how to provide QoS multimedia streaming according to the network status is an interesting subject. In this study, a buffer-aware QoS streaming approach for SDN-enabled 5G vehicular networks has been proposed. The UE factors of mobility information and buffer status have been evaluated to control the streaming bandwidth priority based on the router management of the SDN controller and the handover prediction between eNBs. It makes the most suitable quality for the streaming services able to be determined. In the

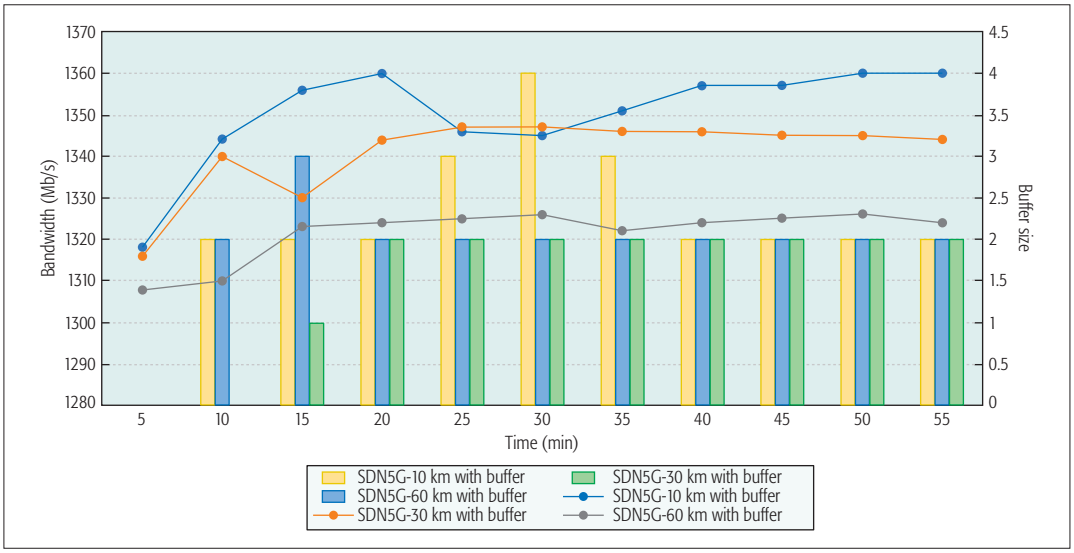


Figure 5. Bandwidth variation and buffer size of UE in SDN-enabled 5G vehicular networks.

experiment, the overall prototype architecture was realized, and an experimental analysis was carried out. According to the experimental results of this article, the bandwidth can be higher than 1280 Mb/s when the UE is handed over between the eNBs at a speed of 60 km/h, and the PSNR analysis shows that the streaming media quality can be increased by 3 dB. The experimental data proves that the method could maintain a certain level of streaming quality on SDN-enabled 5G vehicular networks and ensure smooth and complete streaming services.

Acknowledgment

Financial support for this work from the Ministry of Science and Technology, Taiwan (MOST 105-2221-E-143-001-MY2) is highly appreciated. The authors also extend their appreciation to the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, for funding this work through research group project no. RGP-229.

References

[1] Z He, J Cao, and X Liu, "SDVN: Enabling Rapid Network Innovation for Heterogeneous Vehicular Communication," *IEEE Network*, vol. 30, no. 4, July–Aug. 2016, pp. 10–15.
[2] Y. Pork, "A Feasibility Study and Development Framework Design for Realizing Smartphone-Based Vehicular Networking Systems," *IEEE Trans. Mobile Computing*, vol. 13, no. 11, Nov.2014, pp. 2431–44.
[3] W.-H. Chin, Z. Fan, and R. Haines, "Emerging Technologies and Research Challenges for 5G Wireless Networks," *IEEE Wireless Commun.*, vol. 21, no. 2, Apr. 2014, pp. 106–12.
[4] X. Wang *et al.*, "Cache in The Air: Exploiting Content Caching and Delivery Techniques for 5g Systems," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. 131–39.
[5] T. S. Rappaport *et al.*, "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!," *IEEE Access*, vol. 1, no. 1, May 2013, pp. 335–49.
[6] A. M. Akhtar, X. Wang, and L. Hanzo, "Synergistic Spectrum Sharing in 5G HetNets: A Harmonized SDN-Enabled Approach," *IEEE Commun. Mag.*, vol. 54, no. 1, Jan. 2016, pp. 40–47.
[7] X. Duan and X. Wang, "Authentication Handover and Privacy Protection in 5G HetNets Using Software-Defined Networking," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr. 2015, pp. 28–35.
[8] A. Khan, L. Sun, and E. Ifeachor, "QoE Prediction Model and Its Application in Video Quality Adaptation over UMTS Networks," *IEEE Trans. Multimedia*, vol. 14, no. 2, Apr. 2012, pp. 431–42.
[9] C.-F. Lai *et al.*, "A Network and Device Aware QoS Approach for Cloud Mobile Streaming," *IEEE Trans. Multimedia*, vol. 15, no. 4, May 2013, pp. 747–57.
[10] S. Y. Wu and C. E. He, "QoS-Aware Dynamic Adaptation for Cooperative Media Streaming in Mobile Environments," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 3, Mar. 2011, pp. 439–50.
[11] C. Xu *et al.*, "CMT-QA: Quality-Aware Adaptive Concurrent Multipath Data Transfer in Heterogeneous Wireless Networks," *IEEE Trans. Mobile Computing*, vol. 12, no. 11, Nov. 2013, pp. 2193–2205.
[12] G. Han *et al.*, "Two Novel DoA Estimation Approaches for Real Time Assistant Calibration System in Future Vehicle Industrial," *IEEE Systems J.*, 2015, DOI: 10.1109/JSYST.2015.2434822.
[13] X. Wang *et al.*, "Tag-Assisted Social-Aware Opportunistic Device-to-Device Sharing for Traffic Offloading in Mobile Social Networks," *IEEE Wireless Commun.*, vol. 23, no. 4, Aug. 2016, pp. 1536–84.
[14] C.-F. Lai *et al.*, "Cloud-Assisted Real-Time Transrating for HTTP Live Streaming," *IEEE Wireless Commun.*, vol. 20, no. 3, June 2013, pp. 62–70.
[15] Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2347–76.

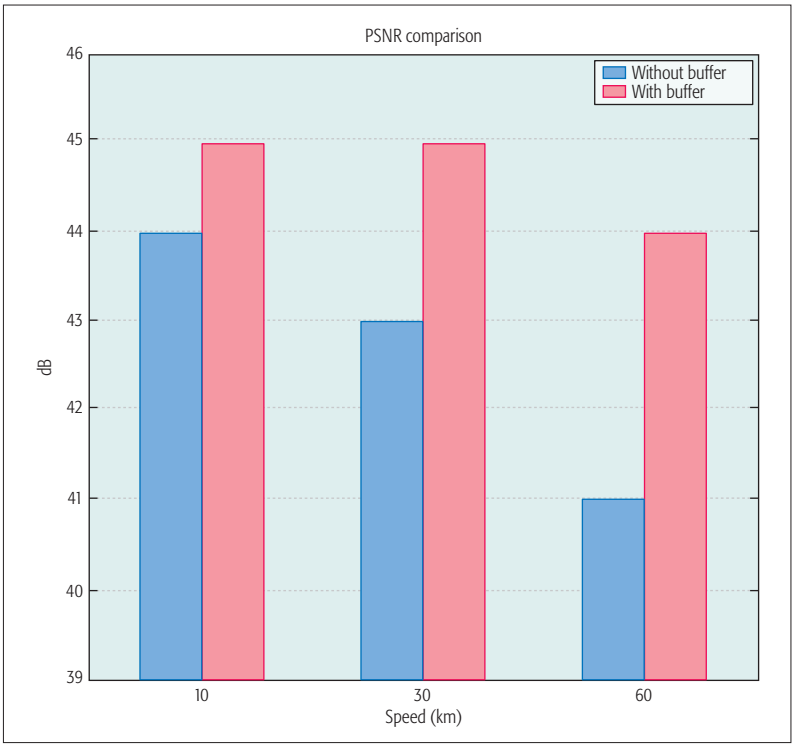


Figure 6. PSNR comparison in SDN-enabled 5G vehicular networks.

Biographies

Chin-Feng Lai [SM'14] has been an associate professor at the Department of Engineering Science, National Cheng Kung University since 2016. He received his Ph.D. degree from the Department of Engineering Science of National Cheng Kung University, Taiwan, in 2008. He serves as an Editor or Associate Editor for the *Journal of Internet Technology*, *IET Networks*, and *KSII Transactions on Internet and Information Systems*.

Yao-Chung Chang [M'03] received his Ph.D. degree from National Dong Hwa University, Hualien, Taiwan, in 2006. He serves as the Chair, Department of CSIE, National Taitung University, Taiwan. He is a recipient of the subsidization program in universities for encouraging exceptional talent, Ministry of Science and Technology, Taiwan, and is the author of more than 45 papers in international journals and conferences. His main research interests include mobile communication networks, IoT, and cloud computing.

Han-Chieh Chao [SM'92] is a joint appointedfull professor in the Department of Electrical Engineering, National Dong Hwa University, Taiwan. He is the Editor-in-Chief of *IET Networks*, the *Journal of Internet Technology*, the *International Journal of Internet Protocol Technology*, and the *International Journal of Ad Hoc and Ubiquitous Computing*. He is a Fellow of IET (IEE). He is a Chartered Fellow of the British Computer Society.

Mohammad Mehedi Hassan [M'12] is an assistant professor with the Information Systems Department at the College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He received his Ph.D. degree in computer engineering from Kyung Hee University, South Korea, in February 2011. His research interests include cloud collaboration, media cloud, sensor cloud, mobile cloud, IPTV, and wireless sensor networks.

Atif Alamri [M'12] is the chairman and an assistant professor of the Information Systems Department at the College of Computer and Information Sciences, King Saud University. He received his Ph.D. degree in computer science from the University of Ottawa, Ontario, Canada, in 2010. His research interest includes multimedia assisted health systems, ambient intelligence, wireless sensor networks, and distributed computing.

Vehicle Software Updates Distribution with SDN and Cloud Computing

Meysam Azizian, Soumaya Cherkaoui, and Abdelhakim Senhaji Hafid

The authors propose an architecture for distributing software updates on vehicles based on software defined networking and cloud computing. They show that using SDN, the emergent networking paradigm, which provides on-demand network programmability, adds substantial flexibly for deploying software updates on vehicles.

ABSTRACT

Vehicles have embedded software dedicated to diverse functionality ranging from driving assistance to entertainment. Vehicle manufacturers often need to perform updates on software installed on vehicles. Software updates can either be pushed by the manufacturer to install fixes, or be requested by vehicle owners to upgrade some functionality. We propose an architecture for distributing software updates on vehicles based on SDN and cloud computing. We show that using SDN, the emergent networking paradigm, which provides on-demand network programmability, adds substantial flexibility for deploying software updates on vehicles. We propose solutions for how vehicular networks can be modeled as connectivity graphs that can be used as input for the SDN architecture. After constructing graphs, we present an SDN-based solution where different frequency bands are assigned to different graph edges to improve the network performance.

INTRODUCTION

Vehicular technology has evolved tremendously during the last 15 years, making vehicles safer, more intelligent, and more pleasant to drive. These advancements have been made possible by embedding intelligence within onboard systems through extensive software coded features. With the role played by software ever expanding in modern vehicles, a new challenge has emerged. Manufacturers are facing the necessity to upload software updates into vehicles either to fix bugs or to improve existing functionality. To do so, customers are usually required to go for service at their dealers. A single trip for service can be inconvenient for customers, but as software components become preponderant in vehicles and the need for updates more frequent, this can become impractical. Recently, several manufacturers have shown interest in new ways of uploading software updates over the air through either Wi-Fi, cellular, or satellite connections. They envision that vehicles will eventually become serviceable remotely just like smartphones are now, with fixes, updates, and new features added over the air.

Ford, which previously delivered updates to its infotainment system with physical USB uploads, has geared up to using Wi-Fi Internet connections for its recent models, and plans to use satellite connections in the future. To download an update, vehicles need to be in range of a Wi-Fi access point at home or elsewhere for the duration of the software upload. Often, this may be either infeasible or impractical. For another manufacturer, Tesla, vehicles receive software update notifications to add new features and functionality over cellular connections. However, the manufacturer advises owners to use Wi-Fi for faster downloads.

With vehicular dedicated short-range communications (DSRC) [1] expected to be available in vehicles very soon, a new opportunity arises to dynamically update software on vehicles by using vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Apart from DRSC, LTE-Direct, which has been in development in recent years in fourth and fifth generation (4G/5G) fora, is also a promising technology for V2V communications in future. In this article, we show how software defined networking (SDN), paired with vehicular communications and cloud computing, can be used to add substantial flexibility for deploying software updates on vehicles. This flexible programmability can be very useful for deploying non-critical software updates (e.g., infotainment) on the fly, without the need to go for service.

SDN has emerged as a powerful networking paradigm that can provide scalable and flexible means to manage networks. With SDN, new protocols can be deployed easily, and a broad spectrum of embedded networking functions modified and manipulated. SDN decouples the data plane and the control plane so that forwarding functions and network functions are dissociated. An SDN-based architecture is composed of two main components: the SDN controller and SDN devices. The SDN controller, as the logically centralized intelligence of the SDN network, can control programmable SDN devices' behavior through a standardized southbound interface protocol called OpenFlow. SDN makes it possible to have unified management of different types of SDN devices regardless of the SDN device vendor [2]. This powerful paradigm works in a simple way. Each SDN device has a flow table with several fields specifying how an incoming packet should be treated. The SDN controller modifies flow tables either proactively, depending on application layer needs and network topology, or reactively, based on traffic-dependent on-demand requests from SDN devices. SDN devices transfer packets based on polices dictated to each of them from the SDN

Digital Object Identifier:
10.1109/MCOM.2017.1601161

Meysam Azizian and Soumaya Cherkaoui are with the Univeristy of Sherbrooke; Abdelhakim Senhaji Hafid is with the University of Montreal.

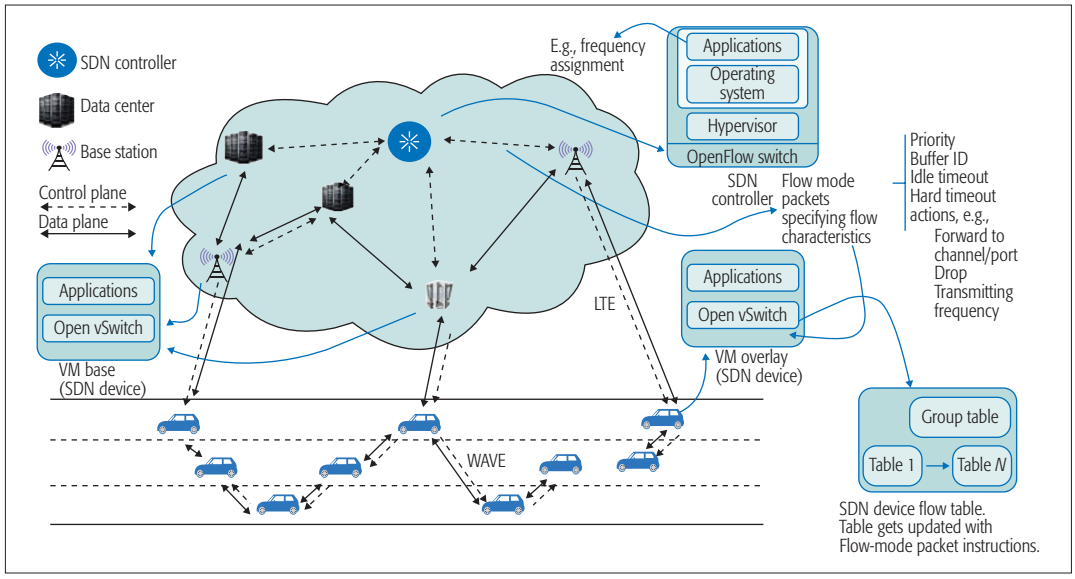


Figure 1. SVC system architecture. The SDN controller instructs all SDN devices (switches) on how flows should be treated.

controller, which has global knowledge about SDN devices; hence, there is no need for hardware configuration.

In order to deploy software updates on vehicles, we propose an SDN-based vehicular cloud architecture (SVC) that leverages V2V communications. In SVC, vehicles are considered SDN devices, and SDN controllers can be located on roadside units (RSUs) or base stations (BSs), reside at the edge of the network, or be located at servers in a data center. Software update using SVC can be considered as a way to leverage SDN for deploying the future Internet of Things (IoT) [3]. V2V communication allows vehicles to cooperate in software update distribution in a similar way to device-to-device (D2D) cooperation. Using SDN with vehicular communications poses two important challenges, though. First, different from wired networks, vehicular networks are prone to frequent topology changes as vehicles move close to/away from each other. A swift and autonomous neighbor discovery mechanism needs to be devised to allow the SDN controller to acquire and maintain a global view of network topology. To address this, we propose a solution to construct vehicles' connectivity graphs based on standard vehicular beaconing conveying position information among vehicles. Vehicles communicate with each other in a distributed way and provide connectivity information to the SDN controller, which constructs the connectivity graphs. Second, V2V communication is known to suffer considerably from interference and hidden node problems. In order to mitigate these problems, we propose that the SDN controller, as a centralized manager of the network, execute a novel scheme that uses mathematical optimization to assign different operating frequencies to vehicles (SDN devices). The frequency assignment makes it possible for vehicles to communicate in the data plane in a multihop manner while fully resolving the hidden node problem. Furthermore, the scheme allows co-channel and adjacent channel interferences to be sizably reduced.

System Architecture and Assumptions

In SVC architecture, we suppose that vehicles, which are SDN devices, are equipped with OpenFlow-capable software switches such as Open vSwitch. We also suppose that SDN devices are capable of virtualization and can host virtual machines (VMs). A VM will be able to install software updates on the vehicle. Here, a software update is considered as a service. When a vehicle is interested in the software update service, the vehicle VM will be replicated at the nearest datacenter which offers that service [4, 5]. RSUs, BSs, and other edge equipment can host micro-data centers and participate in fog computing [4] to deliver services, including software updates to vehicles. They can also be SDN devices or host SDN controllers. The vehicle VM and data center VMs are named VM overlay and VM base, respectively [6]. A VM overlay migrates to other nearby VM bases when it is close to moving out of the communication range of the current VM base. The SDN controller is responsible for managing these VM replications and migrations. SDN controllers are located in some of the data centers or edge equipment, and are connected with RSUs, BSs, and other data centers, which form a cloud together [7]. Therefore, the control plane decisions are not entirely made by a centralized element; several cloud elements can collaborate to make decisions. Figure 1 illustrates SVC architecture.

In SVC, vehicles are equipped with V2V communication technology, and some vehicles may have LTE connections. Vehicles that have LTE connections or are in the communication range of infrastructure elements (e.g., RSUs) transfer the information about their connectivity with other vehicles to the SDN controller. The SDN controller uses this information to construct the vehicles' connectivity graph model in order to update flow tables and allocate frequency bands. DSRC designates four 10 MHz frequency bands, called service channels (SCHs), to be used for service data communications. These frequency bands will be allocated by the SDN controller for SDN data plane software update transfers. One of these fre-

SDN-controllers are located in some of the data centers or edge equipment, and are connected with RSUs, BSs and other data centers which form a cloud together. Therefore the control plane decisions are not entirely taken by a centralized element; several cloud elements can collaborate to take decisions.

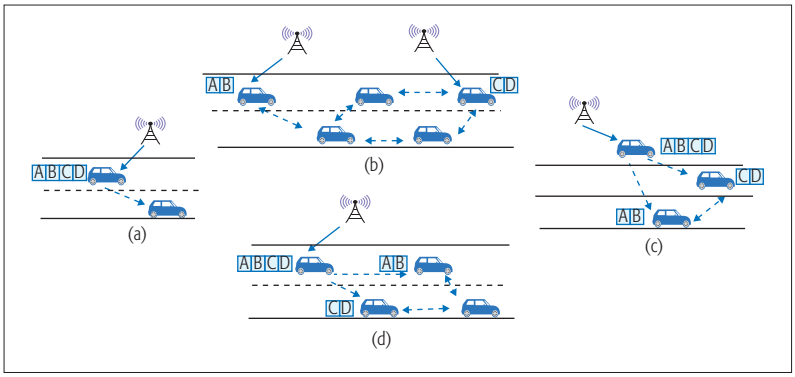


Figure 2. Content distribution: a) the left-most vehicle receives the content $[A|B|C|D]$ and shares it with the neighbor vehicle; b) the left-most and right-most vehicles receive half of the content and share it with their neighboring vehicles. In c) and d), the left side vehicles receive the content and split it before delivery to neighbors. In the aforementioned cases, vehicles collaborate with each other to get the complete content based on the provided instructions from the SDN controller. Therefore, software update distribution with SDN improves network performance by decreasing both used cellular bandwidth and the corresponding usage fee (and also DSRC bandwidth), and software update delivery delay.

quencies is also chosen as the de facto frequency for SDN control plane signalling.

As input to the connectivity graph calculation and frequency assignment, the SDN controller receives information from vehicles regarding their location, received power, and relative mobility with their neighbors. This information can be obtained by each vehicle using standard safety message beacons exchanged in the DSRC control channel (CCH) [1]. Vehicles use the SDN control plane to convey this information to the SDN controller either directly or in a multihop manner.

SDN devices have flow tables, and the SDN controller updates these tables in the control plane via flow-mode packets in order to route software updates to interested vehicles. Service (software updates) advertisement happens in a CCH period as specified by the WAVE standard. Therefore, whenever an update is available and a vehicle is interested, it switches to the SDN control plane signaling channel to send information and receive flow table updates from the SDN controller.

The SDN controller updates the flow tables regularly following a change in topology to avoid the connection loss while a vehicle is receiving a service. However, when the SDN controller cannot update switches due to unexpected situations (e.g., sudden speed change of vehicles or communication problems due to channel fading), vehicles temporarily use other routing protocols, such as general packet switched radio (GPSR), as a backup to avoid connection loss [8]. The occurrence of flow table updates is decided by the SDN controller based on the stability of the constructed graphs. The SDN controller estimates the stability of the constructed graphs by measuring relative mobility between vehicles, and updates the flow tables based on that estimation.

Connectivity Graph Model

To construct the connectivity graph model, SDN controllers need vehicle positions and their calculated relative mobility. To calculate relative mobility, we use a similar method to the one proposed in [9]. Each vehicle calculates the delays of two consecutive standard beacons received from a neighbor to determine the relative mobility with that neighbor.

The use of beacon delays as a metric to calculate the relative mobility is superior to other metrics such as speed or position. Indeed, other metrics may not clearly represent channel conditions such as fading or communication obstacles. For example, two neighbor vehicles in nominal communication range may have almost the same speed, but the channel condition between the two might be highly faded; this can make it impossible for them to communicate.

Each vehicle encapsulates its coordinates and transmission time in standard beacon messages. Therefore, the receiving vehicle can know the transmitter location and calculate the delay of transmission. A vehicle can calculate the relative mobility of a neighbor when it receives the second beacon message from that neighbor. Therefore, each vehicle can construct relative mobility tables and send them to the SDN controller via the control plane, directly or in a multihop manner; this information can be appended to beacon messages to avoid extra messages. Relative mobility is calculated at each node using a logarithm form function represented as: 10 multiplied by log base 10 of (x/y), where the nominator, x, is the new calculated beacon delay, and the denominator, y, is the old calculated one.

After receiving relative mobility information, the SDN controller constructs the directed connectivity graph model. In the graph, each edge represents a connection from one vehicle to another, while vertices represent vehicles. For each edge, the SDN controller examines the corresponding relative mobility value. The SDN controller compares the relative mobility value with a threshold to see if it is strong enough to be considered as a communication link. When communication links have been determined, the SDN controller calculates the routes and updates the corresponding flow tables of SDN devices. Based on the relative mobility corresponding to each edge in the graph, the SDN controller also decides on the frequency for updating flow tables and assigning channels.

For route calculation, and content distribution, the SDN controller can follow several strategies. When a software update is not in high demand, such as a paid new feature, the SDN controller can route the update directly to the interested vehicle using the shortest path. When the software update is popular, the SDN controller can orchestrate delivery by determining clusters of interested vehicles. In each cluster, each vehicle receives part of the software update, and they cooperate to assemble it [10]. This is illustrated in Fig. 2. Another interesting technique the SDN controller can use is distributed caching [11]. Indeed, when a software update is available, it is likely to be requested by a large number of vehicles of the same make. Distributed storage of these updates enhances the opportunities for vehicles' collaboration to access the software update solely through V2V communication.

It is worth noting that the proposed connectivity graph model calculation can be enhanced by using other data. In addition to standard information available from beacons, several other parameters could potentially be used, when available, to construct the connectivity graph and improve its

stability. Examples of these parameters include the estimated vehicle trajectory, which can be acquired from the vehicle navigation system, real-time traffic conditions of roads, and travel history of vehicles. However, these data might not always be obtainable. Furthermore, using such extra parameters can come at the expense of extra overhead.

Frequency Assignment

V2V communication is prone to interference and hidden node problems, which cause frequent collisions in the communication channel. Collisions at the medium access control (MAC) layer cause higher delays and lower throughputs. In order to mitigate these problems, we propose that the SDN controller assign to vehicles (SDN devices), different operating frequencies to be used in the data plane.

Once the connectivity graph model is constructed, it can be used by the SDN controller to assign different frequency bands to be used by vehicles for communicating over the different edges of the constructed graph. The SDN controller, with its global view on the network, plays a centralized controller role in assigning different frequencies to vehicles in order to degrade interference levels and solve hidden node problems.

The SDN controller assigns frequencies in such a way that no two neighbor edges in the nominal communication range of each other use the same frequency band. Therefore, co-channel interference will be highly degraded for dense vehicle situations, or even eliminated in spare network conditions. Also, the SDN controller takes care of adjacent-channel interference by carefully choosing frequencies and assigning them to non-adjacent edges. Hence, adjacent channel interference will similarly be reduced, even if some of this interference is inevitable in highly dense scenarios.

The proposed frequency assignment scheme used by the SDN controller is based on a mathematical optimization model using binary integer programming (BIP). The mathematical optimization model calculates the maximum number of edges (i.e., transmission links) that can transmit (be activated) simultaneously in a single frequency band. The frequency assignment scheme uses the optimization model to recursively assign different frequency bands to different edges.

Optimization Model

As input to the optimization problem, the SDN controller uses the knowledge acquired through constructing the connectivity graph model. The input dataset comprises:

1. The power matrix representing the power received by each node from its neighbors
2. The edge matrix of the connectivity graph
3. The path matrix of the chosen paths toward the vehicle

In order to assign frequencies for different edges, the power matrix representing the received power by each node has to be examined. When vehicles are operating in the same frequency, communication over each edge is potentially interference to communications in other edges. The power matrix is therefore used to calculate the signal-to-interference-plus-noise ratio (SINR) on each edge. An edge in the connectivity graph can be active when the SINR of that edge is adequate; that is, it must pass a minimum threshold value to be considered for activation.

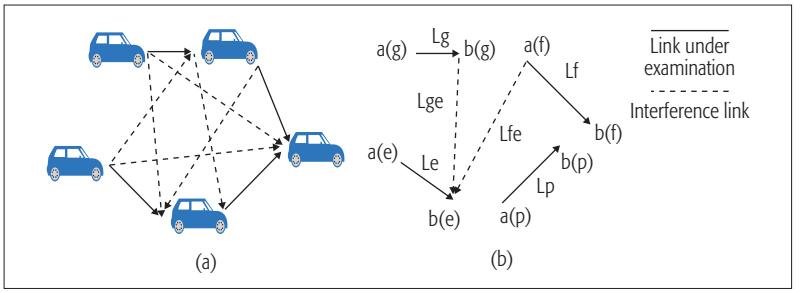


Figure 3. Co-channel interference modeling: a) edges in bold are links under examination by the SDN controller, the others are interference; b) illustration of the effect of interference on a link under examination by the SDN controller.

We write the optimization model as a BIP optimization where all variables are binary. The objective of the model is to find the maximum number of edges that can be active simultaneously in the same frequency. The edges in the objective are the ones that cause the minimum co-channel radio interference to each other. Therefore, the objective function to maximize can be represented as the sum of all edges, where edges are binary variables holding values zero or one, as in [12, Eq. 3]. An edge is assigned value one if it is active, and value zero otherwise. Maximizing the objective function is subject to three constraints.

The first constraint ensures that a vehicle can either transmit or receive at the same time. Therefore, only one edge can be activated at each node; this constraint is represented in in [12, Eq. 4]. The second constraint ensures that an edge can only be activated when the corresponding vehicle is transmitting; we assign value one to the binary variable of the vehicle when it is transmitting and zero otherwise; this constraint is represented by [12, Eq. 5]. The last constraint verifies that the SINR of an edge is strong enough to be considered for activation. *Signal* here stands for the signal strength of an edge under examination. *Interference* is signals from other interfering edges. *Noise* is noise power density. This constraint is represented in [12, Eq. 8]. Figure 3a shows an example of how co-channel interference affects communication links. Figure 3b illustrates the effect of interferences on a link of under examination (Le). We use the branch and bound method to solve this optimization model.

Assignment Scheme

In the DSRC standard, six channels are reserved for services [1]. However, only four of these channels (channels 174, 176, 180, and 182) are dedicated to general-purpose service use. The two remaining channels (channels 172 and 184) are reserved for "public safety applications involving safety of life and property" [13].

The proposed frequency assignment scheme uses the previously presented optimization model in successive rounds, up to four, based on the maximum number of frequency bands available in DSRC. The number of rounds can be less than four if vehicle density is low, and little interference exists. Each round comprises several steps.

First round:

Step 1: The SDN controller executes the optimization model and determines a set of edges that can transmit concurrently without interfering with each other.

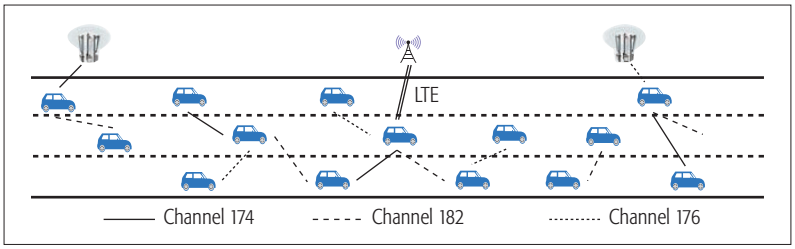


Figure 4. Frequency assignment example. The links assigned to channels 174,182, and 176 are calculated though the first, second, and third rounds of the proposed frequency assignment scheme, respectively. There is no need to proceed to the fourth round as the first three channels can cover the graphs' edge. The graphs are modeled through the proposed graph connectivity scheme.

Step 2: The SDN controller assigns the first channel, channel 174 (5.865 to 5.875 GHz), to this set of edges.

Step 3: The determined set of edges are removed from the input of the optimization model for the next round. This is done by setting the powers of those edges to zero in the new input power matrix.

After the frequency assignment of the first round, it is probable that some edges will be left without frequency assignment. This can be explained by two reasons:

1. Edges sharing the same vertex cannot be activated in the same round (i.e., assigned the same frequency).
2. An edge may have too low an SINR to be activated; some links need to be assigned a different frequency in order for the SINR to become high enough and the link activated in the second stage.

Second round: For the second time, the SDN controller executes the optimization model with the modified data set and gets a new set of edges (first step). This time, the SDN controller assigns channel 182 (5.905 to 5.915 GHz) to the generated set (second step). The reason for choosing this channel is to address adjacent channel interference: no neighbor frequency with the already assigned frequencies. Similar to the first round, the SDN controller updates the input dataset for the next round (third step).

Third round: If some edges are left without frequency assignment in the second round, they are considered in the third round. The round follows the same steps as in the second round with the difference that the assigned frequency band is that of channel 176 (5.875 to 5.885 GHz).

Fourth round: In this round, all edges that remain without frequency assignment in the third round are assigned to operate in channel 180 (5.895 to 5.905 GHz) without following any extra steps. The scheme stops proceeding here, as this is the last frequency band left. Vehicles operating in channel 180 simply use carrier sensing and random backoff delays to avoid collisions as specified in the WAVE standard. Figure 4 shows a vehicular network example where communication links have been assigned different frequency bands based on the proposed scheme.

With the proposed frequency assignment scheme, collisions and interference are reduced in the wireless medium. Therefore, the delay for vehicles to receive their services (software update) is shortened. Figure 5 shows a comparison in terms of the average delivery delay when using multiple frequencies assigned in SVC, and a scheme where vehicles use WAVE with the same DSRC frequency. In the simulations, all vehicles receive the software updates from their nearest data center.

With SVC, the average delay is smaller than with WAVE. This can be explained by several factors, including:

1. Vehicles using WAVE cause more mismanaged interference with each other.
2. Route discovery takes more time with WAVE alone than with SVC, and route recalculation is more frequent with WAVE alone.
3. The hidden node is more frequent with WAVE alone, causing collisions and retransmission delays.

Figure 5 shows that the delay gap between WAVE and SVC increases as the network gets denser. This is expected as the aforementioned problems get worse when density increases. Having a centralized SDN controller improves network performance by carefully managing interference, solving hidden node problems, and assigning adequate flow tables to SDN devices.

Open Research

Some fundamental and interesting research issues are still open to be able to fully realize the promise of the proposed SDN architecture. We have identified some of these areas that need particular attention from both academia and industry.

Incentives for Vehicles: Some incentives should be given to motivate vehicles that use their cellular networks to transfer neighbors' information to SDN controllers. Examples of these incentives include discounts on service, higher bandwidth [14], or free cellular connectivity. Similar kinds of incentives can be given to vehicles to encourage them to cooperate in content delivery (caching, etc.).

Quality of Service Satisfaction: Following frequency assignment, the SDN controller can optimize transmission scheduling in SVC based on several criteria including fairness or service differentiation. Both issues of fairness and service differentiation should be fully investigated given the scarcity of vehicular networking resources and the variety of software installed on vehicles. Fairness can relate to all vehicles having their fair amount of usage of network resources to receive software updates. The SDN controller can also consider different priorities for software updates, translating into different quality of service (QoS) needed for delivery. For example, a safety-related update can be prioritized over a software update that enhances infotainment system features.

Security Considerations: As the SDN controller in SVC has a global view over the SDN network, the network can be secured by re-instructing the SDN device flow tables at any time to mitigate an anomaly (e.g., instructions to drop some packets). The anomaly can be identified by the SDN controller security applications, based on the collected information from the SDN devices. However, security threats in SVC should be fully analyzed to design the corresponding security applications or even to restructure the proposed architecture. Several applications have already been proposed to deal with the security threats

of SDN architectures in general [15]; these applications can be adapted to be used in SVC. Some example of threats can be:

1. Attacks on the SDN controller may lead to the attacker controlling SDN devices' behavior in the data plane by manipulating flow rules.
2. Misbehavior of a cloud element: Since the SDN controller collaborates with cloud elements to define the control plane rules and make decisions, the cloud elements involved should be trusted.
3. Misbehavior of SDN devices: SDN devices that relay flow rules can be intelligently subversive and manipulate flow instructions.

There should be procedures for SDN devices to check the credibility of the received flow instructions.

Conclusion

In this article, we advocate for an architecture using SDN, cloud computing, and vehicular communications to distribute software updates to vehicles, and we show how such an architecture takes shape in SVC. SVC leverages vehicular communications and salient SDN features to distribute software updates in a flexible way to vehicles that need fixes or new features. SVC efficiently uses V2V beaconing information to construct the graphs needed by SDN controllers to control the network in a systematic way. SVC further makes effective use of networking resources by orchestrating channel use among participating vehicles. Some open issues make particularly interesting research topics to investigate in the future, including incentivizing vehicles to cooperate and bolstering the architecture with security features.

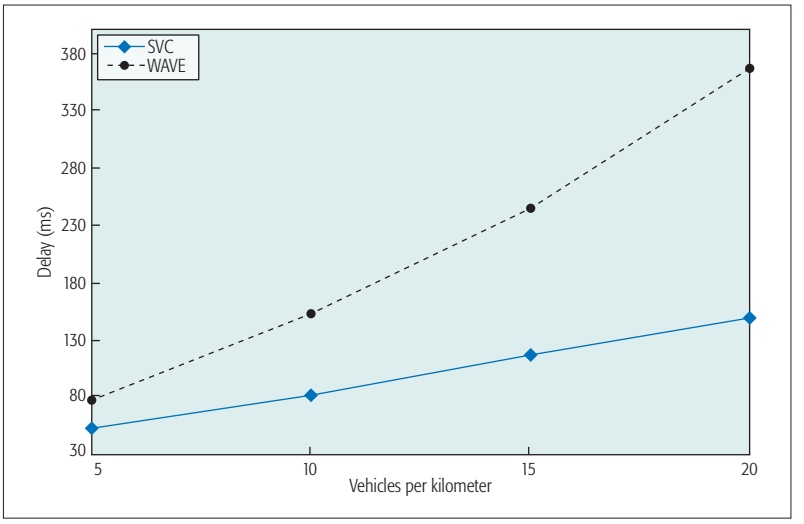


Figure 5. Comparison between SVC and using WAVE alone. The simulation scenario uses a four-lane highway with different vehicle densities. The maximum velocity of vehicles is 25 km/h. The data rate and transmission power for all vehicles are fixed to 6 Mb/s and 20 dBm, respectively. When using WAVE alone, the routing method used is ad hoc on-demand distance vector.

References

[1] R. A. Uzcátegui and G. Acosta-Marum, "WAVE: A Tutorial," *IEEE Commun. Mag.*, vol. 47, no. 5, May 2009, pp. 126–33.

[2] Z. He, J. Cao, and X. Liu, "SDVN: Enabling Rapid Network Innovation for Heterogeneous Vehicular Communication," *IEEE Network*, vol. 30, no. 4, July 2016, pp. 10–15.

[3] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 3, 2015, pp. 2347–76.

[4] M. A. Salahuddin *et al.*, "RSU Cloud and Its Resource Management in Support of Enhanced Vehicular Applications," *IEEE GLOBECOM Wksp. Cloud Computing Systems, Networks, and Applications* , 2014, pp. 127–32.

[5] N. B.Truong, G. Lee, and Y. Ghamri-Doudane, "Software Defined Networking-Based Vehicular Adhoc Network with Fog Computing," *IFIP/IEEE Int'l. Symp. Integrated Network Management*, 2015, pp. 1202–07.

[6] R.Yu *et al.*, "Toward Cloud-based Vehicular Networks with Efficient Resource Management," *IEEE Network*, vol. 27, no. 5, Sept. 2013, pp. 48–55.

[7] Y. Xu and S. Mao, "A Survey of Mobile Cloud Computing for Rich Media Applications," *IEEE Wireless Commun.*, vol. 20, no. 3, June 2013, pp. 46–53.

[8] I. Ku *et al.*, "Towards Software-Defined VANET: Architecture and Services," *IEEE Int'l. Wksp. Mediterranean Ad Hoc Networking*, 2014, pp. 103–10.

[9] Z. Zhang, A. Boukereche, and R. Pazzi, "A Novel Multi Hop Clustering Scheme for Vehicular Ad-Hoc Networks," *ACM Int'l. Symp. Mobility Management and Wireless Access*, 2011, pp. 19–26.

[10] Y. Cao, J. Guo and Y. Wu, "SDN Enabled Content Distribution in Vehicular Networks," *13th IEEE Int'l. Conf. Innovative Computing Technology*, 2014, pp. 164–69.

[11] N. Golrezaei, P. Mansourifard, and A. F. Molisch, "Base-Station Assisted Device-to-Device Communications for High-Throughput Wireless Video Networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, 2014, pp. 3665–76.

[12] M. Azizian, S. Cherkaoui, and A. Senhaji Hafid, "A Distributed Cluster Based Transmission Scheduling in VANET," *IEEE ICC*, 2016.

[13] "FCC Code of Federation Regulations 47, Part 95," Personal Radio Services, 2009.

[14] H. Li, M. Dong, and K. Ota, "Control Plane Optimization in Software-Defined Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 10, 2016, pp. 7895–7904.

[15] I. Ahmad, S. Namal, and M. Ylianttila, "Security in Software Defined Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2317–46.

Biographies

Meysam Azizian received his M.Sc. degree in radio communication from Blekinge University, Sweden, in 2013. In 2012, he was a degree project student with the Department of Electric and Information Technology, Lund University. He is currently pursuing a Ph.D. degree in electrical and computer engineering with the INTERLAB, Université de Sherbrooke, Quebec, Canada. His current research interests are vehicular cloud computing, SDN, and resource sharing.

Soumaya Cherkaoui [M'99, SM'15] is a professor at the Department of Electrical and Computer Engineering, Université de Sherbrooke. Since 2000, she has been the director of Interlab, a research laboratory that conducts research funded by both government and industry. Before joining the Université de Sherbrooke as a faculty member, she worked for industry as a project leader on projects for the aerospace industry. She has co-authored over 200 publications in reputable journals and conferences in the area of communication networks. She has served as a General Chair, Technical Committee Chair, and Editor of many conferences and journals. She is a Professional Engineer in Quebec, Canada.

Abdelhakim Senhaji Hafid is a full professor at the University of Montreal, where he founded the Network Research Lab (NRL) in 2005. He is also a research fellow at CIRRELT. Prior to joining the University of Montreal, he spent several years as a senior research scientist at Telcordia Technologies (formerly Bell Communications Research), New Jersey, working on major research projects on the management of next generation networks including wireless and optical networks. He has extensive academic and industrial research experience in the management of next generation networks, QoS management, and communication protocols.

Enhancing Crowd Collaborations for Software Defined Vehicular Networks

Wei Quan, Yana Liu, Hongke Zhang, and Shui Yu

The authors investigate a new smart identifier networking (SINET) paradigm and propose a SINET customized solution enabling crowd collaborations for software defined vehicular networks (SINET-V). In particular, through crowd sensing, network function slices are well organized with a group of function-similar components. Different function slices are further driven to serve various applications by using crowd collaborations.

ABSTRACT

Vehicular networking is promising to improve traffic efficiency and driving safety, as well as travel experience. However, the traditional network employs a highly coupled design, which is quite limited in its ability to satisfy various challenging vehicular demands. Recently, new studies focus on how to design software defined vehicular networks smartly to meet various vehicular demands. In this article, we investigate a new smart identifier networking (SINET) paradigm and propose a SINET customized solution enabling crowd collaborations for software defined vehicular networks (SINET-V). In particular, through crowd sensing, network function slices are well organized with a group of function-similar components. Different function slices are further driven to serve various applications by using crowd collaborations. We clearly illustrate how SINET-V works and also analyze its potential advantages in several special vehicular instances. Experimental results show that SINET-V has great potential to promote powerful vehicular networks.

INTRODUCTION

Vehicular networking has been paid significant interest in recent years. The time people would normally spend in a vehicle (i.e., car, bus, or train) may last for several hours or even longer. It is greatly expected to enjoy high-quality entertainment services and social communications on the road for pleasant long journeys [1]. On the other hand, issues such as urban traffic congestion and traffic accidents in big cities have become so serious that they cannot be ignored. For example, the traffic congestion level was up to 37 percent, and the number soared even up to 74 percent at evening peak times in Beijing in 2014 [2]; there are about 500,000 traffic accidents in China each year. These traffic issues also promote an urgent requirement on vehicular networks to provide travel assistance, driving safety, and so on. Nowadays, numerous countries and organizations have invested or are investing great efforts in research on powerful vehicular networks.

Up to date, there have been many umbrella communication technologies serving vehicular networks, such as IEEE 802.11p, dedicated short-range communication (DSRC), third generation (3G) communications, WiMAX, Long Term Evolution (LTE), LTE-Advanced (LTE-A) and the Internet of Things (IoT) [3]. However, these communication technologies are all based on the traditional network architecture, which adopts a *highly coupled* design due to historical reasons. Such a rigid architecture makes it difficult to satisfy various challenging demands in the vehicular environment [4, 5]. Therefore, many research efforts have started on the emerging software defined networking (SDN), which is considered as an alternative approach to renovate the traditional networks [6].

SDN is featured with flexible programmability by *decoupling* the data plane and the control plane. It is expected to realize more flexible management, greater service capability, higher data rate, less delay, and better quality in next generation vehicular ad hoc networks (VANETs). Figure 1 illustrates the architecture of software defined vehicular networks (SDVNs). To the best of our knowledge, few studies have been reported on how to make SDN smart in scheduling ubiquitous network resources to meet various vehicular demands. This is really an open gap to fill to promote powerful vehicular networks. Therefore, the scope of this article is to present the studies on how to enable crowd collaborating for SDVNs.

The contribution of our work is that we investigate a new network paradigm named smart identifier networking (SINET), and propose a novel customized SINET solution for the vehicular network (SINET-V). In SINET-V, virtualized function slices are able to be flexibly selected through crowd sensing. Furthermore, crowd collaborations are served to dynamically adapt to various vehicular scenarios and applications, including intra-slice collaborations and inter-slice ones. Practical experiments demonstrate the excellent performance and power of SINET-V.

The rest of this article is organized as follows. We present the related work and background. Next, we analyze the challenges and offer our considerations. Then the SINET-V solution is detailed. Furthermore, we summarize its potential advantages. Finally, we present the performance evaluations in the vehicular scenario.

RELATED WORK AND BACKGROUND

To the best of our knowledge, we are the first to design a network system that enables crowd collaborating to strengthen SDVN architecture in multiple aspects. There are some scattered related works on various individual aspects in the literature.

There are several research studies on SDVN

Digital Object Identifier:
10.1109/MCOM.2017.1601162

Wei Quan, Yana Liu, and Hongke Zhang are with Beijing Jiaotong University; Shui Yu is with Deakin University.

0163-6804/17/$25.00 © 2017 IEEE

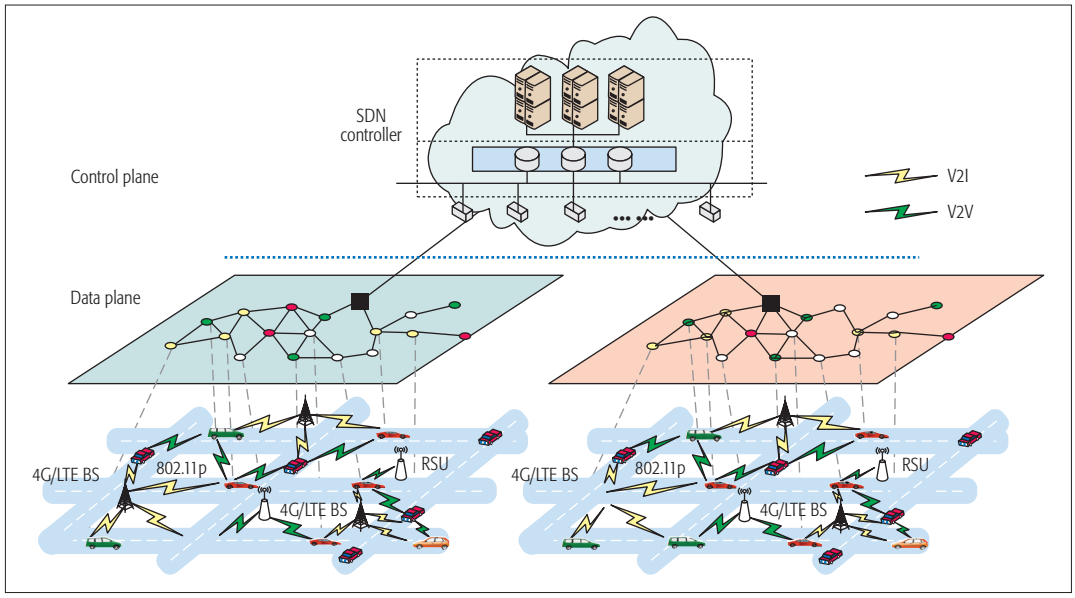


Figure 1. Illustration of a software defined vehicular network.

Vehicular networks are significantly different from conventional wireless communication scenarios. Many challenges hinder their applications, such as highly dynamic topology, frequent information interactions, and strict latency requirement.

architecture. He *et al.* built an SDN-based approach to enable rapid network innovation for vehicular communications [7]. Zheng *et al.* summarized the software defined cloud radio access network (cloud-RAN) architecture for heterogeneous vehicular networks [8]. Li *et al.* presented a hybrid southbound communication mode to balance latency and cost for the software-defined VANET [9]. Zhang *et al.* analyzed a socially aware Internet of Vehicles and proposed a novel perspective and supportive technologies for social vehicle swarms [10]. However, the aforementioned research studies focused on the overall design of network architecture, and failed to consider powerful crowd collaboration and analyze its implementation mechanisms.

Crowd collaboration provides a novel approach to smarten the SDVN architecture. Recently, smart collaborative networking (SCN) has been widely discussed as a novel perspective for future network architecture. It was first proposed in a future Internet project in China, and SINET is a significant output of the project. The concept of smart collaboration is highlighted in the SINET architecture, which is able to flexibly meet various network requirements through crowd wisdom and capacity [11]. Moreover, Zhang *et al.* studied how to promote efficient communications for high-speed railway environments using smart collaborative networking [12]. However, all of these are just preliminary research for some special application scenarios. There is still a long way, and a great opportunity, to develop a fully intelligent SDVN system for future vehicular applications.

In this article, we focus on a customized SINET-based solution to enable crowd collaborating for SDVNs.

Problems and Challenges

Vehicular networks are significantly different from conventional wireless communication scenarios. Many challenges hinder their applications, such as highly dynamic topology, frequent information interactions, and strict latency requirement [13]. Therefore, we have to overcome obstacles in SDVN design. In this work, we focus on three key design considerations for the smart SDVN.

Vehicular security-related assurance: Safety in vehicular networking is more serious than that in traditional networks. Vehicular networking is not only related to the risk of information leakage, but also involved in driving safety (i.e., car safety and personal safety). In 2016, the Tencent Cohen laboratory announced that after several month's extensive study, they could attack Tesla by remote control, including parking status control and driving status control. Therefore, it is critical to find how to guarantee the security in future vehicular networking.

Heterogeneous network integration: Vehicular networks are sophisticated and heterogeneous. On one hand, there are various base stations (BSs) supporting specific wireless techniques, such as 3G, WiMAX, LTE, and even device-to-device (D2D) without BSs. On the other hand, there are many diversified communication modes, including vehicle-to-vehicle (V2V), vehicle-to-roadside (V2R), and vehicle-to-everything (V2X). Besides, different network deployment scales further aggravate its heterogeneity [14]. For instance, a macrocell can support tens of users, while a small cell usually supports no more than 10. Hence, the compatibility of heterogeneous communications must be fully considered in the design of future vehicular networks. It is urgent to use multiple wireless interfaces collaboratively for better performance.

Network load optimization: Due to the randomness of vehicle movement, vehicles can suddenly gather in a given area, resulting in a sharp increase of the network load. This severe jitter affects the network performance greatly. Even worse, the access point or BS would be overloaded when the load is beyond their capabilities. As a result, we should consider meticulous scheduling of ubiquitous network resources for network load optimization.

There is no doubt that these challenges are hindering the further development of vehicular

SINET-V is able to smartly schedule ubiquitous network resources and fully meet diversified vehicular demands. It shows two aspects: through crowd sensing, network function slices are flexibly organized with a group of function-similar components; through crowd collaborations, different function slices are further driven to serve various applications on demand.

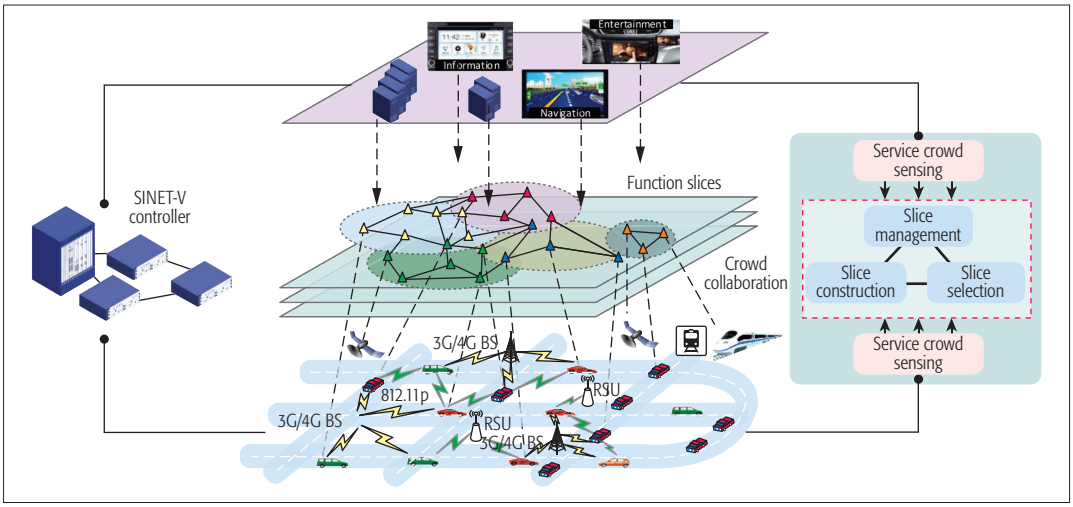


Figure 2. The architecture of crowd collaborations in SINET-V.

networks. How to better solve these practical problems becomes urgent. Nevertheless, it is crystal clear that it is too difficult to solve all the above challenges using one new technology. In practice, most application scenarios do not need us to solve the mentioned issues simultaneously. One application scenario usually focuses on one essential requirement, and another scenario requires another one. For example, low delay is highly required to achieve real-time traffic monitoring, while security is necessary for self-driving applications.

Based on the above analysis, a flexible network architecture is highly required to meet these vehicular demand. It allows us to build smart SDVNs to adaptively meet various vehicular demands by leveraging crowd collaboration and their capacities.

Solution: SINET-V

In this section, we explain how to enhance crowd collaborations for SDVNs in our solution, including its architecture, key mechanisms, protocol, and workflow.

Overview of SINET

SINET is a specific instance of smart collaborative networking (SCN) [12]. SINET can be vertically divided into three layers: the smart pervasive service layer (L-SPS), the dynamic resource adaption layer (L-DRA), and the collaborative network component layer (L-CNC). In particular, to extend this triple-layered network architecture, SINET horizontally contains two domains: the entity domain (D-EN) and behavior domain (D-BE).

More specifically, L-SPS is responsible for naming and description of services. L-DRA dynamically controls network functions to allocate network resources through perceiving service demands and network statuses. L-CNC is responsible for data storage and transmission. D-EN contains three kinds of identifiers to identify different network entities. A service identifier (SID) is used to name and manage pervasive services. A function identifier (FID) is used to mark a network function slice. A node identifier (NID) is used to locate a network component. Analogous to the D-EN, service behavior description (SBD), function behavior description (FBD), and node behavior description (NBD) are adopted to provide further information for each SID, FID, and NID, respectively.

With these basic elements, SINET provides a framework to completely integrate the pervasive services management, dynamic resources adaptation, and network components collaboration. This design allows us to make many kinds of innovations to flexibly meet various network requirements according to smart collaboration.

SINET-V Mechanisms

By leveraging the SINET architecture, we propose SINET-V, a customized solution for SDVNs. SINET-V is able to smartly schedule ubiquitous network resources and fully meet diversified vehicular demands. It shows two aspects: through crowd sensing, network function slices are flexibly organized with a group of function-similar components; through crowd collaborations, different function slices are further driven to serve various applications on demand. The architecture of crowd collaborations in SINET-V is shown in Fig. 2.

Specifically, SINET-V is able to perceive various requirements of vehicular services in L-SPS, including service type, bandwidth, and delay requirement. L-DRA is responsible for dynamically adapting to network resources and building function slices through crowd collaborations. L-CNC is constructed as an overlay network to eliminate the heterogeneity of existing vehicular networks. In L-CNC, different components can carry on the tasks collaboratively, such as caching storage and data transmission.

Different virtual function modules are included in SINET-V. A service identifier registration module and a service management module are used in L-SPS. The service identifier registration module is responsible for storing SID and SBD. The service management module can respond to service registration messages and service request messages by querying the service identifier registration module.

In L-DRA, there is a crowd collaboration module used to achieve intelligent scheduling of network resources. A crowd collaboration module is composed of several sub-modules. A service-aware module perceives service statuses (i.e., service type, data rate, and bandwidth requirement) and assigns different priorities to corre-

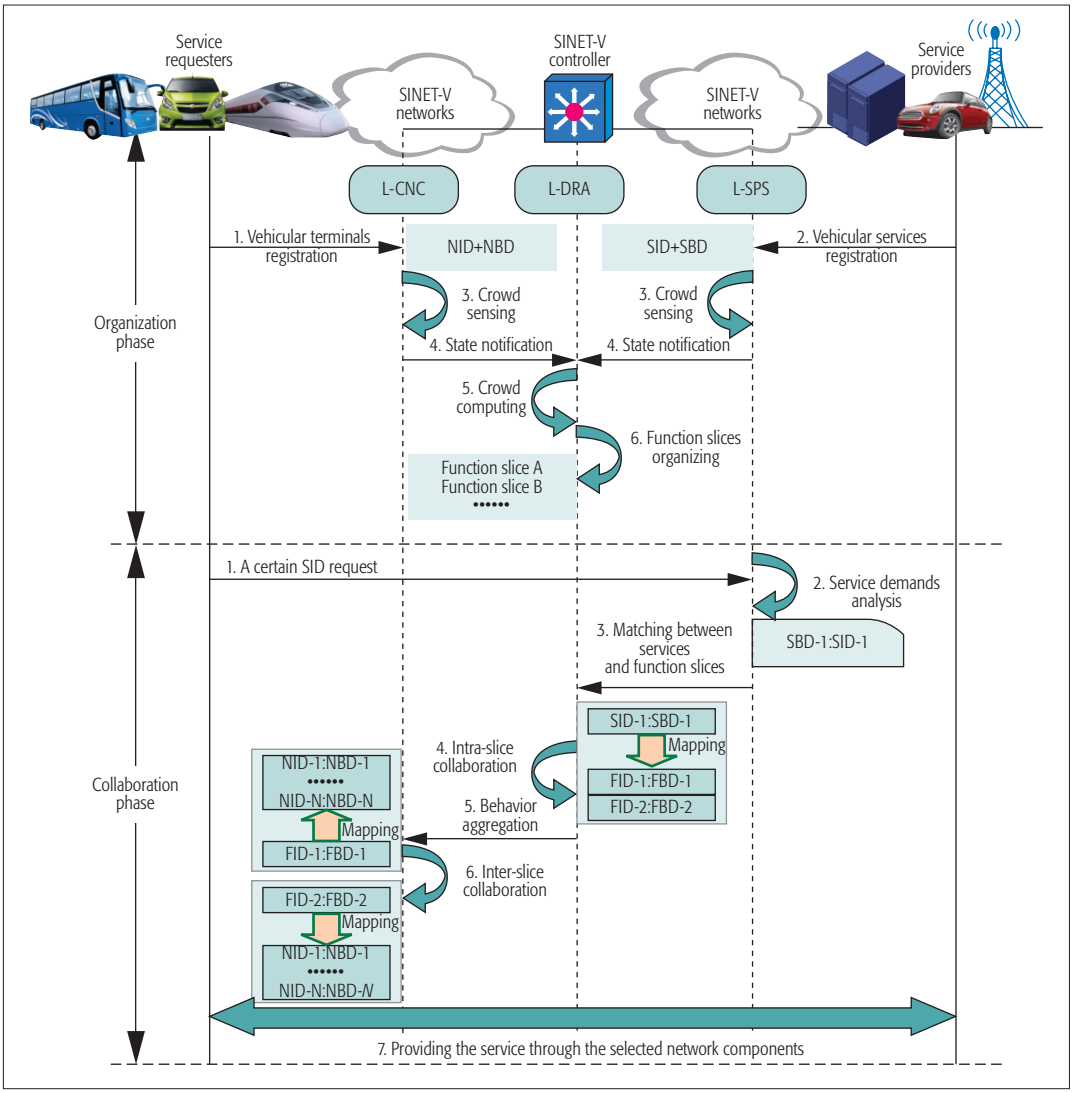


Figure 3. Workflow of SINET-V.

sponding services. A network-aware module is responsible for awareness of network behaviors, including wireless spectrum, network congestion, and network bandwidth. Traffic shaping and data scheduling can adjust the data traffic based on the service and network status. The above sub-modules can cooperate with each other. Through the upper service perception and the lower resource awareness, network function slices are smartly organized with a group of function-similar components, such as low-latency slices, high-bandwidth slices, and low-cost slices. SINET-V controllers are in charge of controlling network function slices, which can be centralized or distributed. The crowd collaboration module can also dynamically adjust components based on real-time feedback of network status. It is worth noting that the same component may belong to one or several function slices at the same time.

L-CNC is in charge of storage and transmission of data, which embraces a component intra-aware module, a component inter-aware module, and a component identifier management module. It is noteworthy that the component intra-aware module is used to perceive internal statuses (e.g., the speed and location of vehicles, supported network interfaces, hardware type, and processing capacity of BS or roadside unit, RSU). The component inter-aware module is responsible for monitoring environmental characteristics, including density of ambient vehicles, interference statuses, and so on. The component intra-aware and component inter-aware modules will send messages to the network-aware module of the upper layer.

Protocols and Workflow

In order to demonstrate our scheme better, we further summarize the typical workflows of SINET-V, as shown in Fig. 3. The whole process is divided into two phases: the organization phase and the collaboration phase.

During the organization phase, the typical workflow mainly contains three processes:

- Register NIDs and SIDs (steps 1, 2). When vehicle terminals access a network, NIDs will be assigned to them. Meanwhile, vehicular service providers (i.e., vehicles, BSs, and content providers) will generate SIDs for their local services and register them.
- Crowd sensing (steps 3, 4). It includes both the upper service perception and the lower resource awareness. The resource awareness is composed of two parts: traffic and road monitoring, and network state monitoring.

SINET-V controllers are in charge of controlling network function slices, which can be centralized or distributed. The crowd collaboration module can also dynamically adjust components based on real time feedback of network status. It is worth noting that the same component may belong to one or several function slices at the same time.

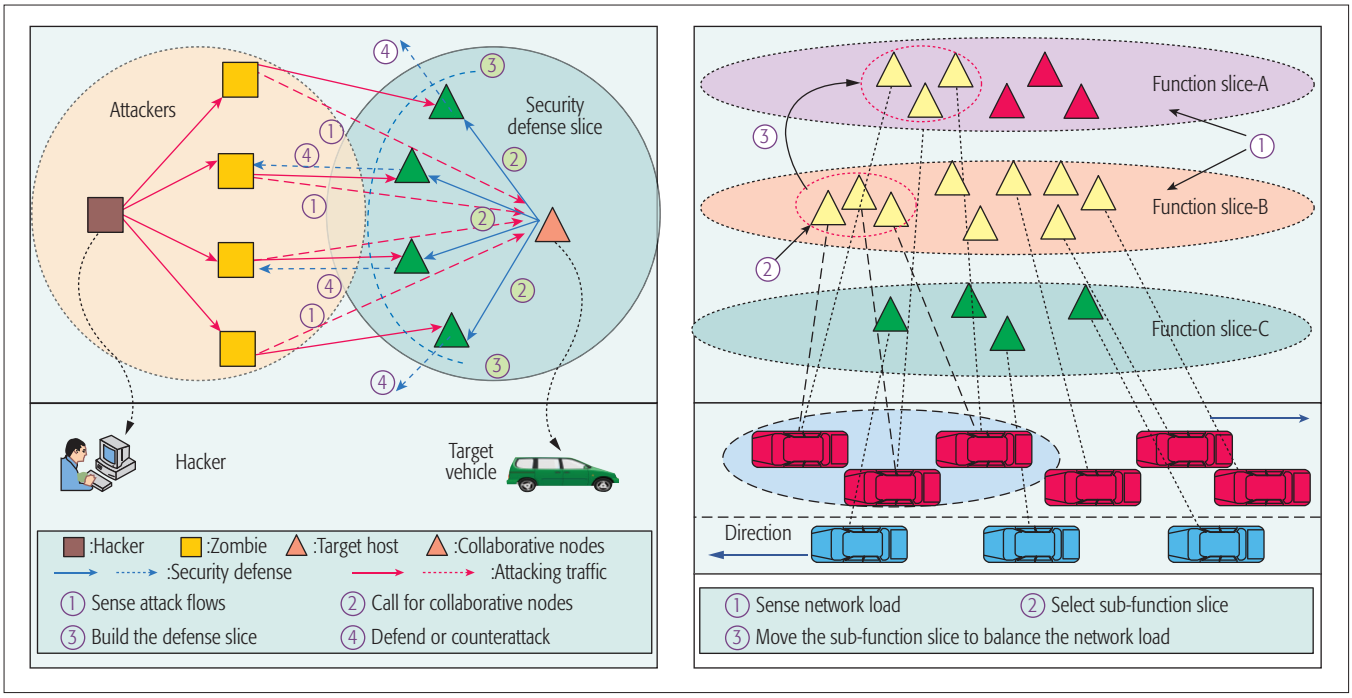


Figure 4. Illustrations of security defense and network load balancing in SINET-V.

- Construct function slices (steps 5, 6). After crowd computing of state notifications, the controller can organize function slices according to service demands and resource status. Game theory can be selected to maximize the benefit of cooperations.

During the collaboration phase, a typical workflow also involves the following three steps:

- Request services (steps 1, 2). When requiring the service, vehicles will send an SBD to the controller. The controller will select the specific SID and SBD after analyzing service demands.
- Select function slices (steps 3–6). Function slices will be decided according to the mapping between FID and SID, which can be implemented using an existing fast lookup algorithm. What's more, different slices can work harmoniously due to the inter-slice cooperation mechanism.
- Establish transmission path (step 7). The network components will be aggregated according to crowd collaboration. Network components further cooperate to establish a path for delivering the service according to an intra-slice cooperation mechanism.

All in all, crowd collaborations are highlighted in SINET-V to achieve smart adaptation between the vehicular services and the network infrastructure. Besides, the entity domain and behavior domain are separated for improving the feasibility by perceiving service demands and network behaviors. The mappings from one namespace to another are used to link the behaviors analysis and entities selection. Meanwhile, SINET-V deploys intra-slice and inter-slice collaborations to achieve dynamic adaption and allocation of network resources.

Potential Advantages

In this section, we present several cases to clearly illustrate how SINET-V addresses the aforementioned challenges and problems.

Guarantee network security: The existing network systems are relatively fixed, which makes the attack actions equally easy. SINET-V employs an intrinsic peculiarity to manage logical function slices dynamically. This feature can be used in security defense for vehicular networks. Figure 4 illustrates an example of security defense in SINET-V. When a targeted host is attacked, it can sense malicious attack flows. Then it immediately initiates the defense function by crowd collaboration. Specifically, the targeted host first calls for collaborative nodes to organize a security defense slice by dispersing requests. The SINET-V controller will arrange suitable network nodes and resources to protect this targeted host. In a nutshell, these collaborative nodes can handle the incoming attack flows instead of the original targeted host. Moreover, they can counterattack the hacker if necessary. Therefore, they are able to establish a logical defensive shield for the targeted host. The dynamic collaborations among these nodes make it harder for an attacker to discover an accurate transmission path or a victim server. Consequently, SINET-V makes it difficult to attack the targeted host and improves the network security.

Support heterogeneous communications: SINET-V constructs an overlay network to eliminate the heterogeneity of the existing vehicular networks. As mentioned earlier, function slices can be organized by a group of function-similar components. Different function slices can work independently. Therefore, function slices can be constructed according to the characteristics of heterogeneous communication means. For example, vehicular nodes supporting time-division LTE (TD-LTE) can be organized within the same function slice, which provides reliable transmission quality through intra-slice collaboration. On the other hand, SINET-V employs inter-slice collaboration. Different function slices can collaborate to undertake some task through inter-slice collaboration.

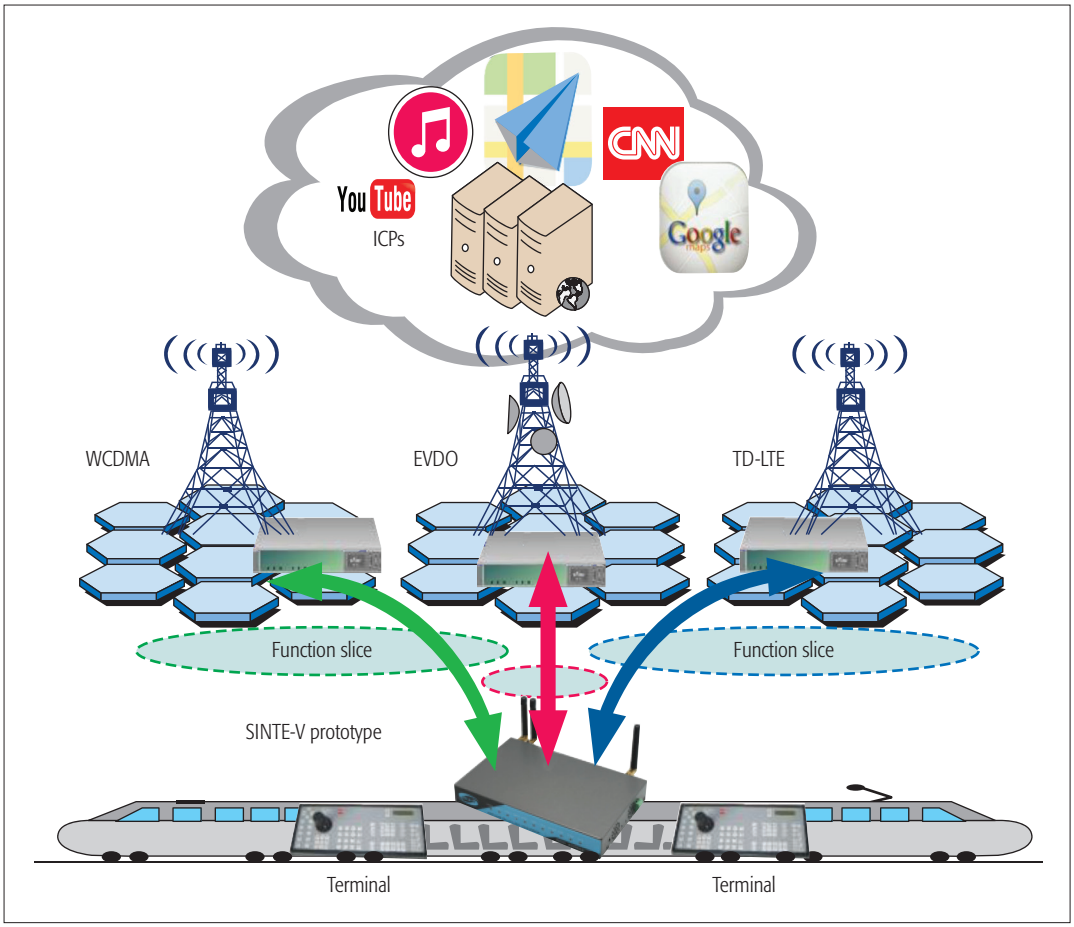


Figure 5. Experimental scenario.

When a targeted host is attacked, it can sense malicious attack flows. Then, it immediately initiates the defense function by crowd collaboration. In specific, the targeted host firstly calls for collaborative nodes to organize a security defense slice by dispersing requests. The SINET-V controller will arrange suitable network nodes and resources to protect this targeted host.

Multiple communication means can be supported simultaneously and selected adaptively according to adjusting the function slices. Therefore, through crowd collaboration, SINET-V can eliminate the heterogeneity of the existing vehicular networks.

Balance network load: Different from the traditional network, SINET-V is more flexible and configurable for load balancing through crowd collaboration. Figure 4 also illustrates an example of network load balancing in SINET-V. The network load can be sensed for each function slice. When a function slice is overloaded, SINET-V will immediately select or organize other available function slices to share the network load. In particular, a sub-function slice can move from this slice to another one. In that case, the load saturation condition of the popular slice is alleviated greatly, and the slices with low load can be used sufficiently. SINET-V can easily achieve network load balance according to crowd collaboration among different function slices.

From the above analysis, we can see that SINET-V is available to adapt to various requirements in vehicular networks by leveraging various crowd collaboration mechanisms. It provides an efficient and complete architecture for highly dynamical vehicular networks.

Experimental Analysis

In this section, we present some preliminary experimental analysis to verify the feasibility and efficiency of SINET-V. We developed a prototype system and tested it in Beijing subway line two, as shown in Fig. 5. Beijing subway line two is covered by multiple cellular networks, wideband code-division multiple access (WCDMA) for China Unicom, evolution data only (EVDO) for China Telecom, and TD-LTE for China Mobile. In our experiments, each network slice was represented by one kind of network connection means, that is, WCDMA, EVDO, or TD-LTE. SINET-V can reduce latency and improve network performance by enabling crowd collaboration among multiple network function slices. A SINET-V controller was employed as the crowd collaboration management unit. We tested the effectiveness of SINET-V in terms of round-trip time (RTT). As for the testing terminals, we adopted the iPhone 6, in which the iPhone Ping Tool was installed. During this experiment, the iPhone Ping Tool continuously attempted to ping a public IP address on our campus every second for acquiring corresponding RTT along the testing subway line two. Then we evaluated the network quality.

Figure 6 shows an intuitive performance comparison between 4G-LTE and SINET-V. We can see that RTT values of SINET-V are significantly lower than those of 4G-LTE. The average RTT is 58 ms in SINET-V, while it is 83 ms in 4G-LTE. In particular, 86 percent of RTT values are smaller than 75 ms, and the valley RTT value remains at around 18 ms in SINET-V, while only 47 percent of RTT values are smaller than 75 ms in the solution of 4G-LTE. The main reason is that SINET-V can dynamically sense and predict network link states [15], and hence flexibly employ the best network slice and

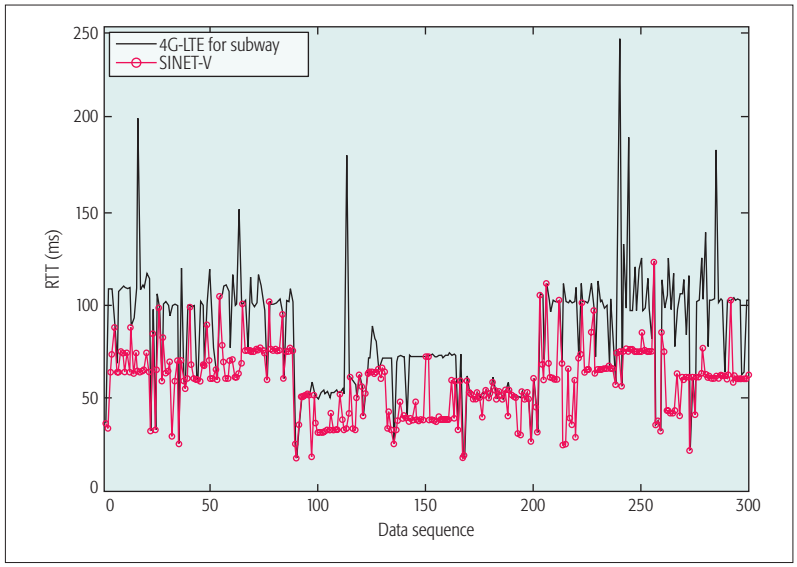


Figure 6. Experimental results comparison.

transmission links through crowd collaboration. In detail, when the quality of one network slice status is poor, a SINET-V controller is triggered to choose another optimal slice(s) through crowd collaboration to serve different applications dynamically. It is worth noting that this experiment is just our primary function implementation of SINET-V, and there is great potential to realize better performance in the near future.

Conclusions

In this article, we propose a novel customized SINET-V solution enhancing crowd collaboration for software defined vehicular networks. In SINET-V, virtualized function slices are flexibly organized by a group of network elements through crowd sensing. Then one or multiple function slice(s) may be motivated to dynamically serve different applications with crowd collaboration, including intra- and inter-slice ones. We analyze its potential advantages in several different vehicular instances. Experimental results show that SINET-V is able to improve the quality of service in a realistic urban vehicular scenario. In the near future, more investigations upon practical applications will be studied to promote the deployment of smart SDVNs.

Acknowledgment

This work was supported by the National Basic Research Program of China (973 Program) under Grant No. 2013CB329101, the National Natural Science Foundation of China (NSFC) under Grant Nos. 61602030 and 61232017, the National Key R&D Program under Grant No. 2016YFE0122900, and the Fundamental Research Funds for the Central Universities under Grant Nos. 2016RC036 and 2015JBM009.

References

[1] T. H. Luan *et al.*, "Social on Road: Enabling Secure and Efficient Social Networking on Highway," *IEEE Wireless Commun.*, vol. 22, no.1, Feb. 2015, pp. 44–51.
[2] Global Traffic Congestion Index, http://global-traffic-congestion-index.silk.co/, accessed on Jan. 28, 2017.
[3] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 4, June 2015, pp. 2347–76.
[4] M. Eiza *et al.*, "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G Enabled Vehicular Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 10, Mar. 2016, pp. 7868–81.
[5] H. Zhang *et al.*, "A Scalable and Smart Hierarchical Wireless Communication Architecture Based on Network/User Separation," *IEEE Wireless Commun.*, vol. 24, no. 1, Feb. 2017, pp. 18–24.
[6] H. Kim *et al.*, "Improving Network Management with Software Defined Networking," *IEEE Commun. Mag.*, vol. 51, no. 2, Feb. 2013, pp. 114–19.
[7] Z. He *et al.*, "SDVN: Enabling Rapid Network Innovation for Heterogeneous Vehicular Communication," *IEEE Network*, vol. 30, no. 4, July 2016, pp. 10–15.
[8] K. Zheng *et al.*, "Soft-Defined Heterogeneous Vehicular Network: Architecture and Challenges," *IEEE Network*, vol. 30, no. 4, July 2016, pp. 72–80.
[9] H. Li *et al.*, "Control Plane Optimization in Software-Defined Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 10, Oct. 2016, pp. 7895–904.
[10] Y. Zhang *et al.*, "Social Vehicle Swarms: A Novel Perspective on Socially Aware Vehicular Communication Architecture," *IEEE Wireless Commun.*, vol. 23, no. 4, Aug. 2016, pp. 82-89.
[11] H. Zhang *et al.*, "Smart Identifier Network: A Collaborative Architecture for the Future Internet," *IEEE Network*, vol. 30, no. 3, May 2016, pp. 46-51.
[12] H. Zhang *et al.*, "Promoting Efficient Communications for High-Speed Railway Using Smart Collaborative Networking," *IEEE Wireless Commun.*, vol. 22, no. 6, Dec. 2015, pp. 92–97.
[13] C. Bian *et al.*, "Theoretical Analysis on Caching Effects in Urban Vehicular Ad hoc Networks," *Wireless Commun. Mobile Comp.*, vol. 2016, no. 16, Nov. 2015, pp. 1759–72.
[14] K. Liu *et al.*, "Cooperative Data Scheduling in Hybrid Vehicular Ad Hoc Networks: VANET as a Software Defined Network," *IEEE/ACM Trans. Net.*, vol. 24, no. 3, June 2015, pp. 1759–77.
[15] H. Zhang *et al.*, "Link State Prediction Based Reliable Transmission for High-Speed Railway Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 12, Dec. 2016, pp. 9617–29.

Biographies

Wei Quan [M'14] received his Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT) in 2014. He is currently a lecturer at the School of Electronic and Information Engineering, Beijing Jiaotong University (BJTU), China. He has published more than 20 papers in prestigious international journals, including *IEEE Wireless Communications*, *IEEE Network*, and *IEEE Communications Letters*. His research interests include future Internet, vehicular networks, and the Internet of Energy. He is a member of ACM.

Yana Liu is currently a Master's student at the National Engineering Laboratory for Next Generation Internet Technologies, School of Electronic and Information Engineering, BJTU. Her research interests include smart collaborative networking and vehicular networks.

Hongke Zhang [M'13, SM'16] is currently a full professor at the School of Electronic and Information Engineering, BJTU, and the director of the National Engineering Lab on Next Generation Internet Technologies, China. His research has resulted in many papers, books, patents, and systems in the areas of communications and computer networks. His h-index is 24. His research interests include next-generation networks and future Internet architecture.

Shui Yu [M'04, SM'12] is currently a senior lecturer at the School of Information Technology, Deakin University. He has published two monographs and edited two books, and authored more than 150 technical papers, including top journals and top conferences, such as *IEEE TPDS*, IEEE *Transactions on Communications*, *IEEE TIFS*, *IEEE TMC*, *IEEE TKDE*, *IEEE TETC*, and IEEE INFOCOM. His h-index is 25. His research interests include networking theory, big data, cybersecurity, and mathematical modeling.

Latency Control in Software-Defined Mobile-Edge Vehicular Networking

Der-Jiunn Deng, Shao-Yu Lien, Chun-Cheng Lin, Shao-Chou Hung, and Wei-Bo Chen

ABSTRACT

A cloud radio access network deployed on top of edge networks as a software-defined radio access network architecture has been regarded as a promising paradigm for the next generation mobile networks, but it has not received considerable attention in the vehicular industry due to distinct design needs. For mobile networks, infrastructures provide powerful computation capability for universal radio resource optimization, and therefore an inherent "cloud-down" design is favorable. On the contrary, to deploy vehicular technologies, sophisticated processing capability has been a baseline feature for the next generation driving machines, which may not solely rely on wireless infrastructures to guarantee driving safety, so an "edge-up" design is preferred. Consequently, this article surveys the recent works on software-defined vehicular networks and proposes a series of edge-up software-defined networking designs, particularly emphasizing the most crucial function of latency control to support possible wireless applications for the next generation driving machines. The proposed designs thus create a paradigm shift to enable software-defined mobile-edge vehicular networking.

INTRODUCTION

The great success of mobile communications deployed in the past decades connects billions of users. Thanks to cellular infrastructures offering universal resource optimization, users with mobility are able to enjoy seamless and reliable wireless services. The paradigm of universal resource optimization emerged from the Universal Mobile Telecommunications System (UMTS), where radio resource management (RRM) is conducted by radio network controllers (RNCs). Although RRM has shifted to evolved NodeBs (eNBs) in Long Term Evolution (LTE) and LTE-Advanced (LTE-A), the design spirit of UMTS opens the concept of joint resource optimization. Subsequently, the architecture of the cloud radio access network (CRAN) emerges, in which baseband units (BBUs) and remote radio heads (RRHs) can be physically separated from an eNB to be massively deployed. Also, computation units (CUs) for optimization can also be implemented apart from an eNB, and universal resource optimization can be conducted through cloud computing technology. In such a CRAN framework, functions in an eNB are thus virtualized. Furthermore, through the S1/X2 interfaces, not only BBUs/RRHs but also small cells are able to exchange information for universal resource scheduling/allocation to extend CRAN to heterogeneous CRAN (H-CRAN).

Although the overall network performance can be optimized through universal resource optimization, the cost of CRAN/H-RAN could be unaffordable as the number of supported mobile devices explosively grows. The scalability concern thus drives the edge network (EdgeNet) or fog network (FogNet), which leverages edge computing technologies to perform resource optimization, information cache, and direct data transmissions at edge nodes. In this context, the optimization complexity can be significantly reduced, and the network does not have to collect user information from all users. By caching high correlation traffic to be forwarded to users at edge nodes, the backhaul flow burden, transmission latency, and energy consumption for information dissemination can be alleviated. However, without joint resource optimization, EdgeNet may suffer from interference, resource congestion, or underutilization, and may be vulnerable in mobility.

There appears to be a trade-off between CRAN/H-CRAN and EdgeNet, and the optimum trade-off has been widely studied. This research reveals that fixed network architectures (CRAN/H-CRAN and EdgeNet) may fossilize the performance and flexibility, which consequently inspired OpenFlow [1] and software-defined networking (SDN) [2] to dynamically optimize the network behavior. This concept further leads to a software-defined architecture harmonization of CRAN/H-CRAN on top of EdgeNet [3], which is known as a cloud-down design, and practical examples are device-to-device (D2D) proximity services in Third Generation Partnership Project (3GPP) Releases 12/13 [4] and IEEE 802.11ax station-to-station (S2S) transmissions. However, the cloud-down design is not substantially advertised in the vehicular industry due to the distinct design needs in vehicular and cellular networks. In vehicle designs, safety is the top concern, which may not solely rely on cellular networks. Instead, advanced driving machines are equipped with sensors, cameras, radars, and sophisticated computing units (CUs) to achieve anti-crash for both human-driven and unmanned vehicles. Nevertheless, mobile networks facilitating wide-range infor-

The authors survey the recent works on software-defined vehicular networks and propose a series of edge-up software-defined networking designs, particularly emphasizing the most crucial function of latency control to support possible wireless applications for the next generation driving machines. The proposed designs thus create a paradigm shift to enable software-defined mobile-edge vehicular networking.

Der-Jiunn Deng is with National Changhua University of Education; Shao-Yu Lien is with the National Chung Cheng University; Chun-Cheng Lin and Wei-Bo Chen are with National Chiao Tung University; Shao-Chou Hung is with National Taiwan University. Chun-Cheng Lin is the corresponding author.

Digital Object Identifier: 10.1109/MCOM.2017.1601165

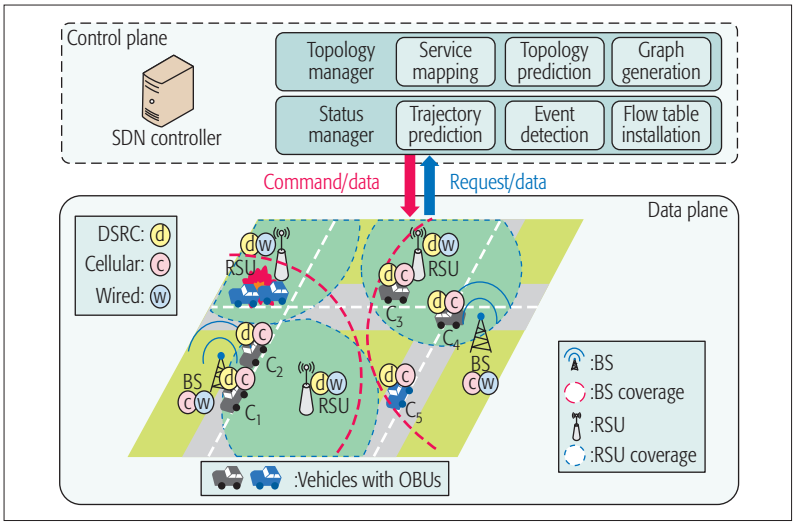


Figure 1. Illustration of SDVN architecture.

mation exchange can act as a powerful remote sensor to fetch well processed knowledge at the remote side. An advanced vehicle can be regarded as a mighty edge node, and thus a favorable mobile network architecture for vehicular societies lies in an edge-up design rather than cloud-down.

For vehicular applications, especially in high mobility, the most critical quality of service (QoS) requirement for wireless services lies in latency. To tailor edge-up software-defined cloud/edge vehicular networking, designs should target latency control. This article consequently reveals a complete series of latency control mechanisms. From radio access steering to processing cache at base stations (BSs), a comprehensive design performance evaluation is provided as an essential foundation for the next generation vehicular networks.

Software-Defined Vehicular Network

In the context of the Internet of Vehicles (IoV), vehicles can be regarded as connected intelligent network nodes, which can access computing resources and storage space in remote cloud servers, offering personalized services [5]. However, when accessing resources in the cyber-world, high communication latency and scarce available bandwidth may greatly harm users' quality of experience (QoE) and hinder the development of IoV. While the traditional client-server paradigm is showing its limits, the software-defined vehicular networking (SDVN) paradigm is emerging as an efficient approach to provide timely services in vehicular networks.

A general framework for SDVN is illustrated in Fig. 1, which consists of the following major components:

•Onboard unit (OBU): Each vehicle in this system is equipped with an OBU in charge of communications of this vehicle with roadside units (RSUs), BSs, cellular infrastructures, and other vehicles through dedicated short-range communications (DSRC).

•RSU: The RSU is deployed at a fixed/static position to communicate with the SDVN controller based on the Openflow protocol to receive status information from vehicles based on DSRC. For communications with the SDVN controller, the RSU can transfer users' service requests to the SDVN controller and receive the packet forwarding commands from the SDVN controller.

•BS: The BS offers a similar function to RSUs, but it is in charge of LTE/LTE-A or New Radio (NR) connection with vehicles and wired packet transmissions with RSUs.

•SDVN controller: The SDVN controller is responsible for centralized management of the networking functions virtualized from the vehicular network according to OpenFlow, which defines how it issues commands for packet flow to RSUs and BSs. The SDVN controller includes two modules: the topology manager creates and maintains the network topology, and the status manager collects and maintains the status information of all nodes.

In IoV, diverse communication technologies can be applied, in which cellular connection imposes a higher cost than DSRC, but it offers a higher transmission data rate and a wider coverage range for seamless services. Nevertheless, to reduce costs, the DSRC would be preferred for communications between vehicles (V2V) in general. Based on this technical preference, data transmissions in SDVNs can be categorized based on data types in the following cases.

Case 1: An SDVN involves a large number of vehicles. Consider broadcasting a public message (e.g., on road closings) to all vehicles in a particular area. This type of message has a feature of small volume but needs to be transmitted immediately. Therefore, the SDVN controller sends this message to each RSU, and each RSU subsequently transfers the message to vehicles within RSU coverage. Then the vehicles transfer the message to other vehicles that have not received the message yet through V2V DSRC communications. Since the packet size is small, OBUs can rapidly transmit it.

Case 2: A vehicle is moving out of the coverage of one RSU coverage to that of another RSU (e.g., in Fig. 1, vehicle c3 moves from the right RSU coverage to the left RSU coverage). Suppose that this vehicle already downloaded a part of some large-size file from the first RSU. Then the SDVN controller can forecast the movement trajectory of the vehicle, and command the next RSU to download the remaining part of the file in advance to shorten the delay time when the vehicle moves between two RSUs.

Case 3: Two vehicles within the same RSU coverage request the same service, and are heading in the same direction (e.g., vehicles c1 and c2 in Fig. 1). The SDVN controller will divide the requested data into two parts, and send the two parts to the two vehicles, respectively. Once the two vehicles receive their respective part of the data, they duplicate and transmit these respective parts to each other through V2V DSRC communications to reduce redundant transmissions.

Case 4: A vehicle is out of coverage from any RSU and other vehicular OBUs (e.g., vehicle c5 in Fig. 1). Communications of this vehicle will be supported by a BS through cellular networks, but more energy may be consumed. To save energy consumption, once this vehicle enters RSU coverage or vehicular DSRC coverage, this vehicle will switch to communicate with this RSU or the encountered vehicle.

Type	Feature	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]
SDVN	Trajectory prediction	v	v			v			
	Reconnection					v			
	Packet flow selection		v	v	v			v	v
	Channel selection	v	v			v			
	Content distribution	v							
	Decentralization						v		v
	Latency control			v			v	v	v
VANET	Large-scale vehicle traffic	v				v	v		v
	Heterogeneous vehicles								
	Limited bandwidth resources	v		v		v	v		v
	Trajectory uncertainty	v				v			
	Short lived connection	v							
	Energy cost		v	v	v			v	
	QoS			v		v		v	v

Table 1. Classification of pervious works on SDVNs.

It is inefficient to transfer data collected by vehicles to a remote cloud for subsequent processing and analysis. Such a constraint suggest moving processing close to data generation units in order to minimize latency, and this is where fog computing comes in.

Case 5: Consider that a car accident occurs in the SDVN region, and an emergency message should be transmitted immediately. To reduce the relay in notifying the influenced vehicles, the SDVN system does not send this message to those unrelated vehicles. For instance, a car accident occurs in the upper left corner of the region in Fig. 1. According to trajectory prediction, vehicles c1, c2, c4, and c5 will not pass by the accident site, and hence only vehicle c3 is notified.

To deploy intelligent transportation systems as well as IoV, the U.S. Federal Communications Commission (FCC) has allocated 75 MHz of spectrum in the 5.9 GHz band for V2V DSRC communications, in which 7 channels are available for safety and non-safety applications. DSRC is used for physical (PHY) and medium access control (MAC) layers in IEEE 802.11p (WAVE) and IEEE 1609.1/.2/.3/.4. Most SDVNs apply OpenFlow [1], which considers a packet relaying machine with multiple flow entries. When receiving a packet, the machine checks whether the packet is matched with some flow entries and takes the corresponding actions. If the packet is not matched with any flow entry, it is transferred to a controller for later computations.

Most related works on SDVNs have focused on topology establishment and trajectory decision. Furthermore, topology establishment is based on trajectory prediction to judge the position and reconnection to the next RSU of each vehicle. Trajectory decision is concerned with packet flow selection and channel selection during transmitting packets. In addition, content distribution, decentralization, and latency control have also been investigated recently. Based on these attributes and the classification of vehicular ad hoc networks (VANETs), some representative works on SDVNs are classified in Table 1.

Some works on topology establishment are reviewed as follows. Cao *et al.* [6] considered an SDVN based on type-based content distribution (TBCD) to support distribution of large-scale data-intensive content in vehicular networks. The SDN controller constructs the network topology by predicting vehicle trajectory according to positions and speeds of vehicles. For content distribution, the proposed TBCD is to classify large-size data into a number of small-size data according to interest groups of vehicles. Then He *et al.* [7] proposed an SDVN architecture with a status manager and a topology manager to address heterogeneity of network facilities, whose network functions are virtualized and centralized to be controlled by the SDN controller. This logically centralized controller can find the optimal packet flow and channels in this heterogeneous vehicular network, and make judgments in advance according to vehicle driving information, to avoid additional transmissions and save energy costs.

The remaining works are based on trajectory decisions, as reviewed in the following. Salahuddin *et al.* [8] proposed an RSU cloud including not only a conventional RSU, but also an RSU micro data center with virtualized network functions. They applied a Markov decision process to determine a transmission path with minimal bandwidth resources and energy costs. To save excessive consumption of network resources due to periodic warning messages from RSUs, Liu *et al.* [9] proposed an SDVN based on GeoBroadcast architecture. To avoid the overheads of packets broadcasted from a source RSU to other RSUs that are transmitted to the data center and then transferred, the source RSU transmits a packet-in message to the SDVN controller, and then the controller helps transmit the packets to the destination according to topological and geographical information. Bozkaya and Canberk [10] considered flow and power management in the SDN controller. The RSU first computes the QoE of vehicles, and marks those with QoE

Although next generation driving machines can be powerful edge nodes for data computing to support safety in high mobility, accessing the cloud cyber-world is still desired to obtain updated information such as local traveling guides, weather conditions, traffic congestion conditions, highway conditions (e.g., a sharp turn, uphill/downhill, under construction), etc.

below a threshold as unsatisfactory vehicles. Then the manager adopts a Kriging spatial interpolation method to compute the strength of the optimal signal of each unsatisfied vehicle. The unsatisfied vehicle is switched to be served and allocated with a bandwidth according to its signal strength by another closest RSU.

Some works on trajectory decisions were based on latency control. To improve the latency-sensitivity in VANETs, Sudheera *et al.* [11] divided controllers into two categories: the main controller is in charge of coordinating the interaction among local controllers, and each local controller is in charge of controlling the local transmissions of RSUs and vehicles in the controlled region. Li *et al.* [12] considered a hybrid network of VANETs and cellular networks, and proposed an optimization strategy to balance the high costs in the cellular networks and uncertain latency in VANETs. Their proposed strategy is to rebate more bandwidth resources to encourage vehicles to adopt cellular networks to send the SDVN control requests. Then the problem is modeled as a two-stage Stackelberg game. To address the latency to access cloud servers and to further promote QoS, He *et al.* [13] adopted a software-defined cloud/fog networking architecture and a novel particle swarm optimization to balance the loads among various cloud/fog devices and to reduce latency.

Latency Control of Radio Access Steering

Nowadays, vehicular applications, such as driving safety and traffic control information, require timely processing to provide a prompt decision or action. It is inefficient to transfer data collected by vehicles to a remote cloud for subsequent processing and analysis. Such a constraint suggests moving processing close to data generation units in order to minimize latency, and this is where fog computing (FC) comes in.

The next generation driving machines (regarded as edge nodes in the following) may utilize two possible mechanisms to exchange information with each other.

1. Edge nodes socially/directly exchange information with each other without relying on signal relay and resource allocation through the CRAN/H-CRAN. This scheme may potentially tackle the issues of complexity, scalability, and heavy traffic burdens in the CRAN/H-CRAN. However, there is no guarantee that all edge nodes needing a particular wireless service are able to successfully receive this service on time. The reason for this concern comes from the lack of good resource coordination among edge nodes. Unlike the CRAN/H-CRAN in which the resource scheduling/allocation optimization is the key feature to reject/mitigate interference well, random access may be a baseline radio access scheme in this mechanism (similar to DSRC). Consequently, interference among edge nodes may drastically impact the performance.

2. Edge nodes rely on the CRAN/H-CRAN for signal relay and radio resource allocation to exchange information with each other, by which, although the aforementioned issues in the CRAN/H-CRAN exist, interference among edge nodes can be avoided through facilitation of a scheduling-based radio access scheme.

It appears that a scheduling-based radio access scheme rejecting interference among edge nodes may provide higher throughput and thus lower latency than random access does. However, by further taking channel variation into design consideration, random access may provide better performance. In light of state-of-the-art scheduling-based radio access (e.g., LTE/LTE-A), when an edge node requests an amount of radio resources, a BS may allocate an exact amount of radio resources as requested by that edge node.

Before scheduling/allocating a radio resource to an edge node, channel estimation/prediction may be applied to all available radio resource for the CRAN/H-CRAN, and radio resource predicted to have an acceptable channel condition can be allocated to the edge node. However, even when performing channel estimation/prediction on each radio resource, there is no guarantee that an edge node can always enjoy an excellent channel condition on the allocated radio resource. In practice, an edge node may still suffer from a poor channel condition on the allocated radio resource. As a resource scheduling algorithm may virtualize the occupation of physical radio resources, the probability of deep fading at each radio resource (i.e., communications on this radio resource are unavailable) can be regarded as independently and identically distributed (i.i.d.) p due to potential randomization of physical radio resources. If an edge node requests one radio resource from the CRAN/H- CRAN, and the CRAN/H-CRAN allocate exactly one radio resource to this edge node, the throughput of this edge node is $1 - p$.

To enhance the throughput of an edge node, a promising scheme is to exploit frequency/spatial diversity. Consider that there are in total S radio resources available in the frequency domain to be shared by L edge nodes. If an edge node needs one radio resource but the CRAN/H-CRAN allocates $1 \le s \le S$ radio resources to this edge node, this edge node is able to successfully transmit data if these s resource blocks (RBs) do not simultaneously suffer from a deep fading channel condition. As a result, the throughput of the edge node is $1 - p^s$, which is enhanced compared to that using scheduling-based radio access. However, in this case, the utilization of each radio resource may be severely degraded.

If the CRAN/H-CRAN allocates one radio resource to an edge node requesting one radio resource, the utilization of this radio resource is $1 - p$. However, if the CRAN/H-CRAN allocates two radio resources to an edge node requesting one radio resource, the utilization of each of these two RBs is $1 - p^2$, which could be lower than $1 - p$. To further enhance the utilization of each radio resource, let S denote a set of radio resources allocated to the ith edge node and $||\prod|| = L$ denote the cardinality of $\prod$ (where $L \le S$). By observing the fact that different edge nodes may suffer from different levels of fading conditions at the same radio resource, the CRAN/H-CRAN thus may allocate these radio resources $\prod$ to other edge nodes. In this case, $\prod$ form a *resource pool* shared by multiple edge nodes using random access. If each edge node utilizes a different

radio resource, these radio resources $\prod$ can be fully utilized, as illustrated in Fig. 2. However, if some edge nodes unfortunately select the same radio resource, collisions occur, and the utilization degrades.

Consequently, there is a trade-off between social information exchange among edge nodes and relying on the CRAN/H-CRAN for radio resource optimization. To achieve optimum radio access steering to a scheduling-based radio access or to a random access, an optimization maximizing the throughput has been analyzed [3]. Nevertheless, the optimum radio access steering deriving from the aspect of minimizing latency still remains open. To address this issue, the optimum latency performance of scheduling-based radio access and random access is analyzed in Fig. 3.

We can observe from Fig. 3 that when channel fading is severe (i.e., a large p), it is likely that a radio resource allocated to an edge node suffers from severe channel fading and cannot be utilized by the edge node. Thus, a scheduling-based radio access scheme may lead to large latency under a large p. On the contrary, since edge nodes at different geographic locations may suffer from distinct levels of channel fading (deep channel fading may occur and vary over each time-frequency resource), adopting a random access scheme allowing multiple edge nodes to share a pool of radio resources may create diversity. Thus, latency of a random access scheme could outperform that of scheduling-based radio access. Such a trade-off may occur at p around 0.63, as demonstrated in Fig. 3. If $p < 0.63$, edge nodes should rely on the C-RAN/H-CRAN for radio resource scheduling; otherwise, edge nodes should socially exchange information.

To practice SDN, a critical challenge is to build up isolation between (virtual) networks. Nevertheless, the proposed radio access steering reveals harmonization between scheduling-based radio access and random access, which can be dynamically configured, and the network(s) reports this decision to vehicles. Thus, it is not necessary to impose the assumption that different networks are isolated when the proposed radio access steering is applied.

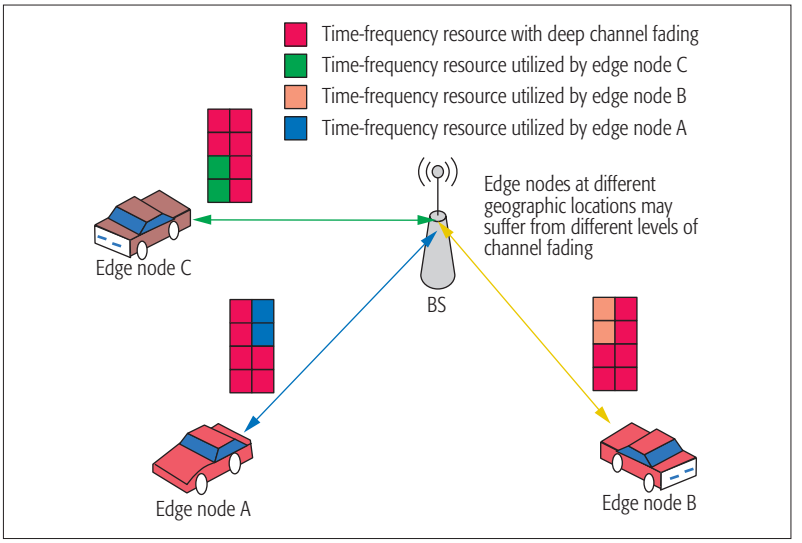


Figure 2. If each edge node utilizes a different radio resource, a pool of radio resources can be fully utilized without interference.

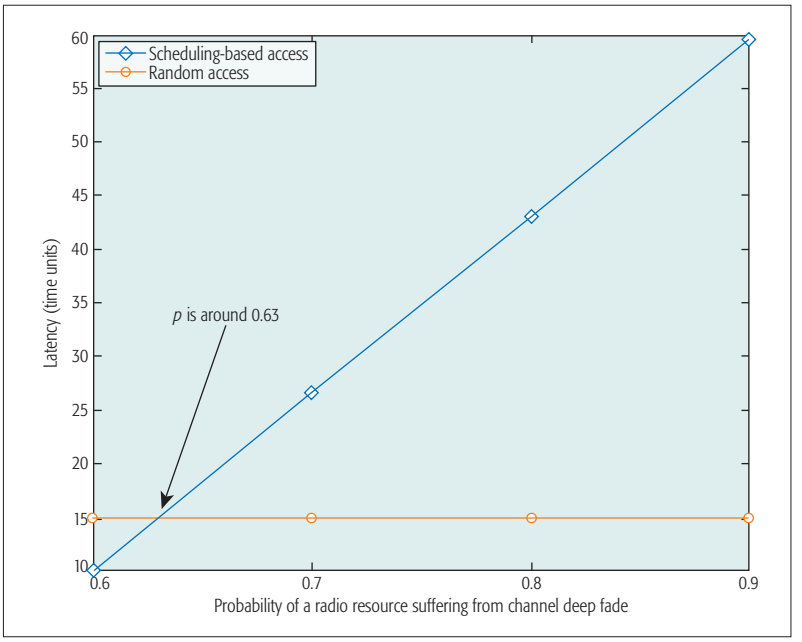


Figure 3. Optimum latency performance of scheduling-based radio access and random access.

Latency Control of Processing Cache at BSs

Although next generation driving machines can be powerful edge nodes for data computing to support safety in high mobility, accessing the cloud cyber-world is still desired to obtain updated information for local travel guides, weather conditions, traffic congestion, highway conditions (e.g., a sharp turn, uphill/downhill, under construction), and so on. For mobile networks, BSs have been ubiquitously deployed to provide seamless wireless services, which thus bridge edge nodes to the cloud cyber-world. Nevertheless, requesting information from the cloud cyber-world may lead to considerable overhead in terms of data flow burdens on the fronthaul and backhaul links and large latency. In fact, BSs deployed at a particular location may forward similar location-based information requests from multiple vehicles to the cloud cyber-world. If frequently requested location-based information can be cached at BSs, BSs can push such information immediately to edge nodes without accessing the cloud cyber-world. Consequently, the latency in obtaining such information can be largely reduced.

Before pushing location-based information to edge nodes, BSs can further process this information. For instance, vehicles may request shortest-path navigation to a particular destination from the cloud cyber-world. Nevertheless, the dynamics and statistics of traffic conditions on different routes at all times could be available on a BS. When a BS receives such navigation requests from edge nodes, a BS is able to find the optimum routes (may not be the shortest path, but could be the shortest driving time), and provides different routes to different edge nodes. In this context, a BS can provide the shortest-driving-time route by processing information

in terms of the shortest path, dynamics/statistics of traffic on different routes, and even reasoning of other vehicles' routing decisions. That is, BSs not only cache location-based information from the cloud cyber-world for edge nodes, but also process this information. BSs can thus be regarded as caching "processes" for edge nodes, as illustrated in Fig. 4. Through caching processes at BSs, latency to make the optimum decision using location-based information can be considerably decreased.

When an edge node requests a particular type of information from a BS, but this BS does not cache this type of information, the BS may need to forward the request to the cloud cyber-world. In this case, an edge node may place this pending task to a queue, and this task can leave the queue only if information is received from the cloud cyber-world. Obviously, this case may lead to worse latency performance and is unfavorable for an edge node. However, although BSs deployed in physical proximity may cache similar location-based information, they may also cache part of distinct location-based information and processing functions. To minimize the occasions of accessing the cloud cyber-world, an edge node may inquire location-based information from as many BSs as possible, and may access the cloud cyber-world only if there are too many pending tasks in the queue.

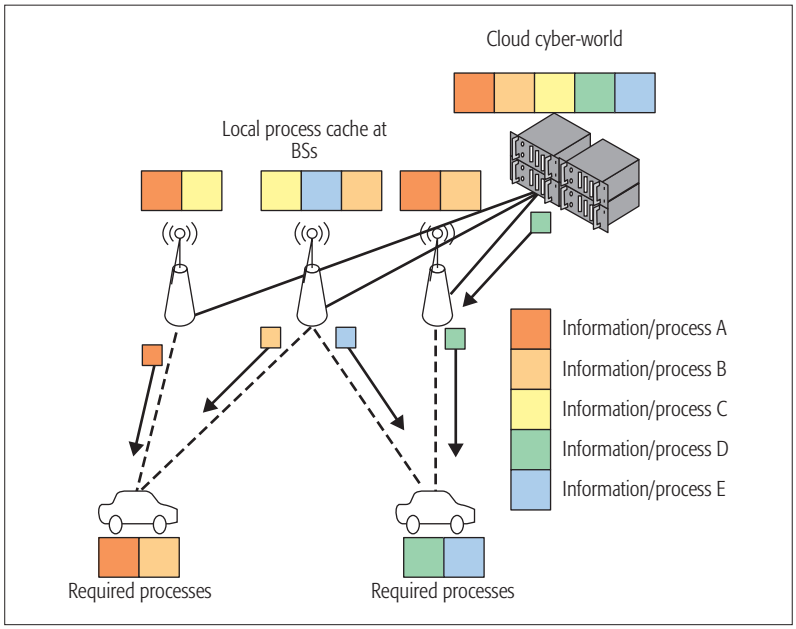


Figure 4. BSs are able to cache location-based information (or processing) for edge nodes, and requested information is provided from the cloud cyber-world only if none of the BSs cache this information (solid lines denote backhaul links and dashed lines denote fronthaul links).

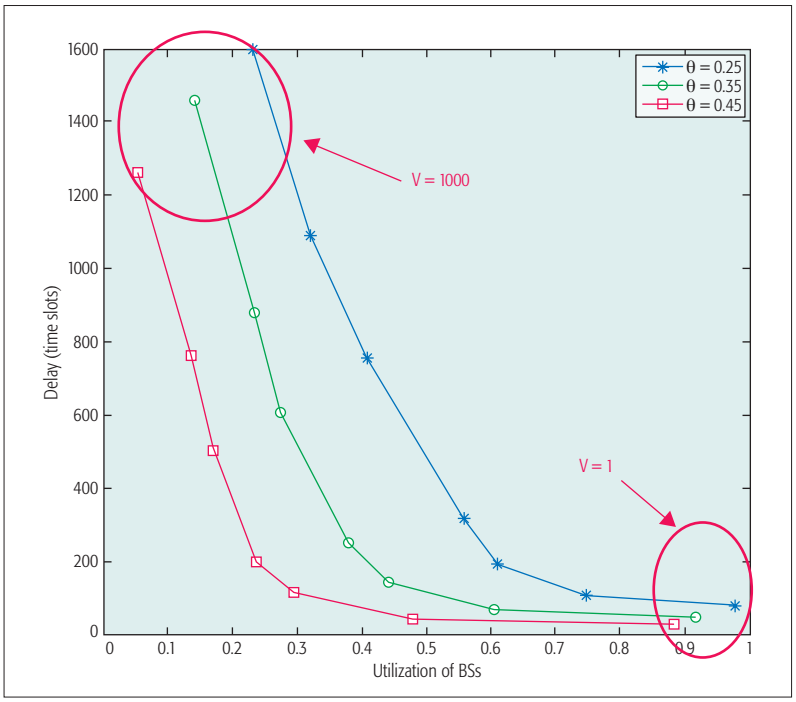


Figure 5. Optimum trade-off between utilization of BSs and latency.

To justify the practicability of the proposed processing cache at BSs, consider that there are 10 possible types of location-based information (or processes) that may be cached at BSs (requested by edge nodes). Each edge node randomly requests three types of location-based information. The arrival rate of the information demands at each edge node follows the Poisson process with a mean 0.5 information per slot. Each BS has a probability 0.25 to cache each of 10 types of information. If a type of information is cached at a BS, this BS is able to provide this type of information to edge nodes at a service rate of 1 piece of information per slot. If an edge node intends to prevent an unacceptable queue length, it may inquire information from as many BSs as possible if the queue length does not exceed a threshold (denoted by V). An edge requests information from the cloud cyber-world if the queue length exceeds V. In practice, an edge node may not be able to request information from all BSs due to limited fronthaul radio resources. Consequently, defining the utilization of BSs as M/N (where M is the practical number of edge nodes inquiring information from a BS and N is the total number of edge nodes that can be serviced by a BS), the optimization thus minimizes the utilization of BSs with a given latency constraint under a certain V. To solve this optimization, a number of schemes have been widely discussed [14, 15]. As a demonstration example, Lyapunov optimization [15], originating from Lyapunov drift theory, is applied. Lyapunov optimization introduces drift-plus-penalty into the control algorithm by imposing a cost V on the network utility and optimizes drift-plus-penalty function subject to queue stability. Through Lyapunov optimization, the optimum trade-off between utilization of BSs and latency can be derived in Fig. 5.

Figure 5 shows that a large V leads to a small utilization of BSs and thus worse latency performance. To improve the latency performance, we further introduce an upper bound of backhual utilization (defined as K/M, where K is the maximum number of edge nodes permitted to inquire information from the cloud cyber-world), denoted as θ. We can also observe from Fig. 5 that a large θ facilitates improvement of latency performance. This result is not surprising in that if there is no BS able to provide the corresponding information/process service, the cloud cyber-world can provide further assistance.

Conclusion

In this article, the foundations of latency control in software-defined mobile-edge vehicular networking are provided, in which we reveal a novel edge-up design in contrast to conventional cloud-down in cloud/edge radio access network research. To further practice the edge-up design, optimum radio access steering as a dynamic switch to a scheduling-based radio access when channel variation is stable or to a random access when channel fading is severe is demonstrated. Furthermore, caching location-based information or processing at BSs is demonstrated. Lyapunov drift theory is further applied to optimize performance. Nevertheless, this new research frontier is just at the beginning stage, and a number of issues still remain open, including architecture design, self-organization, protocols and standards, fog computing technologies, heterogeneity of RSUs, and conflict detection.

This new research frontier is just at the beginning stage, and a number of issues still remain open, including architecture design, self-organization, protocols and standards, fog computing technologies, heterogeneity of RSUs, and confliction detection.

References

[1] N. McKeown *et al.*, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Comp. Commun. Review*, vol. 38, no. 2, Apr. 2008, pp. 69–74.

[2] H. Kim and N. Feamster, "Improving Network Management with Software Defined Networking," *IEEE Commun. Mag.*, vol. 51, no. 2, Feb. 2013, pp. 114–19.

[3] S.-Y. Lien *et al.*, "Collaborative Radio Access of Heterogeneous Cloud Radio Access Networks and Edge Computing Networks," *Proc. IEEE ICC Wksp.*, May 2016.

[4] S.-Y. Lien *et al.*, "3GPP Device-to-Device Communications for Beyond 4G Cellular Networks," *IEEE Commun. Mag.*, vol. 54, no. 3, Mar. 2016, pp. 29–35.

[5] G. Han *et al.*, "Two Novel DOA Estimation Approaches for Real-Time Assistant Calibration Systems in Future Vehicle industrial," *IEEE Systems J.*, in press. DOI: 10.1109/JSYST.2015.2434822

[6] Y. Cao, J. Guo, and Y. Wu, "SDN Enabled Content Distribution in Vehicular Networks," *Proc. INTECH 2014*, IEEE Press, Oct. 2014, pp. 164-169.

[7] Z. He, J. Cao, and X. Liu, "SDVN: Enabling Rapid Network Innovation for Heterogeneous Vehicular Communication," *IEEE Network*, vol. 30, no. 4, July 2016, pp. 10–15.

[8] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles," *IEEE Internet of Things J.*, vol. 2, no. 2, Apr. 2015, pp. 133–44.

[9] Y.-C. Liu, C. Chen, and S. Chakraborty, "A Software Defined Network Architecture for Geobroadcast in VANETs," *Proc. IEEE ICC 2015*, June 2015, pp. 6559–64.

[10] E. Bozkaya and B. Canberk, "QoE-Based Flow Management in Software Defined Vehicular Networks," *Proc. IEEE GLOBECOM Wksps.*, Dec. 2015, pp. 1–6.

[11] K. L. K. Sudheera *et al.*, "Delay Efficient Software Defined Networking Based Architecture for Vehicular Networks," *Proc. 2016 IEEE Int'l. Conf. Commun. Systems*, Dec. 2016, pp. 1–6.

[12] H. Li, M. Dong, and K. Ota, "Control Plane Optimization in Software-Defined Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 10, Oct. 2016, pp. 7895–7904.

[13] X. He *et al.*, "A Novel Load Balancing Strategy of Software-Defined Cloud/Fog Networking in the Internet of Vehicles," *China Commun.*, vol. 13, no. 2, Feb. 2016, pp. 140–49.

[14] K. T. Phan *et al.*, "Optimal Scheduling over Time-Varying Channels with Traffic Admission Control: Structural Results and Online Learning Algorithms," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, Sept. 2013, pp. 4434–44.

[15] L. Georgiadis, M. J. Neely, and L. Tassiulas, *Resource Allocation and Cross-Layer Control in Wireless Networks*, Now Publishers Inc., 2006.

Biographies

Der-Jiunn Deng [M'10] (djdeng@cc.ncue.edu.tw) joined National Changhua University of Education as an assistant professor in the Department of Computer Science and Information Engineering in August 2005 and became a Distinguished Professor in August 2016. In 2010, 2011, and 2012, he received the Research Excellency Award of NCUE. In 2012 and 2015, he also received the Outstanding Faculty Research Award of NCUE. His research interests include multimedia communication and wireless networks.

Shao-Yu Lien (shaoyulien@gmail.com) was an associate professor at National Formosa University, and has been with National Chung Cheng University, Taiwan, since 2017. He has received the IEEE Communications Society Asia-Pacific Outstanding Paper Award 2014, the Scopus Young Researcher Award (issued by Elsevier) 2014, the URSI AP-RASC 2013 Young Scientist Award, and the IEEE ICC 2010 Best Paper Award. His research interests include LTE Pro, 5G New Radio, cyber-physical systems, and configurable networks.

Chun-Cheng Lin [S'06, M'08] (cclin321@nctu.edu.tw) received his Ph.D. degree in electrical engineering from National Taiwan University in 2009. Since 2016, he has been a professor at National Chiao Tung University, which he joined as an assistant professor in 2011. He was an assistant professor at the University of Taipei (2010–2011) and National Kaohsiung University of Applied Sciences (2009–2010). His research interests include wireless networks, information visualization, and algorithm design.

Shao-Chou Hung (d02942008@ntu.edu.tw) received his B.S. and M.S. degrees in electrical engineering from National Taiwan University in 2010 and 2013 respectively. He is currently a Ph. D. candidate in the Graduate Institute of Communication Engineering, National Taiwan University. His research interests include 5G network architecture, cognitive radio networks, and dynamic optimal control in wireless network.

Wei-Bo Chen (s100213030@gmail.com) received his B.S. degree in information management from National Chi Nan University in 2015. Since 2015, he has been studying for an M.S. degree in industrial engineering and management at National Chiao Tung University. His main research interests include metaheuristic algorithms, production scheduling, wireless networks, as well as the Internet of Things.

SOVCAN: Safety-Oriented Vehicular Controller Area Network

Yin Zhang, Min Chen, Nadra Guizani, Di Wu, and Victor C. M. Leung

The authors propose an SDN-based approach to develop the safety-oriented vehicular controller area network, which can guarantee traffic safety based on driver fatigue detection and emotion recognition, which are monitored through the driver's physiological and psychological state.

ABSTRACT

To meet the demands of vehicular networks, such as high throughput, high mobility, low latency, heterogeneity, and scalability, SDN has been applied for raising the user experience through providing high-performance communications between vehicular network nodes, reconstructing the vehicular network structure, and optimizing networking coverage, system security, communication latency, and so on. However, the existing SDN applications in the vehicular network mainly focus on the data communications between the vehicles and other network nodes or devices, while the vehicular controller area network is still limited to some particular applications, only providing users with basic services, but unable to meet the demands in a complex driving environment. Thus, this article proposes an SDN-based approach to develop the safety-oriented vehicular controller area network, which can guarantee traffic safety based on driver fatigue detection and emotional recognition, which are monitored through the driver's physiological and psychological state.

INTRODUCTION

With the development of mobile networks, the Internet of Things (IoT), and wireless sensor networks (WSNs), vehicular networks have gradually become one of the most effective approaches to implement intelligent transportation systems (ITS). For example, IEEE 802.11p is the standard that supports ITS applications in vehicular ad hoc networks (VANETs) [1]. Vehicle networks are expected to analyze and utilize various information inside and outside vehicles themselves through information and wireless communication techniques. Specifically, through vehicle-to-vehicle (V2V), infrastructure-to-vehicle, and vehicle-to-infrastructure (V2I) communications, which are the foundation and key support technologies determining the overall performance of vehicular networks, road safety and traffic efficiency are significantly improved.

However, the traditional wireless communication technologies are not available to meet the advanced demands from vehicular networks, including high throughput, high mobility, low latency, heterogeneity, scalability, and so on. To address the great challenge, software defined networking (SDN) has been applied to vehicular networks to improve the user experience through providing high-performance communications between the vehicular network nodes, reconstructing the vehicular network structure, and optimizing the networking coverage, system security, communication latency, and so on [2]. It can be expected that in future network configuration, various terminals, such as vehicles, will be added to the network. The traditional network structure is not conducive to managing and controlling a large number of network nodes, so they should be part of the control functions that are distributed to the edge of the network, especially in the Internet of Things (IoT) [3]. In particular, the technology of distributed computing can be used in the scenario of vehicle communication in IEEE 802.11p to improve the service quality of vehicular networks. In [4], Liu *et al.* investigate the scheduling for cooperative data dissemination in a hybrid I2V and V2V communication environment. Specifically, an approach based on a centralized scheduler at the roadside unit (RSU) is proposed to represent the first known VANET implementation of the SDN concept.

However, the existing SDN applications in the vehicular network place more attention on V2V, V2I, and even in-vehicle power line communication for data transmission [5–7], while the controller area network (CAN) is still limited to some particular applications, such as, entertainment, navigation, and location-based services, which only provide users with basic services but cannot meet the demands in a complex driving environment. Especially for driver safety, V2V and V2I can provide drivers with vehicular information to reduce the frequency of traffic accidents. For example, safety distance reminders, safety speed alerts, pedestrian reminder, collision avoidance reminders, traffic guidance, and other services can be provided. However, the current CAN cannot easily monitor drivers' physiological and psychological states to avoid traffic accidents due to drivers' fatigue and moods. Therefore, this article proposes an SDN-based approach to develop a safety-oriented vehicular CAN (SOVCAN), which can guarantee traffic safety from the following two aspects.

Drivers' Fatigue Detection: According to statistics, fatigue can significantly reduce a driver's vigilance and increase reaction time, which is an important cause of traffic accidents. Through a camera detecting the state of a driver's eyelids and the frequency of a driver's slight nodding. the system can effectively find the micro sleep behavior, and then alert and warn the driver to prevent traffic accidents.

This work was supported in part by the China National Natural Science Foundation under Grants 61572220 and 61572538, the National Key Research and Development Program of China under Grant 2016YFB0201900, and the Applied Basic Research Program funded by Wuhan Science and Technology Bureau under Grant 2017010201010118. Min Chen is the corresponding author.

Digital Object Identifier: 10.1109/MCOM.2017.1601185

Yin Zhang is with Huazhong University of Science and Technology and Zhongnan University of Economics and Law; Min Chen is with Huazhong University of Science and Technology; Nadra Guizani is with Purdue University; Di Wu is with Sun Yat-sen University; Victor C. M. Leung is with the University of British Columbia.

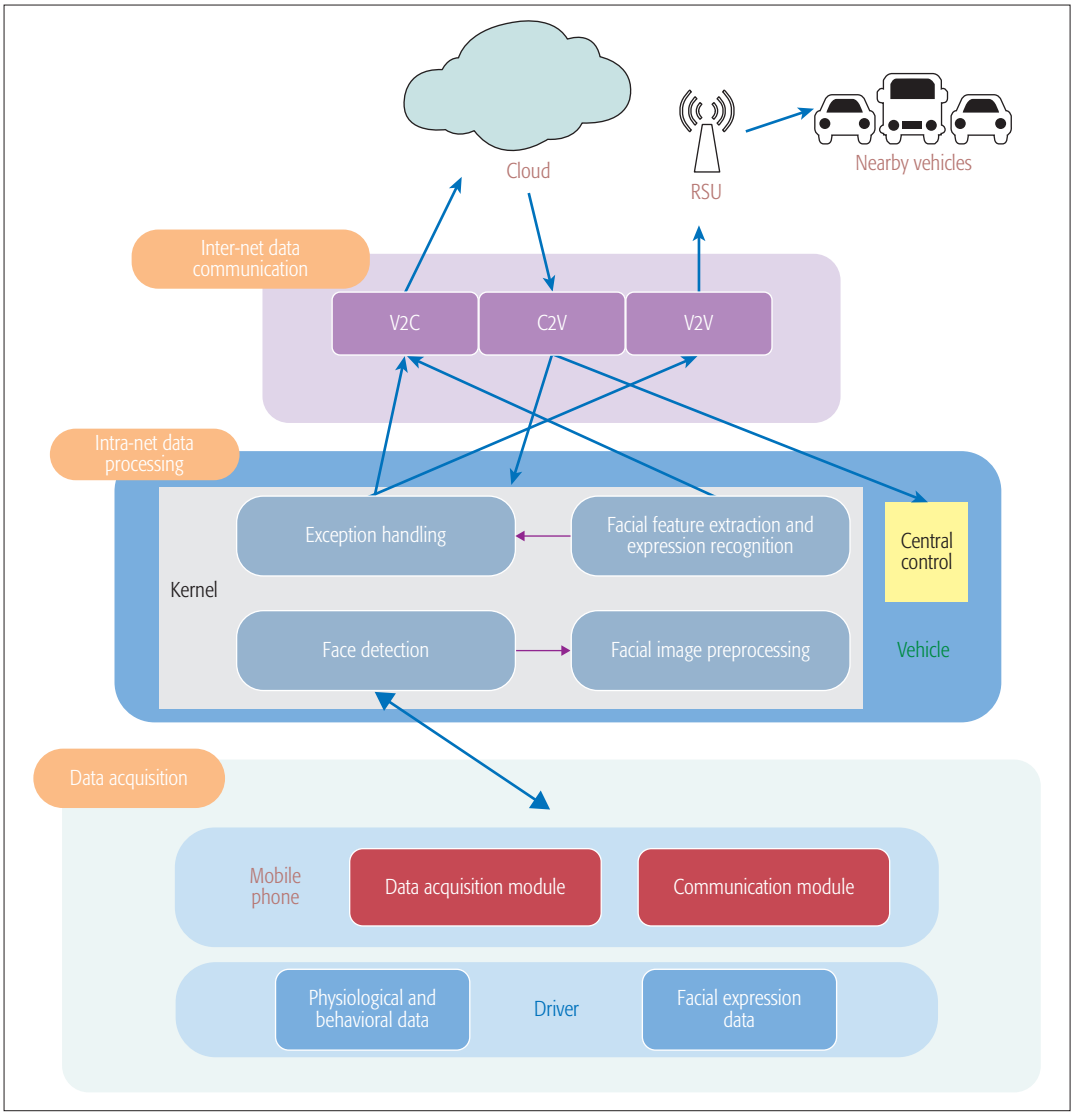


Figure 1. SOVCAN architecture.

Through vehicle-to-vehicle, infrastructure-to-vehicle and vehicular-to-infrastructure communications, which are the foundation and key support technologies determining the overall performance of vehicular networks, road safety and traffic efficiency are significantly improved.

Drivers' Emotional Recognition: In recent years, road congestion and other external factors induced by drivers' emotional abnormalities, leading to open gambling cars or even malicious acts toward pedestrians or other vehicles, have caused major hazards affecting traffic safety. Through the expression recognition and emotional computing method, the system can find drivers' mood swings and effectively avoid road rage.

The remainder of this article is organized as follows. We first present the three-tier architecture of SOVCAN. Specifically, data acquisition, intra-CAN data processing, and inter-CAN data communication layers are described. Then we conclude the article.

SOVCAN Architecture

As shown in Fig. 1, SOVCAN consists of three layers: data acquisition, intra-net data processing, and inter-net data communication.

Data Acquisition: In this layer, drivers' physiological information including responses are collected. The acquisition of physiological signals depends mainly on wearable devices, and physiological response data collection depends on the camera, which can be fused for more comprehensive facial feature extraction and expression recognition [8].

Intra-Net Data Processing: Perceptual data is first transmitted to the onboard intelligence device for analysis, including fatigue identification and emotion perception. If the analysis result of driving state is abnormal, SOVCAN will immediately indicate the car in the vehicular control system for emergency treatment, such as braking, alarming, and speed limiting. Traditional mobile-phone-based computing is different. The vehicle can provide a wealth of resources, particularly energy, and in the SOVCAN computational complexity is not too high. Hence, almost all of the data analysis can be done locally, and the communication overhead can be reduced.

Inter-Net Data Communication: Although most of the data processing can be done within the CAN, in order to retain the driver's data for a long time, we also need to transfer these data to the cloud for preservation. In particular, when the driver changes terminal, it can also download its feature information from the cloud to reduce the time initializing the device. In addition, through the inter-network data communication, we can also send abnormal information to the cloud and

nearby equipment to warn nearby pedestrians and take appropriate emergency measures.

It should be noted that, taking into account feasibility and compatibility, this article uses the smartphone as the CAN hub to provide data acquisition, computing resources, network access, and vehicle control system docking.

Data Acquisition

The system mainly collects two types of data: physiological behaviors and facial expressions through a camera. The data for physiological behaviors is to detect driver fatigue and facial expressions for emotion detection.

Physiological and Behavioral Data Acquisition

At present, there are three main methods of fatigue detection: physiological-signal-based detection, traffic-data-based detection, and physiological-behavior-based detection.

Physiological signals may accurately reflect the extent of human fatigue, and electroencephalography (EEG) [9], heart rate variability (HRV) [10], and so on. This can effectively detect the extent of a person's fatigue. However, these intrusive detection techniques rely on special acquisition devices and can reduce the driver's user experience and hinder normal driving. Moreover, some research indicates that the degree of fatigue can be measured by the steering wheel steering angle and lateral position of the vehicle and other variables in the process of driving traffic data [11]. However, because such methods often require retrofitting existing vehicles, such as the installation of sensors, it is difficult for them to be widely used.

Fatigue testing based on physiological behaviors to analyze the drowsiness of people will need to discover people's fatigue states. For example, the behavior of the eyelid and the head can accurately reflect whether the driver has dozed off [12]. Such methods only need an image capture device to record physiological behavior of the driver and can determine whether he/she is in a state of fatigue. This acquisition method can be very compatible with existing vehicles. Thus, the method in this article is to collect drivers' real-time behaviors by placing a cell phone in the cab.

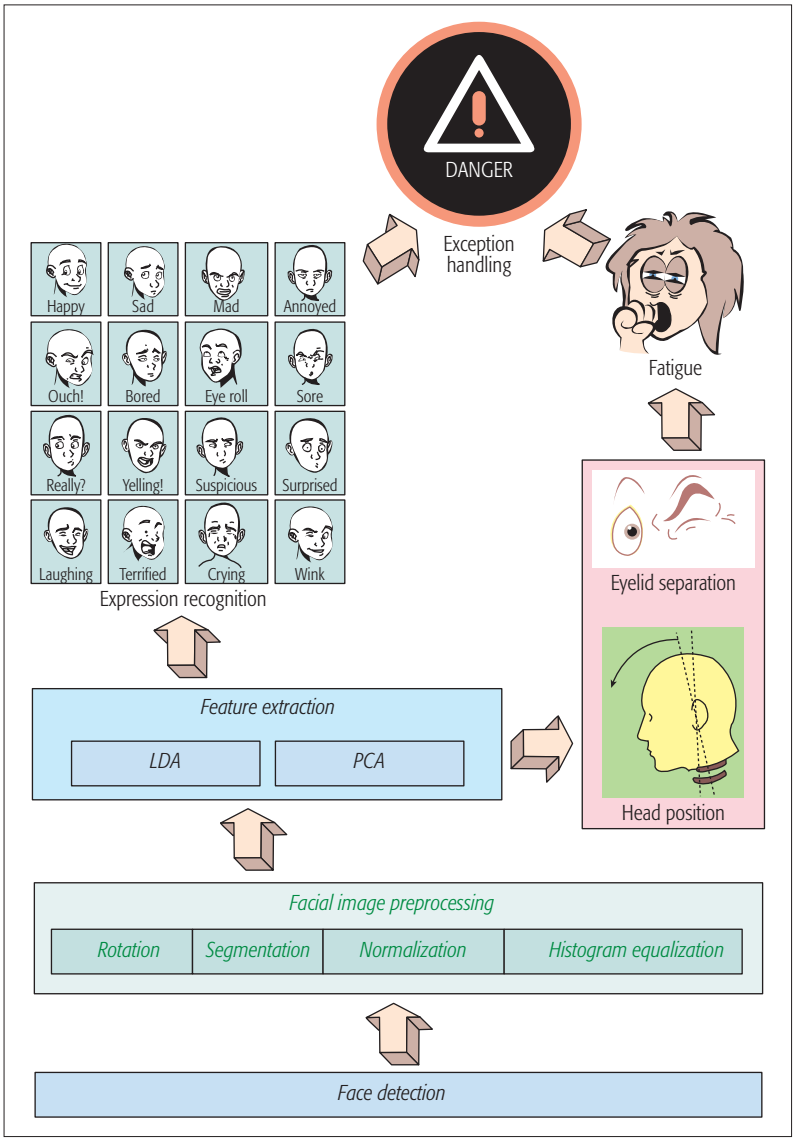


Figure 2. Intra-net data processing.

Facial Expression Data Acquisition

Sentiment analysis is a complex field of study. Currently, it can be divided into three categories:

- Physiology-signal-based emotion analysis [13]
- External-based emotion analysis [14]
- Facial-expression-based emotion analysis [15].

However, based on the way the physiological signal depends on an invasive device to acquire physiological signals, text-based emotion analysis applied to the scenarios has many text resources, such as social networking. These two methods are not applicable to CAN. We only need to record the driver's face image or video and use technologies like image and video segmentation and pattern recognition to analyze the emotional state. The fusion of facial-expressions-based emotion analysis and physiological behavior data collection methods reduce the system overhead and complexity greatly.

Intra-Net Data Processing

The face image acquired by the camera of the mobile phone will be used for fatigue detection and emotion recognition. Its essence is real-time image processing for the driver. As shown in Fig. 2, it includes the following steps: face detection, facial image preprocessing, face geometry extraction and expression recognition, and exception handling.

Face Detection

Face detection is the most important basis for facial expression recognition, which is the basic step for subsequent facial expression preprocessing. Facial expression is the basis of feature extraction and classification. Face detection is to detect the face from an image, extract the face information (eye, nose, etc.), and locate the face position.

Facial Image Preprocessing

Preprocessing of a facial image is essential for expression recognition. First, the result of the above face detection can identify the approximate facial area. Then we can find the location of the eyes and nose in the region. According

to these locations, we can correct the face accurately and do operations such as position correction, scaling, and grey level normalization. After preprocessing, we get most of the regions that are related to the expression. Then we need to exclude some areas unrelated to the expression, such as background, ears, hair, neck, and shoulders, and normalize the size and gray value of the obtained expression areas to reduce the light and the impact of light intensity as much as possible.

Facial Feature Extraction and Expression Recognition

We face image preprocessed dimension reduction, feature extraction's main geometric features, such as eyes, nose, eyebrows, mouth, and other positions, and change its position and measure to determine its size andshape, including distance and proportion. One of the most important features is the geometric characteristics of the eye. The location of the eye can determine the relative displacement of the head, so we can determine whether the driver has micro-sleep-induced nodding behavior. In addition, depending on the closed state of the eyelids, the blink frequency of the driver can be used to estimate the degree of drowsiness of the driver. By using the classifier, we can divide the facial geometric feature space into type space. According to the facial expression database, it is accurate to determine in which emotion the driver's current facial expression belongs.

In our proposal, principal component analysis (PCA) and linear discriminant analysis (LDA) are used for facial feature extraction. In particular, PCA is a reproducible approach to reduce data dimension, while LDA is an effective approach to reduce data dimension and classify data.

Exception Handling

Once the driver is in a state of fatigue or an unusual mood, the vehicle terminal will immediately direct the vehicle control system to take some measures such as acknowledging a warning, emergency braking, and speed limiting.

Inter-Net Data Communication

As shown in Fig. 3, inter-network data communications include three approaches: vehicle-to-cloud (V2C), cloud-to-vehicle (C2V), and V2V.

Vehicle to Cloud

With the resources provided by vehicles, a vehicle terminal can complete most local tasks without offloading any to the cloud for processing. However, in the following scenarios, the CAN still needs to transfer local data to the cloud.

Data Uploading: As most of the data collected in the SOVCAN is video, it requires considerable storage space. Although the local equipment can provide a certain storage capacity, it cannot meet the needs of actual use. For example, the smartphone used in the system can provide 32 GB of storage space to store only 480 min of video with resolution of 1280 × 720. In addition, the training of historical data and analysis is available to improve the accuracy of facial expression classification. Therefore, it is necessary to upload the data to the cloud and save them in the cloud.

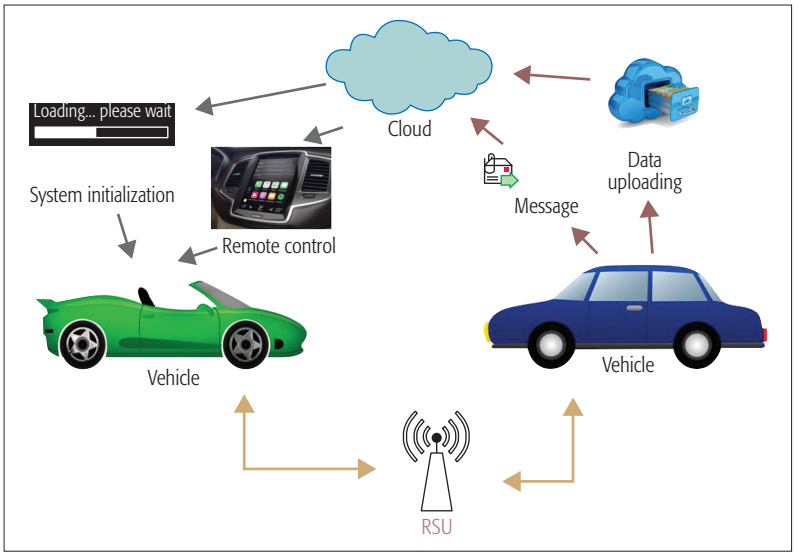


Figure 3. Inter-net data communication.

The real-time requirements for such data transmission are not high, so it mainly uses vehicle-to-RSU (V2RSU), WiFi, and other low-cost means of communication methods.

Message Delivery: It mainly includes requesting messages and exception messages. A requesting message is the message that needs to be sent to the cloud when a vehicular device is initialized or a software error occurs. It indicates that the relevant functional components need to be transferred to the local smart device. When the system finds driver fatigue or abnormal emotion, an exception message will be sent to the cloud for further exception handling. The size of this kind of message is small, and the message is in real time. Hence, in the absence of a low-cost means of communication, it will communicate directly through the mobile network.

Cloud to Vehicle

Depending on the condition of the vehicle, the cloud will also send some data to the vehicle, including system initialization data and remote control messages.

System Initialization: In order to ensure the normal operation of the SOVCAN system, the necessary system function modules must be downloaded from the cloud to the local level, such as to a data processing module, when a vehicle's intelligent equipment is installed or recovered. The scale of the system initialization data is large, and the data is the core of the system. We must exclude the cost and download it to the local level. However, due to its common data, it can be considered to be cached to the equipment at the edge of the vehicular network for improving the download speed and reducing the communication costs.

Remote Control: In extreme cases, when the driver cannot guarantee safe driving, the cloud can send emergency braking commands, controlling the vehicle remotely. The quantity of this kind of control data is small, but its real-time nature is extremely strong. Therefore, no matter how much it may cost to communicate, we must transmit the control information to the onboard intelligent equipment.

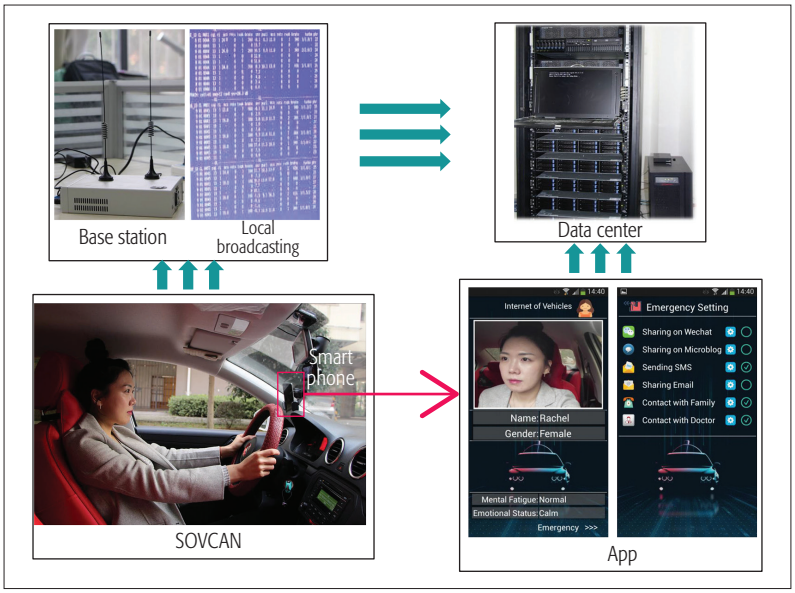


Figure 4. Testbed for SOVCAN.

Vehicle to Vehicle

In addition to the communication between the vehicle and the cloud, there is data communication between vehicles. When SOVCAN detects that the driver's status is abnormal, it will send warning information to nearby vehicles to prompt other drivers to avoid the high-risk driving behavior that the vehicle may incur. Inter-vehicle communication in such scenarios is different from traditional V2V. In conventional V2V, communication between vehicles includes direct communication between vehicles, RSU communication, and base station communication. The V2V communication in SOVCAN is intended to broadcast a reminder message to nearby vehicles. Direct communication between vehicles is too inefficient, and the base station (BS) coverage area is large an hence does not apply to this scenario. Thus, V2V communication uses RSUs to broadcast to nearby vehicles, and the efficiency and cost of this communication are better.

A Testbed for SOVCAN

In order to evaluate the availability of the proposed scheme, we developed a testbed for SOVCAN, which is expected to provide safety-oriented vehicular service based on smartphones through CAN.

Testbed Architecture

As shown in Fig. 4, the SOVCAN-based testbed consists of a smartphone, a BS, and a data center (DC). The detailed mechanism is described as follows.

Smartphone: In SOVCAN, the smartphone plays the most important role to support data sensing and communication. Moreover, with with special software (an Android app) developed by the Embedded and Pervasive Computing (EPIC) Lab at Huazhong University of Technology and Science installed, the smartphone can provide more complex services, including fatigue monitoring, emotion recognition, emergency contact, and so on.

Base Station: In the testbed, a Long Term Evolution (LTE) BS is implemented as an RSU to support V2I and V2V communications. Specifically, through V2I the data is transmitted from the vehicle to the BS, which provides the connection to the cloud. In the V2V communication, once the abnormal statuses are detected and transmitted to the BS, a warning broadcast will be made to the vehicles accessing the BS. In the testbed, Amari LTE is deployed, which includes Iteenb as the LTE access network and LTE mobile management entity (LTE MME) software as the LTE core network involving a service gateway (SGW), packet data network gateway (PGW), home subscriber server (HSS), and so on. The hardware consists of a radio frequency unit, a high-performance computer, and an LTE terminal.

Data Center: In the cloud, a DC, the Inspur In-Cloud Smart Data Appliance, is implemented to provide more storage and computing resources. Specifically, it consists of two main clusters:

1. An admin cluster with 2 nodes, providing 64 CPU cores, 256 GB of RAM, and 3.6 TB of storage
2. A worker cluster with 7 nodes, providing 84 CPU cores, 336 GB of RAM, and 252 TB of storage

In particular, the sensory data is transmitted and stored in the DC as historical data to improve the learning model, while some computation-intensive tasks are offloaded to the DC.

Experiment

In order to verify the availability of SOVCAN in the actual environment, an experiment is designed for evaluation. In this experiment, four volunteers drive the same car deploying SOVCAN about 40 minutes on the same routes. In particular, the route includes normal roads and a long tunnel.

Figure 5 illustrates the recognition accuracy of SOVCAN in this experiment. Through the experiment, the recognition accuracy in the tunnel is obviously lower than that in the normal environment, because the light is darker in the tunnel, which causes a significant negative effect on image processing. Of course, it is simple to verify the availability of SOVCAN, so we do not design more comprehensive experiments including the consideration of more traffic conditions and the external environment, or comparison with other related approaches.

Open Issues and Future Directions

Although the testbed is able to provide the essential services for vehicle safety, more details are not considered for improving the availability and performance.

Low Delay: In order to improve the accuracy of fatigue monitoring and emotion recognition, more physiological and psychological data should be sensed, processed, and transmitted through SOVCAN. In particular, safety message transmissions have a very low delay constraint, such as less than 1 ms.

Frequent Handover: In SOVCAN, the communications between the vehicles, RSU, and cloud are frequently handed over, which is a huge issue for providing reliable communication.

Highly Efficient Services: For the future CAN, vehicular smart devices are not only the control platform but also entertainment centers for users. Different multimedia services need to be provided by vehicular networks. It is a great challenge to improve the service efficiency.

Robustness: The experiment illustrates that recognition accuracy is strongly related to external factors. For example, some accessories on a driver's face significantly affect facial expression recognition, such as glasses or a scarf. Moreover, the quality of the sensory image is limited under some circumstances, such as on bumpy roads or in insufficient light, which considerably lower the system performance.

Conclusion

The rapid development of vehicular networking has brought revolutionary changes to society, covering almost every aspect of daily life. More and more applications, systems, and services for vehicular networking are being expanded. This article proposes SOVCAN, which aims to detect drivers' fatigue and mood swings in CAN to guarantee safe driving. Specifically, according to the different requirements of data communication in SOVCAN, we use SDN technology in three different scenarios: V2C, C2V, and V2V. According to the different demands for real-time communication, efficiency, and cost, appropriate communication is selected in the SDN-based architecture.

In our current work, there are still some technical challenges. In particular, the most critical problems are lack of robustness in facial feature extraction and expression recognition, road bumps obscuring the collection of facial images, and the complex cab background affecting the accuracy of detection in the network data processing. Therefore, in the future, we will try to use non-invasive wearable technology under the premise of keeping the normal driving behavior such as smart clothing to improve the robustness of the system.

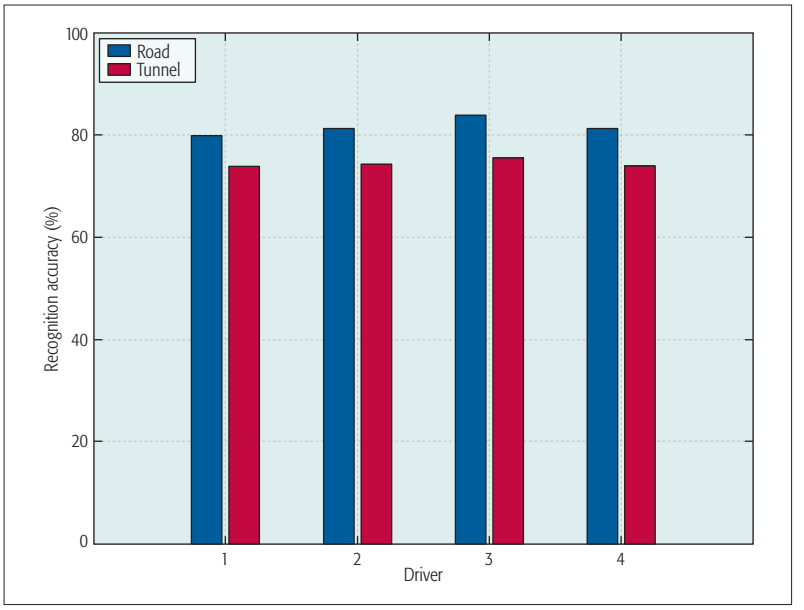


Figure 5. Recognition accuracy of SOVCAN.

References

[1] K. Zheng *et al.*, "Soft-Defined Heterogeneous Vehicular Network: Architecture and Challenges," *IEEE Network*, vol. 30, no. 4, 2016, pp. 72–80.

[2] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Software-Defined Networking for RSU Clouds in Support of the Internet of Vehicles," *IEEE Internet of Things J.*, vol. 2, no. 2, 2015, pp. 133–44.

[3] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2347–76.

[4] K. Liu *et al.*, "Cooperative Data Scheduling in Hybrid Vehicular Ad Hoc Networks: VANET as a Software Defined Network," 2015.

[5] Z. Sheng *et al.*, "A Multichannel Medium Access Control Protocol for Vehicular Power Line Communication Systems," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 2, Feb. 2016, pp. 542–54.

[6] D. Tian *et al.*, "A Dynamic and Self-Adaptive Network Selection Method for Multimode Communications in Heterogeneous Vehicular Telematics," *IEEE Trans. Intell. Transp. Sys.*, vol. 16, no. 6, 2015, pp. 3033–49.

[7] Y. Huo *et al.*, "Queuing Enhancements for In-Vehicle Time-Sensitive Streams Using Power Line Communications," *2015 IEEE/CIC Int'l. Conf. Commun. in China*, Nov 2015, pp. 1–6.

[8] G. Fortino *et al.*, "A Framework for Collaborative Computing and Multi-Sensor Data Fusion In Body Sensor Networks," *Info. Fusion*, vol. 22, 2015, pp. 50–70.

[9] C.-T. Lin *et al.*, "Development of Wireless Brain Computer Interface with Embedded Multitask Scheduling and Its Application on Real-Time Driver's Drowsiness Detection and Warning," *IEEE Trans. Biomedical Engineering*, vol. 55, no. 5, 2008, pp. 1582–91.

[10] M. Patel *et al.*, "Applying Neural Network Analysis on Heart Rate Variability Data to Assess Driver Fatigue," *Expert Systems with Applications*, vol. 38, no. 6, 2011, pp. 7235–42.

[11] S. Taheri, P. Turaga, and R. Chellappa, "Towards View-Invariant Expression Analysis Using Analytic Shape Manifolds," *2011 IEEE Int'l. Conf. IEEE Automatic Face & Gesture Recognition and Wksps.*, 2011, pp. 306–313.

[12] P. R. Tabrizi and R. A. Zoroofi, "Open/Closed Eye Analysis for Drowsiness Detection," *2008 1st IEEE Wksp. Image Processing Theory, Tools and Applications*E, 2008, pp. 1–7.

[13] B. Hu *et al.*, "Eeg-Based Cognitive Interfaces for Ubiquitous Applications: Developments and Challenges," *IEEE Intelligent Systems*, vol. 26, no. 5, 2011, pp. 46–53.

[14] J. Wiebe, "Learning Subjective Adjectives from Corpora," *AAAI/IAAI*, 2000, pp. 735–40.

[15] D. D. Patil and S. G. Deore, "Medical Image Segmentation: A Review," *Int'l. J. Computer Science and Mobile Computing*, vol. 2, no. 1, 2013, pp. 22–27.

Biographies

Yin Zhang [M'13, SM'16] (yin.zhang.cn@ieee.org) is an assistant professor in the School of Information and Safety Engineering, Zhongnan University of Economics and Law (ZUEL), China, and a research fellow in the Embedded and Pervasive Computing Lab,School of Computer Science and Technology,Huazhong University of Science and Technology (HUST). He is an Excellent Young Scholar at ZUEL. He is Vice-Chair of the IEEE Computer Society Big Data Special Technical Community (STC). His research interests include intelligent service computing, big data, and social networks, and so on.

Min Chen [SM'09] (minchen2012@hust.edu.cn) has been a full professor in the School of Computer Science and Technology at HUST since February 2012. He is Chair of the IEEE Computer Society STC on big data. His Google Scholars Citations reached 9300+ with an h-index of 48. He received the IEEE Communications Society Fred W. Ellersick Prize in 2017. His research focuses on cyber physical systems, IoT sensing, 5G networks, mobile cloud computing, SDN, healthcare big data, medical cloud privacy and security, body area networks, emotion communications, robotics, and so on.

Nadra Guizani (nguizani@purdue.edu) is a Ph.D. student and graduate lecturer at Purdue University, completing a thesis on prediction and access control of disease spread data on dynamic network topologies. Her research interests include machine learning, mobile networking, large data analysis, and prediction techniques. She is an active member in both the Women in Engineering Program and the Computing Research Association for Women.

Di Wu [SM] (wudi27@sysu.edu.cn) is a professor and assistant dean in the School of Data and Computer Science,Sun Yat-sen University, Guangzhou, China. He is a member of ACM and Sigma Xi. His research interests are broadly in the areas of networking and distributed systems, cloud computing, big data analytics, network security, and so on.

Victor C. M. Leung [S'75, M'89, SM'97, F'03] (vleung@ece.ubc.ca) is a professor of electrical and computer engineering and holder of the TELUS Mobility Research Chair at the University of British Columbia. He has co-authored more than 1000 technical papers in the area of wireless networks and mobile systems, in addition to 37 book chapters and 12 book titles. He is a Fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada.

Data Offloading in 5G-Enabled Software-Defined Vehicular Networks: A Stackelberg-Game-Based Approach

Gagangeet Singh Aujla, Rajat Chaudhary, Neeraj Kumar, Joel J. P. C. Rodrigues, and Alexey Vinel

To make intelligent decisions for data offloading, an SDN-based scheme is proposed by the authors. In the proposed scheme, an SDN-based controller is designed that makes decisions for data offloading by using the priority manager and load balancer. Using these two managers in SDN-based controllers, traffic routing is done efficiently even with an increase in the size of the network.

ABSTRACT

Data offloading using vehicles is one of the most challenging tasks to perform due to the high mobility of vehicles. There are many solutions available for this purpose, but due to the inefficient management of data along with the control decisions, these solutions are not adequate to provide data offloading by making use of the available networks. Moreover, with the advent of 5G and related technologies, there is a need to cope with high speed and traffic congestion in the existing infrastructure used for data offloading. Hence, to make intelligent decisions for data offloading, an SDN-based scheme is presented in this article. In the proposed scheme, an SDN-based controller is designed that makes decisions for data offloading by using the priority manager and load balancer. Using these two managers in SDN-based controllers, traffic routing is managed efficiently even with an increase in the size of the network. Moreover, a single-leader multi-follower Stackelberg game for network selection is also used for data offloading. The proposed scheme is evaluated with respect to several parameters where its performance was found to be superior in comparison to the existing schemes.

INTRODUCTION

The vehicular network is an emerging technology to provide mobile users with the flexibility to use various services such as entertainment and navigation on wheels. With the help of the IEEE 802.11p/WAVE protocol, vehicles are connected to the Internet seamlessly. Vehicular networks provide an easy way to improve the comfort and safety levels of passengers using short-range wireless communication, such as Bluetooth, hotspots, Zigbee, radio frequency identification, and near field communication. The packets are broadcasted from the source node (vehicles) to the destination using various routing protocols. Vehicles communicate with each other using different communication models such as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-portable (V2P), and infrastructure-to-infrastructure (I2I) communication [1]. By using the aforementioned modes of communications, information is transmitted to vehicular users in different modes (e.g., unicast, multicast, and broadcast transmission). The mobile transportation services are managed by nearby intelligent routers like roadside units (RSUs).

The three major components that act as the backbone for communication between the vehicles and with the infrastructure are the RSU, onboard unit (OBU), and application unit (AU). Figure 1 shows the architecture and communication layout of vehicular networks. Routing in vehicular networks depends on various parameters such as rapidly changing network topology, direction of vehicles' motion, bandwidth limitation, delay incurred, vehicles' speed, connectivity, and signal fading. Various protocols used in vehicular networks are classified as *topology-driven routing* and *geographical-based routing* [1].

VEHICULAR NETWORKS USING CELLULAR TECHNOLOGIES

The communications in vehicular networks (e.g., V2I, V2P, and I2I) are based on the concept of RF-based cellular technology. Cellular technology provides services to users by reusing the available frequency bands for uplink (reverse link) and downlink (forward link). Each channel of particular frequency is allocated for communication by dividing it into frequency bands. The communication channel is affected by various factors, as shown in Table 1 [2, 3]. Various wireless communication technologies are used for providing services to moving vehicles, but it has inherent challenges. With the advent of 5G, these challenges have further grown to a higher level. Some of these challenges are high mobility of vehicles, network congestion, traffic engineering, energy efficiency, load balancing, quality of service (QoS), bandwidth limitation, high data rate requirement, lower latency requirements, security, privacy, and fading of signal strength. Hence, to overcome the aforementioned challenges, data offloading schemes are widely adopted by the research community. However, data offloading is a challenging task in view of the current fifth generation (5G) scenario.

DATA OFFLOADING IN 5G SCENARIO

Data offloading is used to manage huge network traffic using various available networks. Generally, the cellular bands have issues related to the

Gagangeet Singh Aujla, Rajat Chaudhary, and Neeraj Kumar are with Thapar University; Joel J.P.C. Rodrigues is with National Institute of Telecommunications (Inatel), Brazil; Instituto de Telecomunicações, Universidade da Beira Interior, Portugal; ITMO University, St. Petersburg, Russia , and University of Fortaleza (Unifor), Brazil; Alexey Vinel is with Halmstad University.

Digital Object Identifier:
10.1109/MCOM.2017.1601224

0163-6804/17/$25.00 © 2017 IEEE

shortage of spectrum bandwidth. Thus, other available cellular bands and networks are used to manage the load. In this case, the traffic is diverted to unlicensed WiFi spectrum or other network technologies, which helps to reduce the load on the existing cellular bands. Users from 3G, 4G, or 5G networks can utilize data offloading schemes in an affordable and flexible manner, thereby building a heterogeneous network by integrating WiFi with radio networks for 4G/5G users. The advantage of data offloading is unleashing better resource and spectrum utilization. One popular approach for data offloading is device-to-device (D2D) communication.

Types of Data Offloading

The overall objective of data offloading is to maintain QoS at various levels. For this purpose, different types of data offloading mechanisms exist in the literature. Some of these are described as follows.

WiFi Offloading: WiFi is provided to the end users using IEEE 802.11 standards and works like a radio access network for broadband services. By WiFi offloading, traffic is diverted from cellular services to free unlicensed IEEE 802.11 links. One method of data offloading is *unmanaged data offloading* or *network bypassing*. In this method, data services are shifted to nearby WiFi coverage by completely bypassing the cellular network. However, the voice services are managed by the core cellular network. The second method is *managed data offloading* in which an intelligent session-aware gateway is implemented to control the network access by different subscribers. Data services are managed by the intelligent gateway, which forwards the WiFi session data to the Internet. However, it does not entertain any other subscribed content until the session is over. The third method is *integrated data offloading* where cellular and WiFi networks are integrated by loosely coupled and tightly coupled networks [4].

IP Flow Mobility: An IP flow is defined as a sequence of IP packets along with information like IP addresses, port numbers, and transport protocols. It consists of *host-based IP flow mobility* and *network-based IP flow mobility management*. For *host-based IP flow mobility*, mobile IPv6 is used [5]. Concurrently, multiple IP flows such as video, VoIP, and file download are transmitted over the wireless link. Mobile IPv6 allows the IP flow to shift from one wireless link to the other while maintaining QoS on the move. It maintains session continuity without any interruption while exchanging signals. For *network-based IP flow mobility*, proxy mobile IPv6 protocol is used [5].

Wireless Communication Technologies for Data Offloading

Due to the large volumes of wireless traffic, the 5G network is a new, cutting edge technology that provides best and reliable services to vehicular networks. In 5G network architecture, various methods are used for transmission. Different wireless communication technologies such as small cell base stations, massive multiple-input multiple-output (MIMO) technology, and millimeter-wave (mmWave) communication technologies can be used. These communication technologies are discussed below.

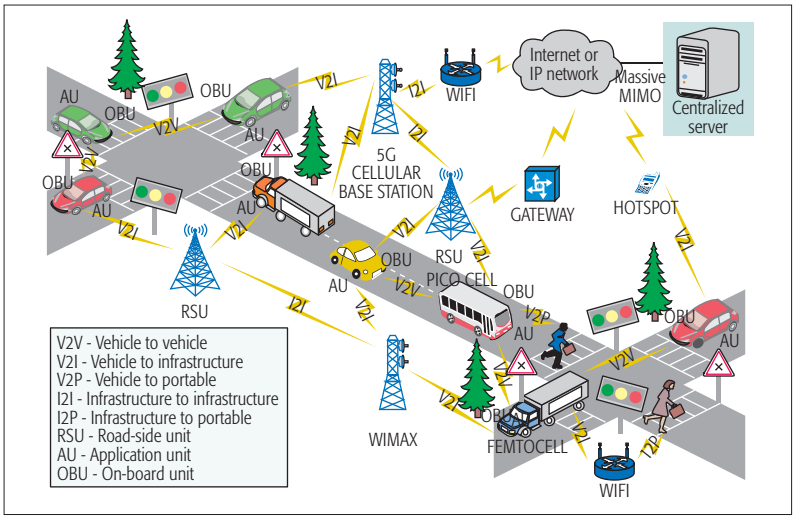


Figure 1. Vehicular network architecture.

Massive MIMO: Massive MIMO is an innovative technology based on large-scale arrays of antenna terminals that are integrated into every base station. Its main objective is to improve the throughput, and energy and spectral efficiency. Every active terminal uses time and frequency division operation. Each active antenna is connected using fiber optic cable. The spectrum efficiency depends entirely on the number of available antenna base stations. Hence, thousands of antennas transmit streams of data to multiple active antennas at a time.

mmWave: It is used to provide high bandwidth transmission, potentially at gigahertz scales. It is very useful in ultra dense networks (UDNs). MmWave with 5G networks uses short-range applications with higher data rate traffic (gigabits per second) compared to 4G. It utilizes unlicensed V-band and licensed E-band. At base stations, massive MIMO is deployed, and mmWave communication is equipped at the antennas of small cell base stations. With this, V-band covers the range of 500–700 m and frequency of 57–67 GHz, while E-band covers range in kilometers with frequency of 71–76, 81–86, and 92–95 GHz [6].

Small Cell Cellular Base Station: By small cells, we mean low-power and low-cost access point cellular base stations. Various types of small cells are femtocells (up to 10–50 m), picocells (100–200 m), microcells (500 m–2 km), and macrocells (30–35 km). These cells are quite useful for indoor environments like office buildings, homes, buses, and shopping malls. These can be deployed in nearby regions in order to extend the cell region. They help to reduce the co-channel interference, and the majority of traffic can be offloaded from macrocell networks [7].

Data Offloading Using Delay-Tolerant Networks

In recent years, delay-tolerant networks (DTNs) have been used to migrate cellular traffic using data offloading schemes. By exploiting the delay-tolerant nature of various non-real applications, service providers can shift the load to DTNs. In this way, multiple mobile data offloading through DTNs can play a vital role in reducing congestion in cellular communication. However, a DTN has its own limitations in terms of limited

Generations	1G	2G	2.5G	2.75G	3G	3.5G	4G	5G
Technology	Analog Voice	GSM	GPRS	EDGE	CDMA 2000	HSPA	WI-FI	IPV6 LAN/WAN/PAN
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	TDMA, CDMA	CDMA	CDMA	CDMA, OFMA	CDMA, BDMA
Switching	Circuit	Circuit, Packet	Packet	Packet	Packet	Packet	Packet	Packet
Band type	Narrow	Narrow	Narrow	Narrow	Broadband	Wideband	Ultra wide	Ultra wide
Handoff	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal, vertical	Horizontal, vertical
Main network	PSTN	PSTN	GSM, TDMA	WCDMA	Packet	GSM, TDMA	Internet	Internet
Carrierfrequency	30 kHz	200 kHz	200 kHz	200 kHz	5 MHz	5 MHz	15 MHz	15 MHz
Bandwidth	150 kHz	5–20 MHz	5–20 MHz	5–20 MHz	25 MHz	25 MHz	100 Mhz	1–2 GHz
Data rate	2.4–14.4 kb/s	14.4–64 kb/s	64–200 kb/s	470 kb/s	3.1–14.7 Mb/s	14.4–63 Mb/s	100 Mb/s–1 Gb/s	1 Gb/s and above
Features	Voice only	Data, voice	Data, voice	Data, voice	Data, voice	HD data, voice	Ultra HD, VOIP	Ultra HD, VOIP

Table 1. Characteristics of cellular technology generations.

storage, battery, and opportunistic communication contacts. Hence, various schemes such as greedy, optimal, and approximation algorithms have been used to handle the data offloading. In this regard, Li *et al.* [8] considered the maximum data offloading as a sub-modular function maximization problem and solved it using the optimal, greedy, and approximation algorithms to resolve the network congestion issue.

Stackelberg Game and Its Applications

A Stackelberg game is a two-period game with a concept of leader and follower [9]. Both leader and follower try to maximize their profits. Hence, it provides dual benefit to both players of the game. Stackelberg game has been extensively adopted for solving real-time problems in various fields like congestion control, channel allocation, network selection, and network design for vehicular networks, UDNs, and data center networks. In [9], a multi-leader multi-follower Stackelberg game has been adopted for mobile users to select the optimal network among WiFi, small cells, and macrocell. The proposed game helps mobile users select the optimal network according to different network metrics. Also, the Stackelberg game has been deployed to increase the network coverage and improve the overall throughput of UDNs [10].

Contributions

Keeping in view all the above issues, the fusion of programmable software-defined networking (SDN) with data offloading could manage the requirements of vehicles in the 5G scenario. Hence, the following major contributions are presented in this article:

- An SDN-based controller is designed for data offloading in vehicular networks.
- A data offloading scheme for software-defined vehicular networks is designed comprising a priority manager and a load balancer.
- A single-leader multi-follower Stackelberg game is proposed for network selection in the data offloading scheme for software-defined vehicular networks.

SDN-Based Controller

Traditional networks are hardware-based, and consist of distributed or decentralized architecture. The forwarding devices (FDs) such as routers, gateways, and switches are used to route the packets from source to destination. The strong coupling between the control and data planes has created enormous complexity in network management and configuration. It becomes difficult to add new networking functionalities and policies. Such networks are prone to network congestion and are unsuitable for handling the increased network traffic. SDN is a promising technology to provide high flexibility and scalability with minimal cost and network congestion. Figure 2a shows its three major components, listed below:

- SDN controller
- FDs
- Application programming interfaces (APIs)

Its architecture basically consists of three decoupled planes: data, control, and application planes [11]. The functionality of all these planes are discussed as follows.

SDN Data Plane

The data plane in SDN is made up of all the FDs like OpenFlow physical switches, OpenFlow virtual switches, OpenFlow routers, and OpenFlow gateways [11]. All the forwarding decisions are made by the SDN controller at the control plane using the logic and programming instructions. This instruction set is installed on the FDs using a southbound interface (SBI) and drivers. The instruction set contains the forwarding decisions to be made for each incoming packet. Each FD contains a list of flow and group tables that are linked by a pipeline. In the flow table, the instruction set contains three units:, rule, action, and statistics. The rule contains sequence number, IP address, medium access control (MAC) address, virtual LAN address, port number, and transport protocols [12]. The actions taken by the forwarding devices includes forwarding, discarding, modifying, replicating, encapsulating, and tunneling of the packet. Finally, the statistics contains a counter for reporting to the controller.

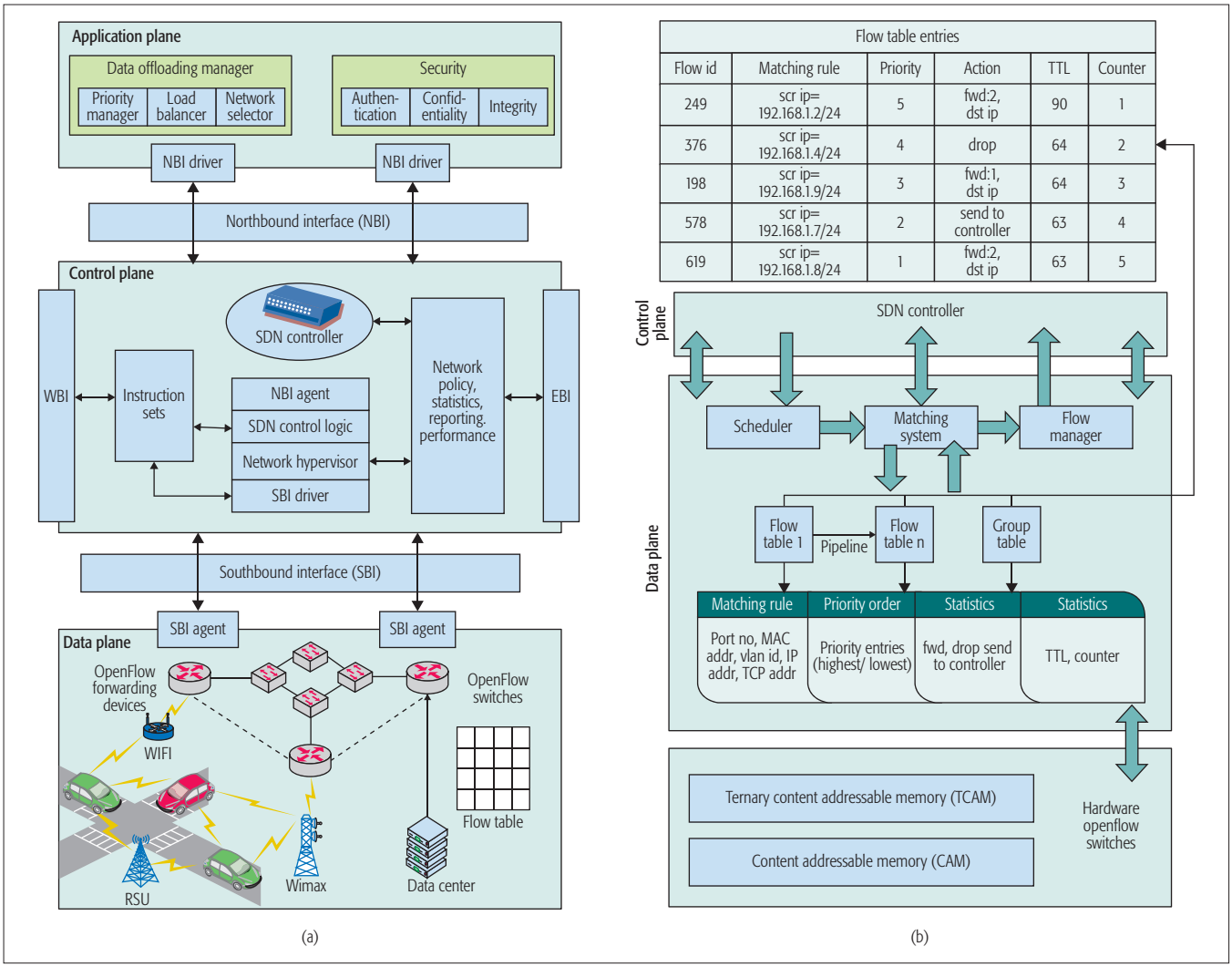


Figure 2. Proposed SDN-based controller: a) architecture of an SDN-based controller; b) flow table management.

Flow Table Management: In the present context, an approach based on efficient handling of flow table entries in OpenFlow switches using a software-defined flow table pipeline (SDFTP) algorithm is used [12]. Figure 2b elaborates the working of the flow table at the data plane. OpenFlow switches are hardware-based devices that consist of content addressable memories (CAMs) and ternary content addressable memories (TCAMs). These memory chips are used for storing thousands of flow table entries and fast forwarding of packets. The flow table entries consist of the following fields: flow id, matching rule, priority, action, TTL, and counter. The process of flow table management works in three steps: First, when an incoming packet arrives, a lookup process is initiated by the scheduler. Second, the packet matching system matches the packet header information with respective flow table and group table. If the flow table entries match, it will send the outgoing packet to the particular destination node. Third, if the flow entry does not match in the flow and group tables, the packet is sent to the controller by the table manager. The controller then modifies and resends the packet again to the OpenFlow switches.

In the proposed work, the software-to-hardware mapping logic (SHML) [12] is used for mapping, insertion, and deletion operations in the flow table.

Insertion Operation: The algorithm applies both the packet matching rule and action along with statistics. The SHML must follow these criteria:

- Mapping the pair of the software-defined flow table with the hardware flow table in which the entry is stored
- Relative entries of priority
- Sequence number of flow id
- Available flow space

Deletion Operation: In a deletion operation, as the controller software deletes an entry from the flow table, the hardware flow table id containing the entry can be retrieved from recorded SHML. Thus, after mapping the particular flow id information, the entry is deleted.

SDN Control Plane

The control plane is the network brain where the SDN controller is present. Hence, a centralized server with a network operating system (NOS) is installed. In NOS, the SDN controller resides. The main functionality of this plane is installing the control commands on the forwarding devices, managing and keeping the global information of

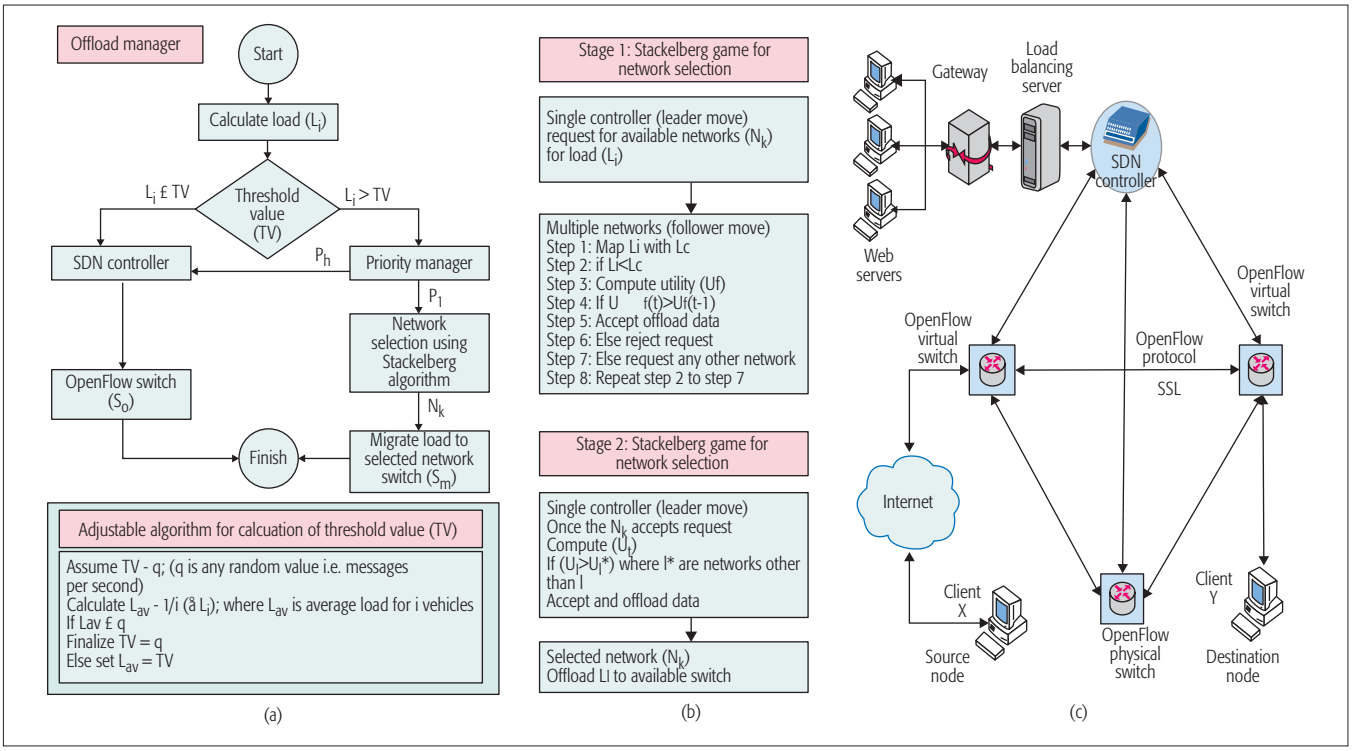


Figure 3. a) Offload manager and algorithm for calculation of TV; b) Stackelberg game for network selection; c) load balancer.

all SDN applications running at the application plane, and collecting the feedback of FDs. All the network policies are created at the control plane and implemented at both the data and management planes. Keeping all the global information from both the application and data planes, it makes decisions about forwarding the incoming packets.

SDN Management/Application Plane

With the help of network virtualization, the controller creates multiple virtual networks on a physical network. By virtualization, multiple virtual machines (VMs) run multiple SDN applications concurrently. Hence, in order to handle larger and smaller resources, network virtualization is an efficient solution. It helps in sharing resources and providing isolation among users, and aggregation for very small-sized resources [13]. SDN applications are the software programs that run in order to manage the resources and network efficiently. By the help of a northbound interface (NBI), the control logic created at the SDN controller deals directly with the internal decisions and keeps the abstract view of the network.

Network Resource Virtualization: By using network virtualization, it becomes easy to create logical virtual network resources that are decoupled from their physical resources at the data plane. Each virtual network interface card (NIC) connected to each other by a virtual switch can run multiple VMs simultaneously. Both the SDN and network virtualization layer work at the control plane, which helps to utilize network resources effectively in order to ensure better integration with the virtual resources.

SDN controllers provide each mobile user an illusion of its own address space, virtual topology, and database technology for storing and mappings between the physical and virtual networks. As the NFV deployment increases with the SDN, it improves network management and reduces network congestion to a great extent.

SDN Interfaces

The OpenFlow protocol allows communication between the two similar and/or dissimilar network devices with the help of interfaces and APIs. These interfaces are as follows:

- Southbound interface: The SBI is an interface between the control plane and the data plane. It offers an API to install the instruction sets at the data plane. At the control plane, the SDN controller decides the action to be taken by the routing protocols, which is then forwarded to the data plane through APIs.
- Northbound interface: The NBI is an interface for developing SDN applications at the management plane. An SDN application consists of one or more NBI drivers or agents to be installed at the network applications. NOSs offer APIs to application developers.
- Eastbound interface (EBI) and westbound interface (WBI): With the help of APIs, both the EBI and WBI will be linked with the other controllers in the network for fault tolerance.

Proposed Scheme for Data Offloading

As shown in Fig. 3, the proposed scheme is divided into four parts:

1. Offload manager
2. Priority manager
3. Network selector
4. Load balancer

The working of different parts of the proposed scheme is described as follows.

Offload Manager: The flow diagram of the proposed offload manager in shown in Fig. 3a. The offload manager works in coordination with the priority manager and network selector. The offload manager calculates the load (L_i) as

$$L_i = \frac{\theta_p(t) - \theta_p(t-1)}{\theta_{\max}} \quad (1)$$

where, $\theta_p(t)$ represents the messages that the pth controller receives at time t, $\theta_p(t-1)$ denotes the messages that the pth controller receives at time $t-1$, and $\theta_{\max}$ is the total number of messages that the pth controller can handle.

The calculated load is compared to the threshold value (TV). If ($L_i \leq TV$), the SDN controller decides the route using its flow tables on the parent network and sent to the OpenFlow switch (S_o). However, if ($L_i > TV$), the load is sent to the priority manager to prioritize the load. The load with higher priority is sent to the SDN controller for route selection using the parent network. In this case, the higher-priority load that could be sent on the parent network should be less than TV value. The lower-priority load is offloaded on another available network selected using the Stackelberg game. Once the optimal network is selected, the load is offloaded to it and migrated to the concerned switch (S_m). The load to be offloaded (L_{off}) must be less than or equal to the load difference of both the controllers and switches; ($L_{\text{off}} \leq (L_i - L_m)/2$), where, L_{off} is the load to be offloaded/migrated, and L_m is the load of the switch where the load is migrated.

The working of the offload manager depends on TV values. It is calculated using the adjustable threshold value calculation algorithm given in Fig. 3a. In this algorithm, a random number (q) is considered as an initial value of TV. Then average load (L_{av}) is calculated using the total load,

$$\left(\frac{\sum_0^i L_i}{i}\right)$$

for i vehicular users. If ($L_{\text{av}} \leq q$), q is finalized as TV; otherwise, average load (L_{av}) is set as TV.

Priority Manager: In this scheme, the load of data streams (L_i) for i vehicular users is divided into high priority (p_h) and low priority (p_l). The high priority load is sent to the SDN controller to follow the normal route using the parent cellular network. However, the low priority load is offloaded to a neighbor network, which is decided by the proposed Stackelberg game for network selection. The proposed work takes into account priority-based scheduling wherein high-priority data streams are scheduled prior to low-priority data streams. This is achieved using a strict priority queuing technique, which discourages the assignment of low-priority data streams before high-priority ones. The priority for respective data streams is decided on the basis of greedy strategies referred to as per-flow priority adjustment and per-router priority adjustment [14]. The former takes into account adjustment of priorities in which the data streams with best deadline guarantee are assigned lower priority, whereas the ones with worst deadline guarantee are given high priority. This is done to meet the deadline of the concerned data streams. On the other hand, the per-router priority adjustment strategy works on similar lines except that it takes into consideration the adjustment of priorities of all the switches and routers through which the data stream passes [14].

Single-Leader Multiple-Follower Stackelberg Game for Network Selection: The Stackelberg game for network selection is used to decide an optimal network on which the load selected by the priority manager is to be offloaded. In this scheme, the game is divided into two stages where the controller acts as a single leader, and various available networks act as multiple followers. The working of the proposed Stackelberg game for network selection is shown in Fig. 3b. The players (leader and followers) in the proposed game play their moves in a sequential manner. In the Stackelberg game, the leader initiates the play and the followers reply back accordingly [9]. In stage 1, the controller requests network (N_k) from the available k networks at a particular instance (t) and location (loc(x, y)). The multiple followers (i.e., available networks) map the required load (L_i) with the available load capacity (L_c). If the requested load capacity is less than the available load capacity of the network, it computes the corresponding utility (U_f). If the utility at the current instance of time shows improvement compared to previous instances, the deal is accepted. The concerned network reverts back with the consent to accept the load to be offloaded. If the requested load in more than the available capacity of the network channel, it rejects the request.

Once the controller receives the acceptance from available networks, it computes the utility for all the networks. The controller compares the utility of various networks and selects the network that shows the highest benefit. The controller offloads the load over the selected network. The selected network receives the offloaded load and routes it according to the path in the flow table. The utility function is defined for both leaders and followers for decision making. The utility functions for controller (U_l) and various networks (U_f) are given as:

$$U_l = \frac{\beta_i \times \eta_{av}}{\tau_{av}} - C_{off}$$

$$U_f = \frac{\beta_j \times \eta_j}{(j+1) \times \tau} \quad (2)$$

where β_j is total bandwidth allocated to j users, η_j is aggregate throughput in the network, ρ is the average delay of packets in the same network, β_i is the bandwidth that would be allocated to the requesting user, η_{av} is the average throughput of the network after including the new load, τ_{av} is the average anticipated delay of packets after including the new load, and C_{off} is the cost associated with the offload.

Load Balancer: The load balancer handles the load over the network by distributing the load optimally to all the available networks. The model of a load balancing network using an SDN controller is shown in Fig. 3c. Suppose client X wants to send data to client Y; the data flow is done by using the SDN controller and load balancer. First, the request is transmitted from the OpenFlow virtual switch directly to the controller. At the control plane, the controller will send the request to the application plane (i.e., load balancing applica-

With the help of network virtualization, the controller creates multiple virtual networks on a physical network. By virtualization, multiple virtual machines (VMs) run multiple SDN applications concurrently. So, in order to handle larger and smaller resources, network virtualization is a viable solution.

The offloading process involves migration from one network to another. For this purpose, the SDN controller has to switch the data from one openflow switch to another which involves some handover. The number of handover occurrences while using an SDN controller is far less than the use of the proposed scheme without an SDN controller.

Simulation parameters	Values
Area	6 × 4 km^2
No. of vehicles	50
Speed of vehicles	20–80 km/h
Data rate	1 Gb/s
System bandwidth	1 GHz
Traffic model	CBR 1 Gb/s full buffer traffic
Carrier frequency	15 MHz
Features	Text, voice, VOIP, ultra HD
Networks available	WiFi, WiMAX, femtocell, picocell

Table 2. Simulation parameters.

tion). At the application plane, the load balancer works, which manages the equal load on the list of web servers. Now, the reply is first sent to the controller; then it sends the reply to the OpenFlow switch through which the data is transmitted to the client Y. The load balancing server controls the working of the offload manger using a load balancing rate (ψ) as given below [15]:

$$\psi = \frac{1/j \times \sum_0^i L_i}{L_{\max}} \quad (3)$$

where $L_{\max}$ is the maximum load a controller/switch can handle.

The load balancing rate lies between 0 and 1. If the value of ψ is close to 1, it means the load is evenly distributed. However, if the value of ψ is low, it means the load is not evenly distributed and the controller needs to migrate the load using the offload manager.

Evaluation

In this article, the performance of the proposed data offloading scheme is evaluated using extensive simulations performed on an area taken from the city of Patiala to generate traffic movements. The simulation parameters are shown in Table 2.

The data generated by each vehicle that is to be transmitted over the cellular channel is shown in Fig. 4a. In order to decide the data to be offloaded, a random number 40 is assumed as the initial value of TV. However, the value of average load (L_{av}) is 42.16, which is more than the assumed TV. Hence, using the adjustable TV calculation algorithm, the TV is set as 42.16 for the offloading process. The data required to be offloaded with respect to TV selected is shown in Fig. 4b. Now, the TV is varied to evaluate its effect on the offloading process. The variation of offloaded data with respect to TV is shown in Fig. 4b. The data offloaded (TV = 42.16) is more than the data offloaded when TV is set as 40 and 45. There is a strong impact on the amount of data to be offloaded with respect to TV value. Hence, the purpose of having a TV in the proposed data offloading scheme is justified for optimal selection of the amount of data to be offloading. The data transmitted with respect to the data offloaded for each vehicle is shown in Fig. 4c. The offloading process involves migration from one network to another. For this purpose, the SDN controller has to switch the data from one OpenFlow switch to another, which involves some handover. The number of handover occurrences while using an SDN controller is far less than the use of the proposed scheme without an SDN controller and is shown in Fig. 4d. Hence, due to such handover some amount of network delay may occur. The network delay with respect to network utilization is shown in Fig. 4e. The results show that the average network delay is lower with the use of SDN controller. Finally, the performance of the SDN-based data offloading scheme is evaluated with respect to the throughput. The results show that the SDN-based scheme achieves higher throughput to prove the effectiveness of the proposed scheme as shown in Fig. 4f.

Conclusion

Focusing on the issues such as service availability and latency for most modern applications, the evolution of 5G technology is occurring. However, within the present set of constraints like high mobility and congestion in the network, it is becoming a challenging task to offload the data to either centralized servers or other devices in the network. In such scenarios, an intelligent controller needs to be designed that can make decisions within the constraints of latency and congestion in the network. Hence, in this article, we propose a new data offloading scheme for 5G-enabled SDN-based vehicular networks. To make intelligent decisions with respect to data offloading, priority and offload managers are designed. For network selection used for data offloading, a single-leader multi-follower Stackelberg game is designed. The performance of the proposed scheme is evaluated by selecting different network parameters.

In the future, we will evaluate the effect of number of channels and interference, along with security issues for vehicular data offloading.

Acknowledgments

This work was partially supported by Finep, with resources from Funttel under Grant 01.14.0231.00, under the Centro de Referência em Radiocomunicações project of the Instituto Nacional de Telecomunicaçãoes (Inatel), Brazil, by the Government of Russian Federation under Grant 074-U01, and by FCT - Fundação para a Ciéncia e a Tecnologia funding Project UID/EEA/500008/2013.

References

[1] A. Dua, N. Kumar, and S. Bawa, "A Systematic Review on Routing Protocols for Vehicular Ad Hoc Networks," *Vehic. Commun.*, vol. 1, no. 1, Jan. 2014, pp. 33–52.
[2] M. K. Arjmandi, "5G Overview: Key Technologies," *Opportunities in 5G Networks: A Research and Development Perspective*, CRC Press, 2016, pp. 19–31.
[3] X. Ge *et al.*, "5G Ultra-Dense Cellular Networks," *IEEE Wireless Commun.*, vol. 23, no. 1, Feb. 2016, pp. 72–79.
[4] A. Aijaz, H. Aghvami, and M. Amani, "A Survey on Mobile Data Offloading: Technical and Business Perspectives," *IEEE Wireless Commun.*, vol. 20, no. 2, Apr. 2013, pp. 104–12.
[5] J. Kim, Y. Morioka and J. Hagiwara, "An Optimized Seamless IP Flow Mobility Management Architecture for Traffic Offloading," *2012 IEEE Network Operations and Management Symp.*, Maui, HI, 2012, pp. 229–36.
[6] E. G. Larsson *et al.*, "Massive MIMO for Next Generation Wireless Systems," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. 186–95.

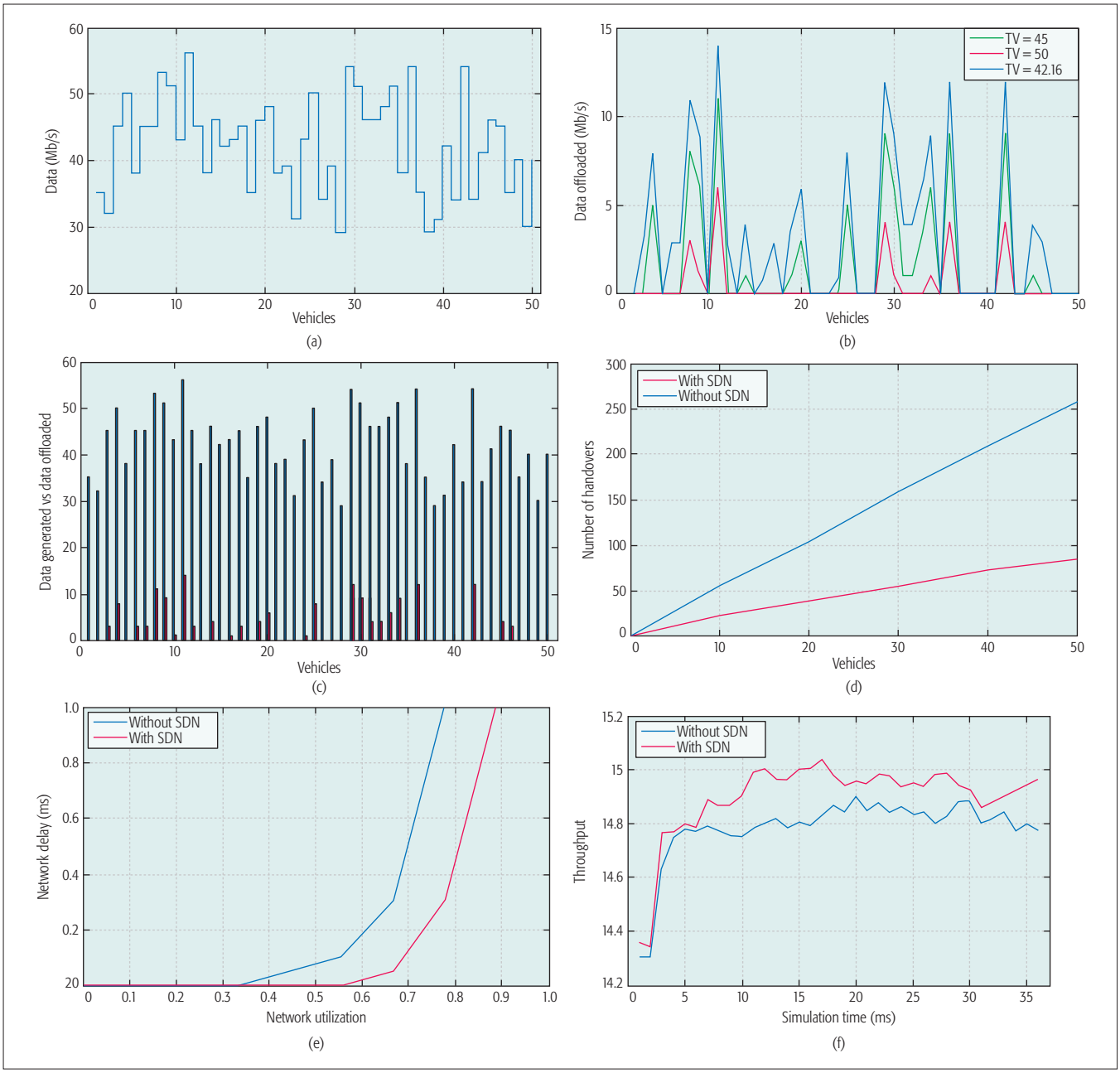


Figure 4. Evaluation results: a) data generated by each vehicle; b) data offloaded; c) data transmitted vs. data offloaded; d) number of handovers due to data offloading; e) average network delay vs. network utilization; f) throughput.

[7] U. Siddique *et al.*, "Wireless Backhauling of 5G Small Cells: Challenges and Solution Approaches," *IEEE Wireless Commun.*, vol. 22, no. 5, Oct. 2015, pp. 22–31.

[8] Y. Li *et al.*, "Multiple Mobile Data Offloading through Delay Tolerant Networks," *6th ACM Wksp. Challenged Networks*, New York, NY, 2011, pp. 43–48.

[9] H. Zhang *et al.*, "Multi-leader Multi-Follower Stackelberg Game among Wi-Fi, Small Cell and Macrocell Networks," *IEEE GLOBECOM*, Austin, TX, 2014, pp. 4520–24.

[10] Y. Liu *et al.*, "Game-Theoretic Hierarchical Resource Allocation in Ultra-Dense Networks," *IEEE 27th Annual Int'l. Symp. Personal, Indoor, and Mobile Radio Commun.*, Valencia, Spain, 2016, pp. 1–6.

[11] H. Li, M. Dong and K. Ota, "Control Plane Optimization in Software-Defined Vehicular Ad Hoc Networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 10, Oct. 2016, pp. 7895–7904.

[12] X. Sun, T. S. E. Ng and G. Wang, "Software-Defined Flow Table Pipeline," *IEEE Int'l. Conf. Cloud Engineering*, Tempe, AZ, 2015, pp. 335–40.

[13] R. Jain and S. Paul, "Network Virtualization and Software Defined Networking for Cloud Computing: A Survey," *IEEE Commun. Mag.*, vol. 51, no. 11, Nov. 2013, pp. 24–31.

[14] N. An *et al.*, "Dynamic Priority-Adjustment for Real-Time Flows in Software-Defined Networks," *2016 17th Int'l. Telecommun. Network Strategy and Planning Symp. (Networks)*, Montreal, Quebec, Canada, 2016, pp. 144–49.

[15] Y. Zhou *et al.*, "A Load Balancing Strategy of SDN Controller Based on Distributed Decision," *2014 IEEE 13th Int'l. Conf. Trust, Security and Privacy in Computing and Communications*, Beijing, 2014, pp. 851–56.

Biographies

Gagangeet Singh Aujla [S'16] (gagi_aujla82@yahoo.com) is pursuing a Ph.D. at Thapar University, Patiala, Punjab, India. He received his B.Tech degree in computer science and engineering from Punjab Technical University, Jalandhar, Punjab, India, in 2003, and his M.Tech degree from Punjab Technical University in 2012. He has many research contributions in the areas of smart grid, cloud computing, vehicular ad hoc networks, and software-defined networks.

Rajat Chaudhary [S'17] (rajatlibran@gmail.com) is pursuing a Ph.D.at Thapar University. He received his B.Tech degree in computer science and engineering from UPTU, Lucknow, India,

in 2010, and his M.Tech degree from UTU, Dehradun, India, in 2012. He has many research interests in the areas of networking and software-defined networks.

Neeraj Kumar [M'16] (neeraj.kumar@thapar.edu) is working as an associate professor in the Department of Computer Science and Engineering, Thapar Univesity. He received his M.Tech. from Kurukshetra University, India, followed by his Ph.D. from SMVD University, Katra, in CSE. He was a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 150 research papers in leading journals and conferences of repute. His research is supported by UGC, DST, CSIR, and TCS. He is an Associate Editor of *IJCS*, Wiley, and *JNCA*, Elsevier.

Joel J. P. C. Rodrigues [S'01, M'06, SM'06] (joeljr@ieee.org) is a professor and senior researcher at the National Institute of Telecommunications (Inatel), Brazil, and a senior researcher at the Institute of Telecommunication, Portugal. He is the leader of the NetGNA Research Group (http://netgna.it.ubi.pt), Past Chair of the IEEE ComSoc Technical Committees on eHealth and Communications Software, and a Steering Committee member of the IEEE Life Sciences Technical Community. He is the Editor-in-Chief of three international journals, and a co-author of over 500 papers, three books, and two patents. He is the recipient of several Outstanding Leadership and Outstanding Service Awards from IEEE Communications Society and several best paper awards.

Alexey Vinel [M'07, SM'12] (alexey.vinel@gmail.com) received his Bachelor's (Hons.) and Masters' (Hons.) degrees in information systems from Saint-Petersburg State University of Aerospace Instrumentation, Russia, in 2003 and 2005, respectively, and his Ph.D. degrees in technology from the Institute for Information Transmission Problems, Moscow, Russia, in 2007, and Tampere University of Technology, Finland, in 2013. He is currently a professor of data communications at the School of Information Technology, Halmstad University, Sweden. He has been involved in research projects on vehicular networking standards, advanced driver assistance systems, and autonomous driving. He has been an associate editor for *IEEE Communications Letters* since 2012.

Increase Your Knowledge of Technical Standards

The foundation for today's global high-tech success

Prepare yourself to enter the high-tech industry by learning how technical standards develop, grow, and relate to technologies worldwide.

IEEE Standards Education is dedicated to helping engineers and students increase their knowledge of technical standards, applications, and the impact standards have on new product designs.

Begin your journey into the high-tech world: http://trystandards.org

Stay current with access to regularly updated educational programs

Discover learning opportunities through tutorials and case studies

Understand the role of technical standards in the world

For information about IEEE Standards Education, visit http://standardseducation.org

IEEE
Advancing Technology for Humanity

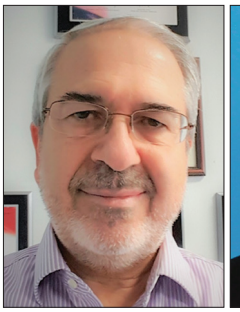
5G NETWORK SLICING – PART 2: ALGORITHMS AND PRACTICE


Konstantinos Samdanis


Steven Wright


Albert Banchs


Antonio Capone


Mehmet Ulema


Kazuaki Obana

The emerging fifth generation (5G) networks are expected to support a plethora of different services and applications with diverse and often conflicting performance requirements. Network slicing enables network operators to allocate logical self-contained networks toward service providers, virtual operators, and vertical segments, with specific service-oriented functionality over a common physical network infrastructure providing the means of supporting efficiently diverse services.

By means of software defined networks (SDNs) and network functions virtualization (NFV), operators can deliver automation, flexibility, and programmability, allowing legacy functions to be partitioned or migrated in data center environments, advancing virtual network architectures. However, certain network slicing attributes, including function customization, performance and security requirements, management operations, and control, can be supported in a number of different ways by combining different types of cloud and network resources that influence in a distinct way the associated capital and operational expenses.

To ensure that network slicing can deliver the desired benefits, operators need to rely on service and network intelligence, user context awareness, and machine learning, which can empower slicing algorithms to perform admission control, slice selection, policing, and closed-loop performance maintenance. Common resource abstraction, service representations, and flexible service chaining are also key technology attributes related to such slicing algorithms, facilitating service exposure and programmability as well as a joint optimization of virtual network functions and service allocation. In mobile environments service continuity is also significant, and hence network slicing algorithms and operations should consider not only user mobility but also service mobility and even new mobility mechanisms related to particular types of slices.

Network slicing also has practical attributes and limitations with respect to slice instantiation, resource virtualization, and certain slice operations. For ensuring scalability and rapid slice instantiation, the use of slice templates is a valuable asset, which needs to be designed carefully in advance considering performance requirements and the desired service flexibility. Although network slices are self-contained networks, certain types of resources cannot be isolated but must be shared, for instance, spectrum , due to its highly dynamic nature. Network slicing algorithms should take such practicalities into account, introducing tactics and mechanisms to deal with resource sharing, particularly for highly dynamic resources.

This Feature Topic includes five outstanding articles that focus on the 5G network slicing algorithms and practice considering the resource allocation mechanisms, service provision, and performance assurance in different segments of the network, such as the radio, transport, and core. These articles provide an insight on the service orchestration and slice operational aspects, pointing out key enabling technologies for ensuring the desired customization and performance.

The first article, "The Algorithmic Aspects of Network Slicing," by S. Vassilaras, L. Gkatzikis, N. Liakopoulos, I. N. Stiakogiannakis, M. Qi, L. Shi, L. Liu, M. Debbah, and G.S. Paschos, focuses on resource allocation and control algorithms related to real-time management of network slicing considering orchestration as an instance of virtual network embedding, while taking into account the dynamic nature of contemporary networks.

In the second article, "A Cloud Native Approach to 5G Network Slicing," S. Sharma, R. Miller, and A. Francini elaborate a service-oriented concept of 5G slicing analyzing the paradigm shift from a network of entities to a network of capabilities with respect to the entire life cycle of network slicing considering the design, instantiation, and orchestration. The article also presents a proof-of-concept implementation demonstrating service customization.

The following article in this series, "5G-Crosshaul Network Slicing: Enabling Multi-Tenancy in Mobile Transport Networks," by X. Li, R. Casellas, G. Landi, A. de la Oliva, X. Costa-Perez, A. Garcia-Saavedra, T. Deiß, L. Cominardi, and R. Vilalta, brings light to the next generation of transport networks integrating backhaul and fronthaul segments considering the coexistence of distributed and cloud RAN architectures. The article elaborates the design of a control plane for enabling multi-tenancy that allows flexible and efficient allocation of transport and cloud resources.

The next article, "Network Slicing Based 5G Networks: Mobility, Resource Management and Challenges," by H. Zhang, N. Liu, X. Chu, K. Long, A.H. Aghvami, and V. C. M. Leung, analyzes mechanisms for efficient resource management considering joint power and sub-channel allocation in spectrum sharing taking into account co-tier and cross-tier interference, while proposing a new mobility scheme to enhance 5G network flexibility based on network slicing.

The last article, "Network Slices toward 5G Communications: Slicing and LTE Networks," by K. Katsalis, N. Nikaein, E. Schiller, A. Ksentini, and T. Braun, elaborates the notion of service-oriented network slicing concentrating on an eMBB deployment prototype. The article emphasizes service control and programmability based on the Open Air Interface and the Juju framework.

We hope that these five articles provide an overview to the readers with a representative taste of 5G network slicing algorithms and practice.

BIOGRAPHIES

KONSTANTINOS SAMDANIS (konstantinos.samdanis@huawei.com) is a principal researcher at Huawei for 5G carrier networks. He is involved in research for 5G SDN/NFV architectures and network slice OS, also being active at BBF in wireless-wired converged networks and the 5GPPP Architecture WG. Previously he worked for NEC Europe, Germany, as a senior researcher and a broadband standardization specialist involved in numerous EU projects and 3GPP. He received his Ph.D. and M.Sc. degrees from Kings College London.

STEVEN A. WRIGHT (s.wright@ieee.org), M.B.A., Ph.D., J.D., has been involved in the communications industry in research, development, program management, product management, university faculty, and board roles, resulting in 50+ patents and a number of diverse publications. He has presented his research at international conferences in Europe, Asia, Australia, and the United States, and founded the IEEE NFV SDN conference.

ALBERT BANCHS (banchs@it.uc3m.es) is a professor with the University Carlos III of Madrid (UC3M) and has a double affiliation as deputy director of the IMDEA Networks institute. Before joining UC3M, he was at ICSI Berkeley, Telefonica I+D, and NEC Europe Ltd., respectively. He has authored more than 100 peer-reviewed publications, as well as several patents and standardization proposals. A current major focus is on the 5G architecture work within the 5G NORMA European project.

ANTONIO CAPONE [SM] (antonio.capone@polimi.it) is a professor at Politecnico di Milano, where he is the director of the ANTLab and vice-dean of the School of Engineering. He serves on the TPCs of major conferences in networking, is an Editor of *IEEE Transactions on Mobile Computing*, *Computer Networks*, and *Computer Communications*, and was an Editor of *ACM/IEEE Transactions on Networking* from 2010 to 2014.

MEHMET ULEMA (mehmet.ulema@manhattan.edu) is a professor at Manhattan College, New York. Previously, he was with AT&T Bell Laboratories and Bellcore. He also serves as Director of Standards Development in ComSoc. He has had leadership roles for many major IEEE conferences. He is on the Editorial Boards of the *IEEE Journal of IoT* and the *Journal of Network and Services Management*. He received his Ph.D. from Polytechnic University, Brooklyn, New York, and his B.S. and M.S. from Istanbul Technical University.

KAZUAKI OBANA (kazuaki.obana.uz@nttdocomo.com) is an executive research engineer and leads the ICT Network Cloud Research Group in Research Laboratories, NTT DOCOMO. He is involved in research on future mobile core networks for the 5G era, standardization in ETSI ISG NFV, and open source activity in OPNFV. He holds B.E. and M.E. degrees in electrical engineering from Waseda University, Tokyo, Japan.

The Algorithmic Aspects of Network Slicing

Spyridon Vassilaras, Lazaros Gkatzikis, Nikolaos Liakopoulos, Ioannis N. Stiakogiannakis, Meiyu Qi, Lei Shi, Liu Liu, Mérouane Debbah, and Georgios S. Paschos

The authors focus on the algorithmic challenges that emerge in efficient network slicing, necessitating novel techniques from the communities of operation research, networking, and computer science.

ABSTRACT

Network slicing is a technique for flexible resource provisioning in future wireless networks. With the powerful SDN and NFV technologies available, network slices can be quickly deployed and centrally managed, leading to simplified management, better resource utilization, and cost efficiency by commoditization of resources. Departing from the one-type-fits-all design philosophy, future wireless networks will employ the network slicing methodology in order to accommodate applications with widely diverse requirements over the same physical network. On the other hand, deciding how to efficiently allocate, manage, and control the slice resources in real time is very challenging. This article focuses on the algorithmic challenges that emerge in efficient network slicing, necessitating novel techniques from the communities of operation research, networking, and computer science.

INTRODUCTION

Traditionally, cellular networks have been architected to support specific services: voice, messaging, and Internet access. However, wireless operators are now faced with the major challenge of supporting a number of diverse vertical industry applications in order to expand the wireless market. Thus, next-generation networks should simultaneously accommodate applications and services with requirements as diverse as ultra-low latency and high resilience for real-time control of critical systems and scalability to hundreds of thousands of connected devices toward the Internet of Things (IoT). Table 1 provides a summary of typical examples of such services, which illustrate the wide diversity of their associated requirements. *Network slicing* (NS) is a key enabling technology for this paradigm shift.

THE NETWORK SLICING CONCEPT

The concept of NS is not a new one; it has been proposed in the context of distributed service architectures, such as content delivery networks, large-scale distributed testbed platforms, and distributed cloud computing systems [1]. However, its introduction to *wireless* networks is quite recent. A *network slice* is a virtual network that is implemented on top of a physical network in a way that creates the illusion to the slice tenant of operating its own dedicated physical network. A virtual link between virtual nodes A and B with capacity β_{AB} can be realized as a multihop physical path with reserved bandwidth β_{AB} on all physical links constituting the path. A virtual node implements a specific network functionality as a physical node (e.g., a router or a firewall) would do in a traditional network. Virtual links can be easily established with software defined networking (SDN) routers. SDN allows the administrator to remotely configure the physical network in order to reserve on demand networking resources for the slice. Virtual nodes can be implemented as virtual network functions (VNFs) running on general-purpose hardware forming a cloud infrastructure. Network slicing requires a high degree of flexibility, which was only made possible by the recent advent of network functions virtualization (NFV) and SDN. On a physical network consisting of SDN routers and data centers with NFV functionality, it is possible to rapidly instantiate and reconfigure slices with diverse and time-varying requirements.

Network slicing offers a number of significant advantages that are particularly useful in the design of next generation wireless networks, namely the following.

Slice Isolation: The complete isolation of slices allows for simpler and more efficient design of each slice with the goal of meeting the requirements of the particular vertical applications and services offered by the slice tenant. In addition, network failure, overload, or security attacks in one slice will not affect the operation of other slices in the network.

Simplified Service Chains: In contrast to traditional cellular communications in which all services consist of the same functions, in NS each service may rely on a different subset of functions.

Flexible VNF Placement: NFV introduces an additional degree of freedom regarding the placement of these functions on the network. Intelligent placement may improve network performance and reduce operating costs.

Transparent Slice Management: Subsets of the physical network resources might belong to different network domains (or even operators). Network slicing provides an abstraction of the physical resources and makes slice management transparent to the slice tenant.

To illustrate the flexibility offered by NS, we consider three indicative applications in Fig. 1. The figure shows the basic VNFs required for each application as well as the corresponding

Digital Object Identifier:
10.1109/MCOM.2017.1600939

Spyridon Vassilaras, Lazaros Gkatzikis, Nikolaos Liakopoulos, Ioannis N. Stiakogiannakis, Meiyu Qi, Mérouane Debbah, and Georgios S. Paschos are with Huawei Technologies France SASU.; Lei Shi and Liu Liu are with Huawei Network Research.

Case	Application	Requirements
Broadband access in dense areas	Open-air event, stadium	High traffic volume, throughput (up to 10 Gb/s), ms latency
Broadband access everywhere	Minimum coverage everywhere	Guaranteed 50+ Mb/s
High user mobility	Trains, vehicles, aircrafts, and drones	Connectivity in 3D and at over 500 km/h
Massive Internet of Things	Sensors, smart wearables, and meters	Diverse RATs, low power, 1 million connections per km^2
Extreme real-time communications	Robotic control and autonomous cars	Sub-ms latency, reliability, mobility
Ultra-reliable communications	Smart grid, eHealth, and public safety	Redundancy, ms latency

Table 1. Use cases [2].

network domains where these VNFs can be placed. For example, traditional voice and broadband services require complicated control plane functionalities such as authentication and mobility management, placed at the core cloud. IoT services could be implemented with a simplified control plane; for example, a smart meter service that monitors the energy consumption of houses does not require mobility management functionality. Video delivery services can be optimized if user plane and caching functionality is available at the edge cloud, which reduces backhaul traffic and improves user experience. Network slicing enables service-specific resource allocation, which leads to a simplified, smaller, and cost-efficient network.

For all these reasons, NS has been recognized as a key element in the design of future wireless networks by the Next Generation Mobile Network (NGMN) Alliance [2], the Open Networking Foundation (ONF), as well as many telecom vendors and wireless operators.

A Wireless Network Slicing Architecture

Network slicing has already been considered in late 4G and early 5G specifications. However, this ongoing process has not yet produced a standardized architecture for NS. In order to discuss the involved algorithmic problems, we focus on a generic architecture, explained below. Eventually, some of its aspects might differ from future 5G NS standards, but we believe that the basic algorithmic components will remain the same.

The architecture we are considering is depicted in Fig. 2, showing the interactions of one (or more) physical *network operator(s)* with multiple *enterprises* (e.g., over-the-top [OTT] services, virtual network operators). The role of the network operator is to provide the resources and to ensure the harmonic coexistence of different slices, while the role of enterprises is to place slice requests and then manage the provided slice. More specifically, in the life cycle of slices, the following important operations take place:

- Planning of slice requirements (by enterprise)
- Creation of slice (by network operator)
- Intra-slice network management (by enterprise)
- Orchestration of different slices (by network operator)

We detail them below.

For a new slice to be instantiated, an enterprise must first determine the required slice functionality and resources. It is envisioned that slice

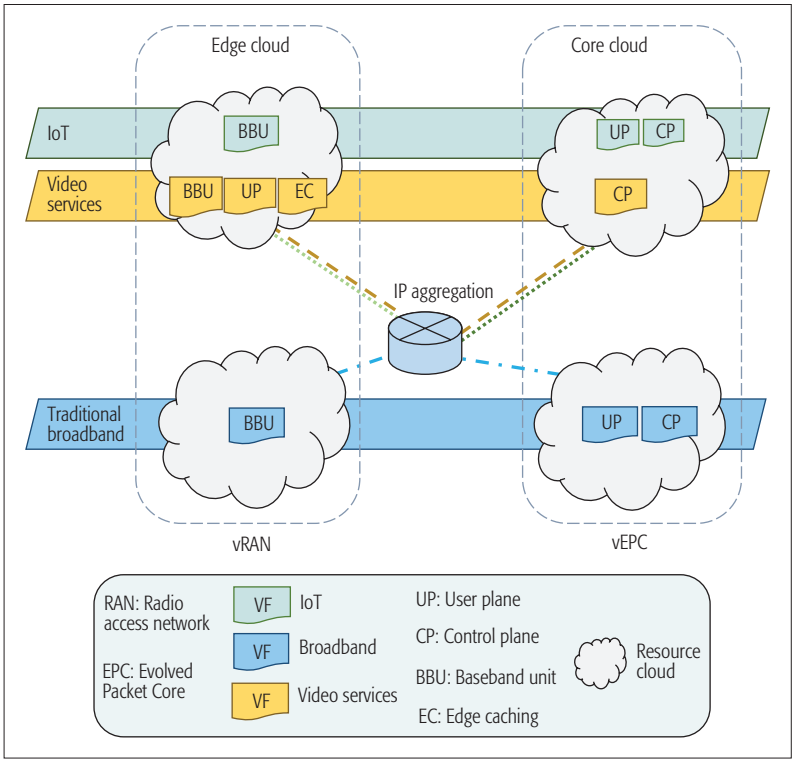


Figure 1. Network slices supporting indicative applications with diverse requirements. Each slice consists of different VNFs, which can be placed on different physical network domains.

templates will be available for the most common types of services [3]. Thus, an enterprise may select the slice template that fits its purpose and parameterize it according to its needs. However, in order to be able to support novel services, a more flexible approach is also needed. In the extreme scenario, an enterprise could reserve processing, storage, and bandwidth resources at will, similar to the way that resources are reserved in the cloud, and deploy on top only the necessary VNFs. In this case, the enterprise can determine the network topology (topological design) and the size of each component (dimensioning) via classical network planning tools such as Netsim. The enterprises notify their slice requests via a specific interface (e.g., an intent-based language such as NEMO).

Upon receiving a slice request, the network operator faces the problem of embedding a concrete virtual network onto the physical network in an efficient way. This step involves decisions on

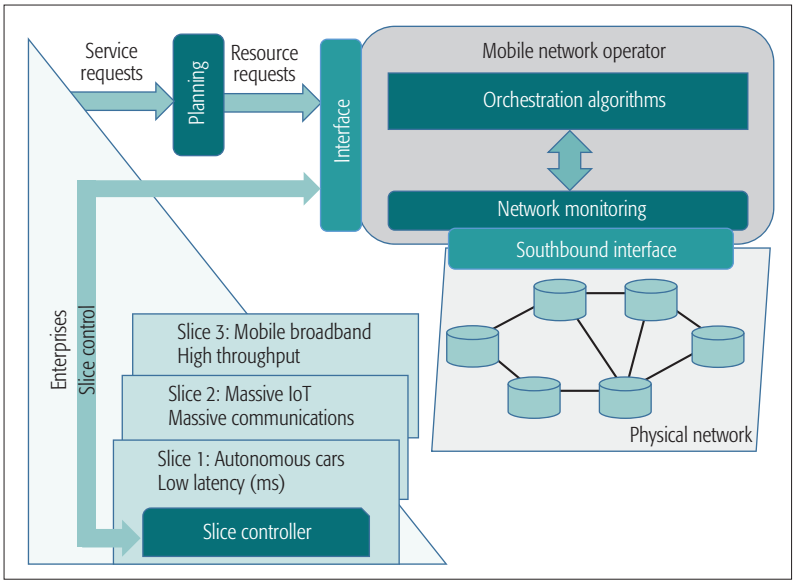


Figure 2. A high level architecture for wireless network slicing.

placing and interconnecting several VNFs, which can be formally expressed as a constrained optimization problem. The algorithmic considerations of this step are described in the second section of this article. Based on the solution to this problem, the network operator creates the slice using SDN and NFV technology.

Once the slice has been created, the tenant (enterprise) can normally manage the provisioned slice resources in the same way it would manage a dedicated physical network. For this purpose, the network operator needs to expose a number of control functions to the enterprise controlling the slice.

In addition, from time to time, the enterprise may request to scale up or down the reserved resources (e.g., to address a traffic burst). The details of the complex interactions between the network operator and the enterprise during the lifetime of a slice are subjects of ongoing development and standardization work [4] and are outside the scope of this article. However, the presented abstraction level is sufficient for our discussion of dynamic NS algorithmic aspects in the third section.

Aim and Objectives

The NS paradigm makes network management flexible and opens new horizons for network efficiency. At the same time, it raises a number of challenging issues that are receiving increasing attention from the research community. The goal of this article is to provide directions on the most suitable algorithmic tools to address a multitude of NS problems.

To this end, in the second section, we investigate the efficient NS problem and demonstrate that, for a given set of slices, orchestration at the operator level can be seen as a special instance of the virtual network embedding (VNE) problem. We delineate several NS problem variants and extensions, and identify open research topics. In the third section, we analyze the envisioned mechanisms to deal with network requirements that vary over time and outline how existing network engineering techniques can be applied in the NS context. We then conclude the article in the fourth section.

Optimal Network Slicing

The NS problem is a combined optimization problem of placing network functions over a set of candidate locations and deciding their interconnections. The mathematical problem can be formulated using the well studied virtual network embedding (VNE) problem — see [5] for a comprehensive survey.

Virtual Network Embedding

We are given a physical network G and a virtual network H, and we are asked to "embed" or "map" the virtual onto the physical network.

The physical network $G = (V, E, \boldsymbol{\beta}, \mathbf{c})$ has nodes $v \in V$ and links $e \in E$ characterized by capacities $\beta_v \geq 0$ and $\beta_e \geq 0$, respectively. In the online operation of the network, β can play the role of *residual capacity*, that is, the remaining resource of the node or link after we take out the current utilization. Each node v and link e is also associated with a cost, c_v and c_e, respectively. Depending on the application, costs may reflect congestion, preference in terms of operator agreements, load balancing, or real cost of operation.

The virtual network $H = (N, L, \mathbf{d}, M)$ with virtual nodes N and virtual links L has capacity requirements d_n and d_l for each virtual node $n \in N$ and link $l \in L$, respectively. The usage cost is a linear function of the used capacity, that is, the cost of a virtual node n with capacity demand d_n using a physical node v with cost c_v is $c_v\, d_n$. Each virtual node n can be embedded in exactly one physical node from a set of physical nodes M_n, which is a subset of the set of all physical nodes V.

An embedding of H onto G consists of mapping:

- Each virtual node $n \in N$ onto a physical node $v \in M_n$
- Each virtual link (m, n) onto a loop-free physical path, connecting the two physical nodes u and v to which the virtual nodes m and n have been mapped

A *feasible embedding* is an embedding in which all link and node capacity constraints are satisfied; that is, the sum of capacity demands of all virtual nodes embedded on a physical node is less than the capacity of this physical node, and the sum of demands of all virtual links going through a physical link is less than the capacity of this link. The VNE problem is defined as finding the feasible embedding with the least cost.

The basic VNE problem is an integer linear program (ILP), which is NP-hard as it can be proven by reduction to the *multi-way separator* problem. Even with a given virtual to physical node mapping, the problem of optimally allocating a set of virtual links to single physical paths reduces to the *unsplittable multicommodity flow* problem and therefore is also NP-hard. Nevertheless, multiple heuristic approaches are available [5]. For example, one may decompose the original joint NS problem into a node embedding and an integral min cost multicommodity-flow problem (link embedding). In [6], the former is addressed via a heuristic based on availability of resources, and the latter via solving a continuous relaxation of the ILP followed by rounding.

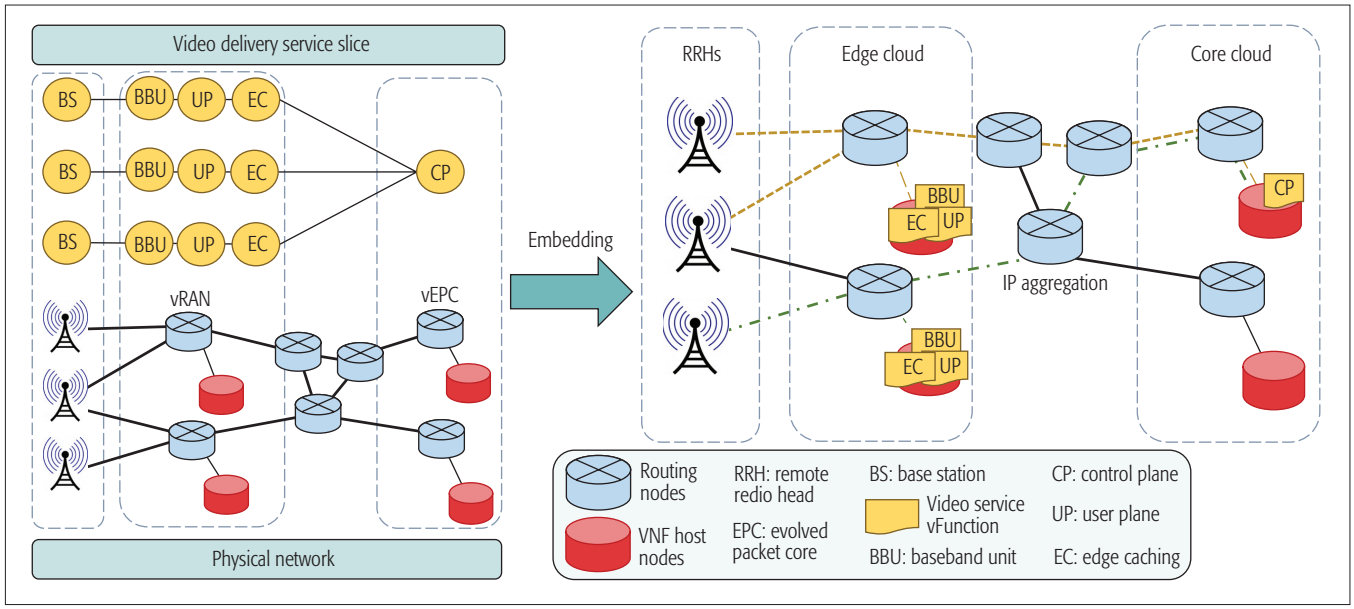


Figure 3. An example of embedding a video delivery slice on a simplified wireless network. Here, CP and UP refer to one or more VNFs at the corresponding plane.

Network Slicing

To decide how to create a slice, we may equivalently study the embedding of an appropriate virtual network, reflecting the required slice components. We define slice $H' = (N, L, \mathbf{d}, M)$, where L, $\mathbf{d}$ are links with capacity requirements as before, while the virtual nodes N represent VNFs. As a result, the connectivity of H' also describes how the different VNFs are connected. In this case, the location constraint sets M_n can be used to capture both the capabilities of physical nodes to run a specific VNF and the location requirements of the applications and users of the network. The *Network Slicing* problem is to find the feasible slice embedding with the least cost. By appropriately selecting the embedding sets M_n and virtual links, costs, capacities, and demands, any NS problem can be represented as an extended VNE problem.

In Fig. 3 we illustrate some key aspects of the NS problem. We focus on the implementation of a video delivery slice over a mobile wireless network. A graph representation of the virtual network, the substrate physical network, and the resulting embedding of the VNFs are depicted.

The specific slice consists of four types of VNFs (baseband unit, edge caching, user plane, and control plane) and the corresponding communication links.[1] Supporting such a video delivery service requires the implementation of one service chain per base station (BS) that terminates at the core network. Multiple VNFs may run on the same or different physical nodes, as long as connectivity is ensured and capacity constraints are satisfied. Notice that out of the several possible interconnection paths, the optimal one has to be selected.

The embedding of the three BSs is trivial, since each one has to be associated with a specific remote radio head. BBU, UP, and EC VNFs can be embedded on any of the physical resource nodes in the vRAN area, while the CP VNFs can only be embedded on the vEPC resource nodes. This basic example illustrates that the optimal VNF placement and interconnection depends on all problem parameters including physical node and link costs, capacities, and communication requirements.

Basic NS as an Optimization Problem

From the above discussion, it is evident that the basic NS problem is a constrained *optimization* problem. In its simplest form this is a VNE-type of problem, in which we have to jointly decide:

- The optimal placement of VNFs at resource nodes
- The necessary link capacity reservations for their interconnection, under additive link and node capacity constraints so that the overall resource utilization cost is minimized

Such problems, though NP-hard, can be cast as ILPs. Thus, they can be solved using standard ILP solvers like CPLEX™ or Gurobi™.

Next, we quantify the potential cost benefits of optimized NS with a simple numerical example. Consider the physical network of Fig. 4. The physical link and node capacities/costs are shown in parentheses, while the slice resource requirements are also given per service category. For example, the video service (type II) has small bandwidth requirement between user plane and control plane functionality, due to edge caching, which ensures that video service is obtained directly at the edge for popular videos. Similarly, IoT slices may rely on a simplified control plane and hence require a smaller bandwidth. Different network functions can be embedded on either a virtual radio access network (vRAN) or virtual Evolved Packet Core (vEPC) (the embedding options are also given in the figure), or on both in the special case of UP for video services. To quantify the benefit of NS, we embed these slices onto the physical network by solving the NS optimization problem.

In Fig. 4 we depict the obtained network cost of utilized resources according to the optimal slicing.[2] The baseline assumes that all three services are treated according to the traditional mobile broadband approach, as type I. To perform the

[1] For simplicity we group together as a single VNF and denote by UP and CP a number of required VNFs in the user and control plane, respectively, which are not already shown as standalone VNFs.

[2] By setting all costs equal to 1, one may optimize resource utilization.

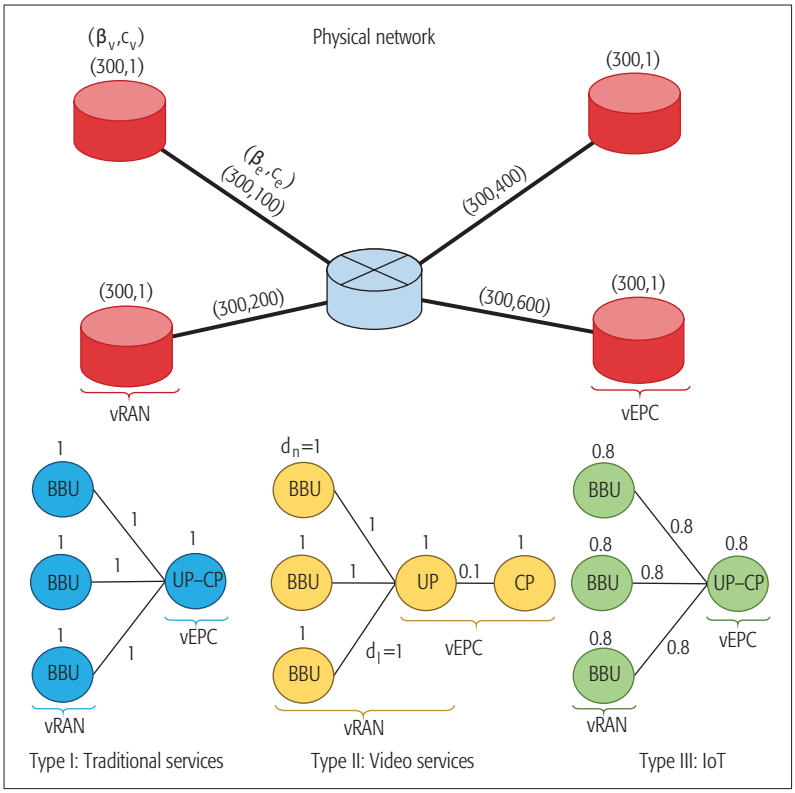


Figure 4. The three types of services and the physical network used in the simulation.

comparison, we create two possible mixes of traffic representing future projections, a) one representing medium market penetration in which slices of types I, II, and III are requested in proportion 2:1:1, and b) one where slicing has become the de facto standard and the requests are in proportion 1:2:2. Then we scale up the slice resource requirement. Cost savings of up to 25 and 40 percent can be achieved through slicing in the two scenarios. Interestingly, the improvement is not monotonically increasing with network load. In some situations of high load, the vRAN resources are exhausted and cannot accommodate further caching functionality, leading to a reduction of relative cost benefit. This indicates that the slicing flexibility is better exploited under proper dimensioning of the network.

For real-life network scenarios, exact ILP solution approaches are impractical as they require immense computational and storage capabilities. In addition, the time requirement to instantiate a new slice might be in the range of seconds or less, whereas solving such an optimization problem exactly would require tens of minutes. For this reason, as already mentioned, heuristic approaches are used to provide near-optimal solutions to the basic NS/VNE problem in a short time.

Variants of the Network Slicing Problem

A number of variants and extensions to the basic NS problem are of great practical interest for next generation wireless networks.

Survivability constraints. In this case, redundant physical resources (nodes or paths) must be reserved to protect the slice from physical node or link failures. Many types of survivable slices can be considered: protection against single or multiple failures, correlated failures with shared risk groups, different types of protection (1+1, 1:1, shared backup, etc.), and different recovery schemes. Any efficient algorithm that solves the basic NS problem using a shortest path algorithm (e.g., Dijsktra's algorithm) as a subroutine could be extended to solve the 1+1 protection problem by substituting this subroutine with an efficient algorithm solving the 1+1 shortest pair of paths problem [7]. On the contrary, any protection scheme with shared backup introduces significant complexity, making efficient algorithms for the basic problem inadequate for the extended problem.

Quality of service constraints. The feasible embedding must also satisfy some quality of service (QoS) constraints. For example, each physical element (link or node) is associated with a fixed latency, and each virtual link can tolerate up to a maximum end-to-end latency. For each virtual link embedded to a given physical path, the sum of the individual latencies of the nodes and links forming the path must be less than the maximum virtual link latency. A number of other QoS constraints, including maximum jitter, maximum probability of packet loss, and so on, can be applied in isolation or in combination, substantially increasing the complexity of the problem. As in the survivability case, an efficient algorithm for the basic problem can be extended easily to the case of a single additive QoS constraint (e.g., a maximum delay constraint) by using an efficient algorithm for constrained min cost path computation.

Optical network constraints. As a large part of the network infrastructure of the future will be optical, taking optical network constraints into account is of significant importance. Optical network constraints are related to wavelength continuity and physical layer impairments (PLIs). PLIs cause notoriously difficult problems in path selection because they create nonlinear degradation to the optical signal. PLIs are also known to cause cross-wavelength signal interference. This can lead to the extremely complicated situation where one virtual network embedding can cause quality degradation to other embeddings and therefore impose additional constraints to the NS problem. Multi-layer (electrical and optical) NS has also received attention in the literature. In all such cases, the most promising approach is to decompose the problem into many independent subproblems [8].

Distributed operation. A centralized NS algorithm has complete knowledge of the physical network and all slices that need to be embedded. In some cases, this centralization of information might not be possible. Examples could include slices that traverse multiple operators and multiple SDN domains, or involve scalable designs with multiple SDN controllers. In these situations, a distributed slicing algorithm is required. Auction algorithms assuming a cost-utility model for the various actors in NS have been proposed for centrally supervised or fully distributed VNE and NS [9, references therein].

NFV specific constraints. The virtualization of network functions introduces novel characteristics that do not appear in traditional networking. For example, the bandwidth requirement of a flow may change as it passes through a VNF due to compression/decompression, or processing at

the VNF may introduce additional node latency, which is a function of the overall VNF load. Although it has been shown that such constraints can be incorporated in an ILP NS formulation [10], deriving efficient NS algorithms that address those issues is an open research topic.

Unique Challenges of Network Slicing

A number of important requirements are unique to NS and have not been addressed in the literature, to the best of our knowledge. These requirements are divided into the following broad categories:

End-to-end constraints. In the QoS routing literature, QoS constraints (e.g. maximum allowable end-to-end latency) are typically imposed per path and the possibility of a constraint across many paths is not considered. In NS, it is reasonable to consider an end-to-end latency requirement for a service chain, which is a latency constraint across a tandem of paths.

Heterogeneous requirements. In traditional network embedding, extensions such as QoS and survivability constraints are uniformly applied to the entire network. In NS, it is envisioned that different slices will have different requirements as they will serve diverse end-user applications. Even in the same slice, some links might require an increased degree of protection or QoS compared to others. For many solution approaches, extending the algorithm to the heterogeneous requirements case is not straightforward.

Multitenancy and nonlinear resource utilization. Multitenancy has been extensively studied in the literature of data center virtualization, since running multiple virtual machines on the same physical server introduces a non-negligible resource utilization overhead. In practice, due to contention for the shared physical resources, the utilized computational capacity on a virtual node is more than the sum of the resources allocated to each virtual node. This type of resource utilization model can be captured with the use of nonlinear functions. Similarly, if statistical multiplexing of traffic is desired, this can be modeled with nonlinear utilization functions on the physical links. Clearly, departing from linear cost functions complicates the solution of the resulting optimization problems considerably.

Slice fairness. A challenging problem is to decide how to split resources among different competing slices. In classical network flows, this challenge is resolved by the use of fairness metrics. However, the basic notion of fairness must now be generalized to involve entire slices instead of flows, and allow the consideration of multiple resources, like bandwidth, processing power, and memory, which leads to the problem of *slice fairness*. Some directions to resolve slice fairness include formulating the NS with convex utilities, and using the concept of multi-resource fairness [11] from the related literature of cloud computing.

Dynamic Network Slicing

Communication networks are inherently dynamic: a widely known example is the diurnal fluctuation of network flow that follows human activity. Other phenomena may also lead to time-varying slice requirements: cultural and sports events, service attacks and server downtime, variability of wireless channels, time-varying cost of virtual resource at different locations, failures of optical links, and so on. *The primary goal of dynamic NS is to allow the network operator to reconfigure and migrate the slices in order to match the network variability.*

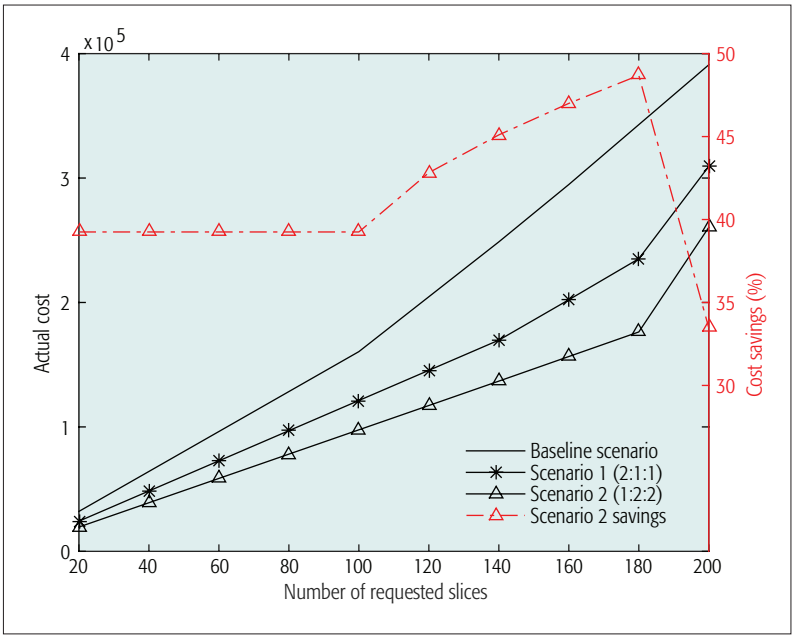


Figure 5. Quantifying the benefits of network slicing for heterogeneous services in resource utilization. Whereas the actual costs are increasing with load, the relative cost savings, as depicted by the red line, are improving up to the point where the vRAN resources are exhausted.

Dynamic NS is designed to support elastic networks (i.e., networks that change shape over time).[3] In elastic networks, the classical resource reservation explained in the previous section may not be enough, since the slices may need to scale up and down over time, or even change shape. Below we explain how to use monitoring and online optimization to provide effective dynamic Network Slicing.

Network State Monitoring and Prediction

To correctly drive the resource management decisions in the dynamic setting, the network operator needs to maintain an accurate depiction of resources that are currently used and their availability over time. A challenging problem therein is to model the resource utilization as a time evolving process.

Current network monitoring tools provide a static view of utilization for each network resource (link and node capacities, VNF capabilities, etc.). In a dynamic environment, the impact of embedding a particular slice on future slice requests is unclear. For example, consider the case of optimally embedding a slice based on static information. Once a new slice request arrives, a reconfiguration of the old slice might be needed due to resource contention. However, slice reconfiguration comes at a cost and hence a prediction mechanism of future resource utilization can be helpful.

Typically, prediction mechanisms rely on the use of historical data. In our context, techniques from machine learning can be used to exploit the raw monitored data from the SDN controllers and

[3] For example, the elastic content distribution networks (elastic CDNs) by Akamai Technologies and Juniper Networks use virtualized caching servers that can be installed at different locations possibly closer to the user demand.

The methodology of dynamic Network Slicing creates an arena of online optimization problems. To optimize the use of available resources and meet the time-varying slice requirements, the network operator needs to constantly optimize the slice resource allocation, while deciding to admit or not new slices.

derive predictions for the impact of new slices into the network [12].

Online Optimization

The methodology of dynamic NS creates an arena of online optimization problems. To optimize the use of available resources and meet the time-varying slice requirements, the network operator needs to constantly optimize the slice resource allocation, while deciding whether or not to admit new slices. This falls into the area of online optimization, where powerful algorithmic tools exist, such as stochastic network optimization and the domain of online competitive algorithms [13]. The *online NS* problem is related to other classical online problems such as:

- The online minimum cost multicommodity problem
- The online network embedding problem
- The online VNF placement problem
- The online packing problem
- The online facility location problem

and different variations of them.

Below, we consider methodological approaches for optimization problems of NS with an evolutional character.

A typical way of solving online problems is by using the offline optimization counterpart in two phases: quick assignment and readjustment [14]. The quick assignment phase exploits quick but suboptimal algorithms to decide how to embed the slices one by one. These assignments bring the system to a suboptimal configuration. Then the reconfiguration algorithms resolve the global offline resource optimization, and the slices are reconfigured into a well performing configuration. Trade-offs between cost and frequency of reconfigurations have been studied in [14] for the minimum cost multicommodity flow problem.

When the global optimization is difficult (as are most cases in NS), the mentioned approach spends a considerable amount of time on suboptimal configurations. To alleviate this phenomenon, a promising direction is to utilize the technique of Bandwidth Calendaring [15] The idea applies to slices with either predictable behavior or requested with early pre-booking. The network operator can construct a calendar of slice demands and resolve a time-expanded NS optimization problem covering a large period of time (e.g., a week or more).

When calendaring construction is not possible, the online optimization problems can be solved directly by online algorithms. The classical approach in this realm is to model the problem in the adversarial setup, meaning that the algorithms fight against the worst possible scenario of demand arrivals [13]. Although this typically results in conservative algorithms, it also provides very strong results in the form of algorithms with competitive ratios.

Conclusion

Network slicing is a novel methodology for provisioning resources in the upcoming wireless networks. This article illustrates numerous algorithmic challenges of slice optimization, which also represent promising research directions. Tools from the operation research, theoretical networking, and computer science are envisioned to provide network optimization algorithms and control techniques that can give practical answers to these challenges.

References

[1] F. Esposito, I. Matta, and V. Ishakian, "Slice Embedding Solutions for Distributed Service Architectures," *ACM Computing Surveys*, vol. 46, no. 1, Oct. 2013, pp. 6:1–6:29.

[2] NGMN Alliance, "NGMN 5G White Paper," Next Generation Mobile Networks Ltd., Frankfurt am Main, Germany, Mar. 2015.

[3] N. Nikaein *et al.*, "Network Store: Exploring Slicing in Future 5G Networks," *10th ACM Int'l. Wksp. Mobility in the Evolving Internet Architecture*, Sept. 2015.

[4] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From Network Sharing to Multi-Tenancy: The 5G Network Slice Broker," *IEEE Commun. Mag.*, vol. 54, no. 7, July 2016, pp. 32–39.

[5] A. Fischer *et al.*, "Virtual Network Embedding: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 4, Apr. 2013, pp. 1888–1906.

[6] R. Mijumbi *et al.*, "A Path Generation Approach to Embedding of Virtual Networks," *IEEE Trans. Network and Service Management*, vol. 12, no. 3, July 2015, pp. 334–48.

[7] M. R. Rahman and R. Boutaba, "SVNE: Survivable Virtual Network Embedding Algorithms for Network Virtualization," *IEEE Trans. Network and Service Management*, vol. 10, no. 2, June 2013, pp. 105–18.

[8] S. Peng, R. Nejabati, and D. Simeonidou, "Impairment-Aware Optical Network Virtualization in Single-Line-Rate and Mixed-Line-Rate WDM Networks," *OSA J. Optical Commun. and Networking*, vol. 5, no. 4, Apr. 2013, pp. 283–93.

[9] F. Esposito, D. D. Paola, and I. Matta, "On Distributed Virtual Network Embedding with Guarantees," *IEEE/ACM Trans. Net.*, vol. 24, no. 1, Feb. 2016, pp. 569–82.

[10] B. Addis, D. Belabed, M. Bouet, and S. Secci, "Virtual Network Functions Placement and Routing Optimization," *IEEE 4th Int'l. Conf. Cloud Networking*, Oct. 2015.

[11] A. Ghodsi *et al.*, "Dominant Resource Fairness: Fair Allocation of Multiple Resource Types," *8th USENIX Symp. Networked Systems Design and Implementation*, Apr. 2011.

[12] L. Nie *et al.*, "Traffic Matrix Prediction and Estimation Based on Deep Learning in Large-Scale IP Backbone Networks," *Elsevier J. Network and Computer Applications*, vol. 76, no. C, Dec. 2016, pp. 16–22.

[13] G. Even, M. Medina, and B. Patt-Shamir, "On-Line Path Computation and Function Placement in SDNs," B. Bonakdarpour and F. Petit, Eds. *Stabilization, Safety, and Security of Distributed Systems*, Springer Lecture Notes in Computer Science, vol. 10083, Nov. 2016.

[14] S. Paris *et al.*, "Controlling Flow Reconfigurations in SDN," *35th Annual IEEE INFOCOM*, Apr. 2016.

[15] L. Gkatzikis *et al.*, "Bandwidth Calendaring: Dynamic Services Scheduling over Software Defined Networks," *IEEE Int'l. Conf. Commun. (ICC)*, May 2016.

Biographies

Spyridon Vassilaras [M'05, SM'15] has been a principal research engineer at the Huawei France Research Center since December 2014. His main research interests are in network performance evaluation and optimization. He received his Dipl.Eng. degree from the National Technical University of Athens (1995) and his M.S. and Ph.D. degrees from Boston University (1997, 2001). From 2003 to 2014 he was a researcher and professor at Athens Information Technology. He has participated in nine EU funded projects and published numerous research papers.

Lazaros Gkatzikis [S'09, M'13] is a senior research engineer at the Huawei France Research Center. Previously, he held research-related positions at KTH Royal Institute of Technology, Sweden; Technicolor,France; and CERTH-ITI and the University of Thessaly, Greece. His research interests include network optimization, game theory, and performance analysis. He received his Ph.D. degree in computer engineering and communications from the University of Thessaly.

Nikolaos Liakopoulos received his B.S. in physics and M.S. in control and computing from National Kapodistrian University of Athens, Greece, in 2012 and 2015. In 2016 he joined Huawei France Resarch Center in the Network Control and Resource Allocation Team and is working toward his Ph.D. in collaboration with Eurecom and UPMC. His research focuses on distributed and centralized control for wireless networks and design of algorithms, specifically in software defined wireless networks and 5G network slicing.

Ioannis Stiakogiannakis [S'10, M'14] is a senior research engineer at Huawei. His experience has been in the design, development, and evaluation of algorithms for communication networks, such as 5G, LTE, elastic optical networks, and software defined networks. He is an IEEE Wireless Communications Professional, certified with IEEE WCET. He received his Dipl.-Ing. and Dr.-Ing. degrees from the School of Electrical and Computer Engineering, National Technical University of Athens in 2007 and 2011, respectively.

Meiyu Qi received her B.Sc. in mathematics from the University of Tianjin, China, in 2005. Then she obtained her M.S. in operation research from the same university in 2007. She finished her doctoral thesis at the University of Augsburg, Germany, in 2011. In the same year, she joined Huawei as a networking algorithm researcher in the Transmission Technologies Research Department. Her research expertise focuses on mathematical programming of algorithmic/meta-heuristic algorithmic applications in optical and IP networks. Since 2013, she has worked on SDN-related algorithm research.

Liu Liu received his M.Sc. and Ph.D. degrees in communication and information systems at the University of Electronic Science and Technology of China in 2011 and 2015, respectively. He was a visiting scholar in computer science and engineering at the State University of New York at Buffalo from 2012 to 2014. He joined Huawei as a research engineer in 2015. His research interests focus on network planning and optimization, uncertainty optimization, approximation algorithms, and cloud computing.

Lei Shi got his Master's in computer science from the University of Sichuan, China, in 2005. In the same year, he joined Huawei as an engineer in the WDM product line, and in 2007 became a networking algorithm researcher in the Transmission Technologies Research Department. His research expertise focuses on mathematical programming algorithmic/meta-heuristic algorithmic applications in IP, optical, and microwave networks.

Mérouane Debbah [S'01, M'04, SM'08, F'15] entered the Ecole Normale Supérieure de Cachan, France, in 1996 where he received his M.Sc. and Ph.D. degrees, respectively. Since 2014, he is vice-president of the Huawei France R&D Center and director of the Mathematical and Algorithmic Sciences Lab. His research interests lie in fundamental mathematics, algorithms, statistics, information, and communication sciences research. He is a WWRF Fellow. He has managed 8 EU projects, and 24 national and international projects, and received more than 16 best paper awards for his research contributions.

Georgios S. Paschos [S'01, M'06, SM'15] is a principal researcher at Huawei Technologies, Paris, France, leading the Network Control and Resource Allocation team, since November 2014. Previously, he held positions at VTT,Finland; CERTH-ITI and University of Thessaly, Greece; and Massachusetts Institute of Technology. He received his Dipl.Eng. from Aristotle University of Thessaloniki (2002) and his Ph.D. degree from the University of Patras (2006). He has received two best paper awards and serves as an Associate Editor for *IEEE/ACM Transac tions on Networking* and as a TPC member of IEEE INFOCOM.

A Cloud-Native Approach to 5G Network Slicing

Sameerkumar Sharma, Raymond Miller, and Andrea Francini

The authors present a cloud-native approach to network slicing that advances a fundamental rethinking of the mobile network to shift its architectural vision from a network of entities to a network of capabilities, and its driving purpose from a network for connectivity to a network for services.

ABSTRACT

5G networks will support very diverse and challenging requirements. Network slicing offers an effective way to unlock the full potential of 5G networks and meet those requirements using a common network infrastructure. This article presents a cloud-native approach to network slicing that advances a fundamental rethinking of the mobile network to shift its architectural vision from a network of entities to a network of capabilities, and its driving purpose from a network for connectivity to a network for services. The approach covers the entire life cycle of network slices, encompassing their design, creation, deployment, customization, and optimization. We provide an overview of our cloud-native approach to network slicing and describe a proof-of-concept implementation that demonstrates its key principles.

INTRODUCTION

The fifth generation (5G) network will power a new era of applications, services, and use cases, many of which are still unknown [1–3]. Besides an ever growing number of mobile broadband subscribers, there will be government agencies and enterprises in industries old and new, connected through all sorts of devices and machines. The requirements for network capabilities will be very diverse and extremely demanding [4, 5]. As shown in Fig. 1, they include ultra-low end-to-end latency (less than 1 ms), ultra-high bit rates (in the gigabit-per-second range), ultra-high availability and reliability, massive density of connected devices, and energy efficiency.

Network slicing is the distinctive new 5G technology that will make it possible to support diverse requirements at the finest level of granularity over a common network infrastructure. A network slice is a connected set, or chain, of network functions, logically creating a dedicated virtual network that satisfies the specific requirements of a service, use case, or business model [6]. Figure 2 depicts a conceptual view of various network slices supported by a common network infrastructure. When the network functions are virtualized (i.e., implemented in software over general-purpose hardware) [7], network slices can be designed flexibly to support the most diverse needs, and operated elastically for efficient handling of variable network and service loads. Network slicing enables multiple virtual networks to operate independently over a shared infrastructure [8].

When designing a network slice, it may be natural to proceed by simply mapping the functions of the legacy network onto virtualized instances that run in dedicated software modules (like dockerized containers and/or virtual machines) and then chaining the functions together based on the requirements of the supported services. This plain translation from legacy hardware to a virtualized environment has obvious benefits with respect to the provisioning, operation, and performance of the network, but misses two key opportunities that are created by the most recent advances in cloud technologies.

First, the distributed cloud infrastructure that constitutes the backbone of the 5G network is the ideal environment for decomposing the large monolithic network functions of legacy hardware into a broad catalog of modular network capabilities of varying granularity. Those capabilities can then be chained in many ways to form network slices that support the most diverse services. Second, the design of a network slice can be continuously enhanced through autonomous optimization driven by insights collected at runtime from the network and the services. We envision that analytics, machine learning, and autonomic network management functions will enable the automation and optimization of the network slice life cycle, from design and creation to optimization and deletion. The comprehensive leveraging of cloud technologies is a distinctive feature of our cloud-native approach to network slicing.

This article significantly expands and deepens an introductory description of dynamic end-to-end network slicing previously given in [9]. We start with a discussion of the general concept of network slicing and then highlight its benefits. Next, we review the distinctive characteristics of our cloud-native approach to network slicing and illustrate their expression in every phase of the network slice life cycle, from design and creation to operation and optimization. Finally, we present a proof-of-concept system that demonstrates our cloud-native approach in an end-to-end mobile network.

THE ENABLING ROLE OF NETWORK SLICING

Network slicing will be instrumental to the realization of some of the key possibilities enabled

Digital Object Identifier:
10.1109/MCOM.2017.1600942

The authors are with Nokia Bell Labs.

0163-6804/17/$25.00 © 2017 IEEE

by 5G. The following subsections outline those possibilities and the role of network slicing in their realization.

Rapid Launch of New Applications and Services

Legacy mobile networks were designed for the delivery of personal communication services and content, such as voice, video, and web browsing. 5G will be the network of a fully mobile and fully connected society. The widespread dissemination of wearable devices and wirelessly connected objects will pave the way to a broad variety of new applications and services. In addition to giving impulse to the advancement of human-centric applications, such as those for augmented reality/virtual reality (AR/VR) immersion, 5G networks will bring into existence applications that rely on fundamentally new paradigms for the exchange of data, such as machine-to-machine (M2M) and vehicle-to-vehicle (V2V) communications. These applications will automate and mobilize a variety of industries, including energy, health, public safety, smart city, manufacturing, logistics, media, and automotive.

Network slicing will make it feasible to rapidly introduce new applications without large additional capital investments. The modularity of the network function chains that make up the network slices will expedite the process of creating and activating new services. By promoting an open service ecosystem, network slicing will facilitate the cooperation of diverse specialized entities in the realization of enriched services and solutions.

Coexistence of Heterogeneous Use Cases and Business Models

Beyond connectivity, 5G will offer operators unique opportunities to create new business models and enable new use cases for consumers, enterprises, and industry-specific services, as well as for content and application providers. Operators understand that the success of the 5G family of technologies will come from their ability to provide value-added solutions for all types of requirements while meeting the unique needs of every stakeholder [6]. Network slicing enables the coexistence of multiple end-to-end virtual network instances, each dedicated to a specific class of service, use case, or business model [8].

Heterogeneous Performance Guarantees

5G will guarantee unprecedented levels of network performance with respect to all quality of service (QoS) metrics (data rate, packet latency, availability, reliability, etc.). New physical and link-layer technologies for the wireless link and new mobile access protocols will be essential to meeting the stringent new requirements. The contribution of the network and end-to-end transport layers will also be needed to close critical gaps that exist in legacy networks, such as the relatively poor performance of the Transmission Control Protocol (TCP) over typical wireless links.

Dedicating a separate physical network to each combination of requirements is too expensive. Network slicing provides the foundation for a shared network infrastructure to satisfy the performance requirements of the most diverse services and applications.

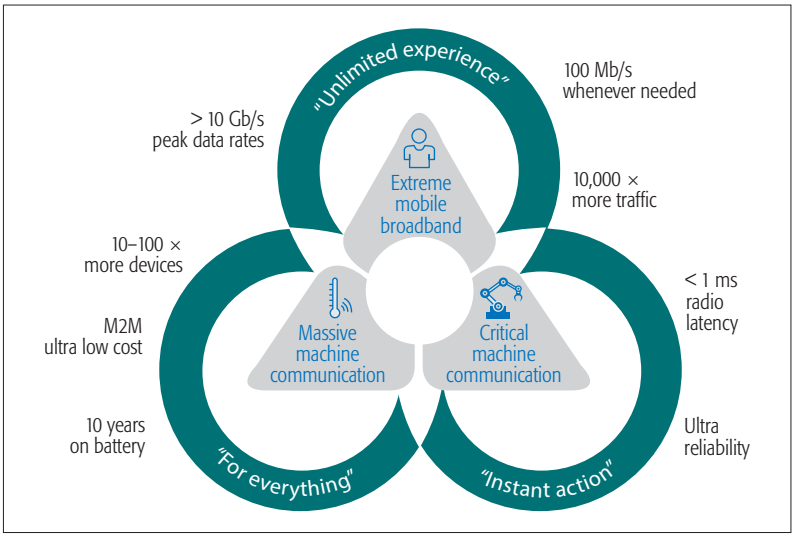


Figure 1. 5G networks will support very diverse and extreme requirements.

Capital and Operational Expenditure Savings

5G network slicing enables multiple, logically isolated networks to run on a common physical infrastructure. It abates the capital cost of introducing new applications and services because it marginalizes the impact of their deployment on the physical infrastructure of the network. Being conducive to the elastic redistribution of hardware resources among services based on their current traffic and data processing loads, it also shifts the criterion for dimensioning the overall network infrastructure from the sum of the peak demands of the individual services, whenever they occur, to the peak of the aggregate load generated jointly by all services.

With a unified approach to operations and management, network slices will significantly reduce the operational expenses of service providers compared to separate physical networks. Sizeable savings will come from simplified software maintenance and upgrades, from automation powered by analytics and machine learning, and also from much lower energy consumption, because a common framework for energy efficiency is easier to run on a less diversified hardware and software base.

The Cloud-Native Approach

Our cloud-native approach extends the vision of the Next Generation Mobile Network (NGMN) Alliance [6] on the concept of 5G network slicing. It combines modern design principles and key enabling technologies from cloud computing to create a novel architecture and framework for all phases of the network slice life cycle.

Enabling Cloud Technologies and Design Principles

Our cloud-native approach to 5G network slicing leverages a broad set of cloud technologies, some of which are mature, while others have just started emerging. The most prominent ones are: distributed cloud infrastructure, cloud-native applications, network functions virtualization (NFV), containerization and end-to-end orchestration; micro-services; software-defined networking (SDN); programmable networking; intent-based network programming [10]; network big data,

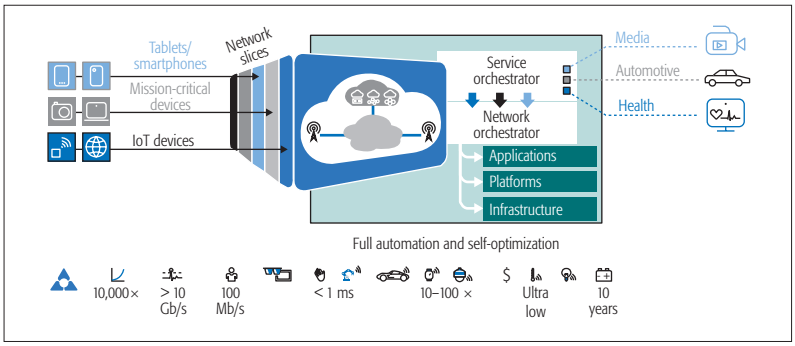


Figure 2. Network slices in 5G.

analytics, and machine learning; service-oriented architectures; and network insights as a service (NIaaS).

The approach also embraces the following design principles.

Virtualized and Distributed Infrastructure: Wherever possible, the 5G network functions and capabilities should be developed and deployed on a distributed cloud infrastructure that leverages cloud-native applications and proven technologies for virtualization and containerization. Dedicated and purpose-built network elements should be used only when strictly irreplaceable.

Shift from Network of Entities to Network of Capabilities: Past and present networks are built on large and monolithic network entities. The mobility management entity (MME), serving gateway (SGW), and packet data network gateway (PGW) are just a few LTE examples. The virtualization of these network entities is becoming more and more common, but their monolithic nature remains. So far, virtualization has primarily changed the way network functions are deployed, not the way they are designed. Instead, the cloud-native approach eliminates the functional partitions of legacy equipment. The slices become chains of modular network capability units (NCUs) that are easy to deploy and manage, and made to work in unison over a common infrastructure of general-purpose processors (GPPs). An NCU is a unified abstraction of a network capability (e.g., packet scheduling) or function (e.g., network authentication). NCUs are modular and can be easily chained and connected to form larger network functions or end-to-end network slices. NCUs can be defined at different levels of granularity and can be implemented in various forms, as containerized applications, native micro-services, or complete virtualized network functions.

Shift from Network for Connectivity to Network for Services: Legacy networks were built primarily to provide connectivity. The 5G network should be built to provide a broad set of very diverse services. Accordingly, the cloud-native design of a network slice is driven from the ground up by the features of the service or group of services that the slice will support. This ensures that 5G network slices will have not only the unique capabilities that are required for their corresponding services, but also the ability to dynamically adapt those capabilities to the specific needs of each service.

Dynamic Programmability and Automation: SDN was originally conceived for dynamic and flexible control of data path functions like routing and traffic management. The cloud-native approach extends the SDN paradigm to the full set of functions and capabilities that are abstracted into NCUs, yielding network slices where not only the data plane but also the control and management planes are highly programmable. Analytics and machine learning enable pervasive automation of the processes for optimization of the slices and thus help abate the complexity of running many network slices concurrently.

End-to-End Perspective: 5G network slices span across all network segments, from access to core, from metro to transport. Application endpoints, in both network servers and user equipment (UE), may also be included depending on the type of application and underlying service. The cloud-native approach emphasizes the contribution to the capabilities and performance of the 5G slice that comes from every NCU in its service chain. In every cloud-native slice, the individual segments of the network are no longer treated as separate, independent entities. Instead, they compose a cohesive end-to-end vision where the contribution of each segment to performance assurance is fully specified in every aspect, from the allocation of per-metric budgets to the measurements and enforcement actions that occur while the slice is in operation. Analytics and context awareness support the real-time adaptation of services and network slices to the effects of service-load variations on end-to-end performance. Such an end-to-end perspective is instrumental in meeting the challenging service requirements of 5G with network slices that are efficiently designed and implemented.

Easy Design of Network Slices: The modularity of the NCUs that abstract the network capabilities simplifies the initial design of new network slices. A slice is simply built as a forwarding graph of NCU nodes. Proven orchestration and management technologies are then used to instantiate and activate the forwarding graph on the distributed cloud infrastructure. Slice templates help eliminate routine errors from the slice creation process. The template provides the primary and more general features of the new slice. Next, the specialized capabilities are added in sequence to adapt the slice to the requirements of particular services, use cases, and business models.

Architectural Features

Combination of the design principles and enabling technologies that we have just discussed yields network slices with a common set of architectural features. These common features are listed below:

- Every slice supports groups of services, use cases, or business models that have similar requirements. For example, an operator can run a mobile broadband slice that offers a variety of broadband services to its customers, including web browsing, audio and video streaming, and chat.
- Every slice is composed only of the network capabilities that satisfy the requirements of the supported services, use cases, or business cases. For example, only a slice that supports ultra-low-latency use cases includes an NCU that guarantees ultra-low latency in the access network.

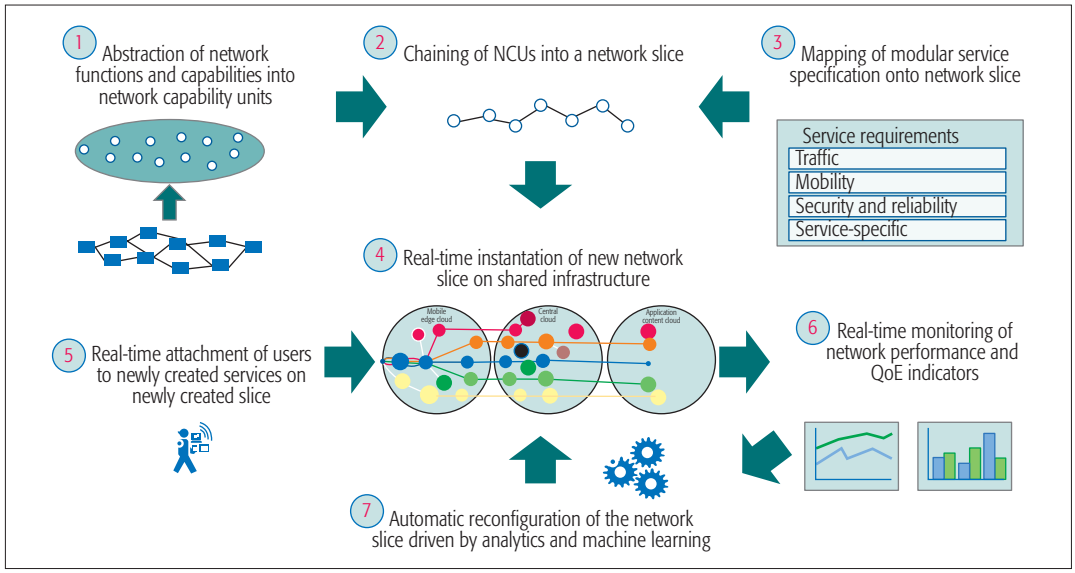


Figure 3. Life cycle of a cloud-native network slice.

The modularity of the NCUs that abstract the network capabilities simplifies the initial design of new network slices. A slice is simply built as a forwarding graph of NCU nodes. Proven orchestration and management technologies are then used to instantiate and activate the forwarding graph on the distributed cloud infrastructure.

- The NCUs that compose a slice are not limited to the user plane. They can also provide functionality for the control and management planes. For example, an NCU may instantiate a dynamic controller for optimization of video streaming quality of experience (QoE), or a type of billing application that is relevant to the business case supported by the slice.
- Every slice is dynamic and keeps evolving while it is in operation. It subscribes to an automation framework that uses real-time monitoring, analytics, and machine learning to refine and optimize it in response to variations in service requirements and traffic load.

Life-Cycle Management of Cloud-Native Network Slices

We logically divide the life cycle of cloud-native network slices into three phases: design and creation, orchestration and activation, and analytics and optimization. Figure 3 offers a seven-step workflow overview of the three phases, which we further describe in the following subsections.

Design and Creation Phase

The design and creation phase is where the network slice is conceptually constructed. The phase includes the following steps:

1. Creation of a catalog of NCUs. NCUs are abstractions of network functions and capabilities and constitute the building blocks of all network slices. The granularity of the NCUs is at the discretion of the virtualized network provider and should reflect the composable capabilities of the network. The creation of the NCU catalog logically precedes the design of network slices. However, the need to add a new NCU to the catalog typically emerges in the middle of designing a new slice, so the NCU catalog keeps expanding as new slices are designed.
2. Chaining of NCUs to form a network slice. The result is a forwarding graph of the slice with all associated NCUs and their relationships.
3. Mapping of one or more services to the newly created slice.

Orchestration and Activation Phase

The orchestration and activation phase consists of the following steps:

4. Instantiation of the network slice on the shared physical infrastructure. The NCUs of the slice are orchestrated on the distributed cloud infrastructure in their designated form of virtualization (virtual machines or dockerized containers). The connectivity of the forwarding graph is established between the NCUs.
5. Activation of the slice and corresponding services. Users are associated with the services of the slice, and traffic starts flowing through the slice.

Analytics and Optimization Phase

The analytics and optimization phase starts upon activation of the network slice. It involves the following steps:

6. Continuous monitoring of the performance indicators for the network slice (network load, utilization of allocated resources, end-to-end delay, data throughput, outages, etc.) and its associated services (service level agreements, QoE, etc.).
7. Automatic reconfiguration of the network slice based on the output of analytics processes and machine learning optimization tools.

Proof-of-Concept System

In this section, we describe a proof-of-concept (PoC) system for our cloud-native approach to network slicing. The PoC system implements the complete life cycle management of network slices. It contains the interfaces and logic for designing, creating, orchestrating, and activating the slices. It provides a front-end graphical user interface (GUI) to assist in the visualization of the concept, design, and deployment of network slices. It is implemented over a real end-to-end network: when a slice is activated, the virtualized capabilities of the network slice are retrieved from a slice repository and orchestrated in real time into the appropriate resources.

The PoC system includes a default slice for basic mobile wireless access. The activation of a new slice produces immediate changes in the

The design of a network slice consists of the selection and connection of its NCUs. If a new slice requires capabilities that no NCU in the catalog can offer, one or more new NCUs must be on-boarded within both the NCU repository and the front-end design interface. The slice must be complete with all its NCUs before the service can be activated.

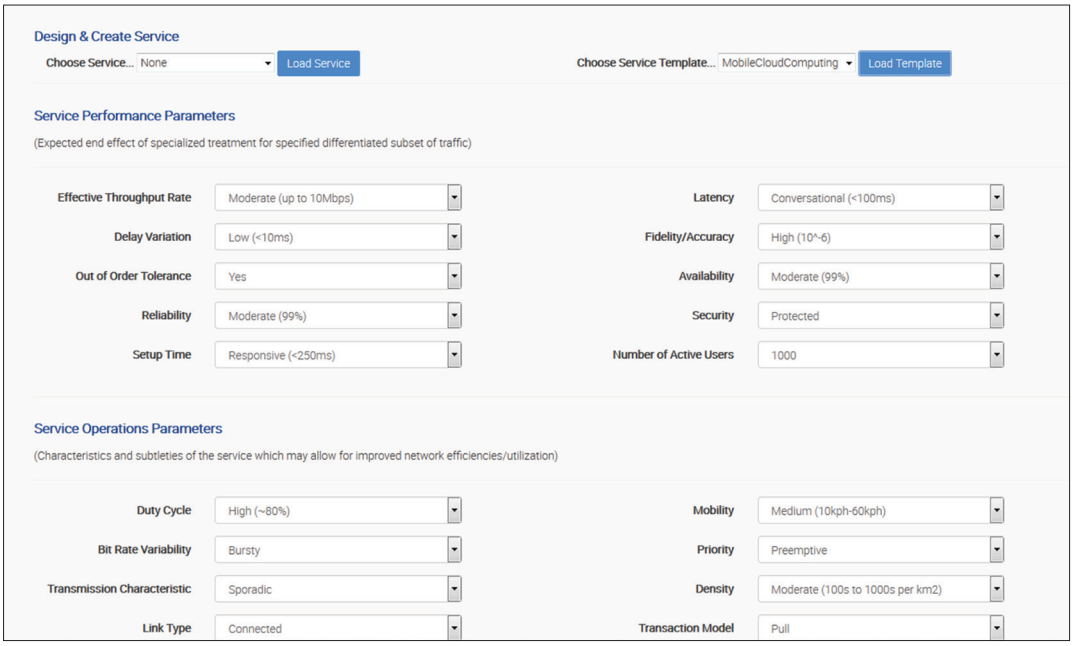


Figure 4. GUI for design and creation of a service.

behavior of the applications it supports vs. the default slice (e.g., improvement in video quality or reduction in end-to-end packet latency). The PoC system has been showcased at numerous key industry events for demonstration of a variety of 5G network slicing use cases, including dynamic service optimization, integration of SDN-programmable transport, and new verticals, such as Industry 4.0 [11].

Service Design and Creation

Service design is the decomposition of a use case into a modular service specification. Service creation is the step of storing the service specification in the service repository. The service specification guides the design of the network slice to ensure that the slice will meet the service requirements, for example, by filtering the NCU catalog so that only NCUs which are relevant to the service are included in the slice.

To streamline the creation of new services, the PoC system features a service specification template that consists of a set of unique, non-overlapping parameters and value ranges that distinguish each service and the way the network must support it. These parameters and their chosen values translate into network capabilities and performance objectives that ultimately define the service. Note that these parameters do not include implicit or explicit references to specific technologies or implementations.

The service parameters are further categorized into service performance parameters, service operations parameters, and service monitor and control parameters (Fig. 4 shows examples of the first two sets). The service parameters and their value ranges can keep evolving over time as the network refines its support of existing services and adds new slices to support new services.

Not all parameters are relevant to all use cases, and not all combinations of parameters result in a practical service definition. However, those that are meaningful are used during the creation and orchestration of the network slices. Also note that the number of services created is at the discretion of the service provider and is dictated by the granularity of the service definition and network capabilities specified. That is, a single service can support a wide range of distinct use cases if defined broadly enough, and a single network slice can support multiple services if the requirements of those services are met by the capabilities of the slice.

Network Slice Design and Creation

The design of a network slice consists of the selection and connection of its NCUs. If a new slice requires capabilities that no NCU in the catalog can offer, one or more new NCUs must be onboarded within both the NCU repository and the front-end design interface. The slice must be complete with all its NCUs before the service can be activated.

An NCU may represent either a data-plane or control-plane capability. The relative complexity of the NCUs does not need to be the same. NCUs may be micro-capabilities implemented in dynamic nimble containers or macro-capabilities implemented in more static and robust virtual machines. The granularity of the decomposition is at the discretion of the network provider and should reflect the services to be offered. The representation of capabilities is fluid. That is, several micro-capabilities may be combined to create one macro-capability.

Once the network capabilities have been abstracted and the corresponding NCUs created, a network slice can be designed. In the GUI of the PoC system, the NCUs are shown as bubbles. Designing a network slice consists of linking the available NCUs into graphs/chains to meet the needs of one or more services. Figure 5 shows a network slice as an NCU chain. The figure presents a simplified version of the capability decomposition of our demo network. The tool allows a user to design the slice from scratch by

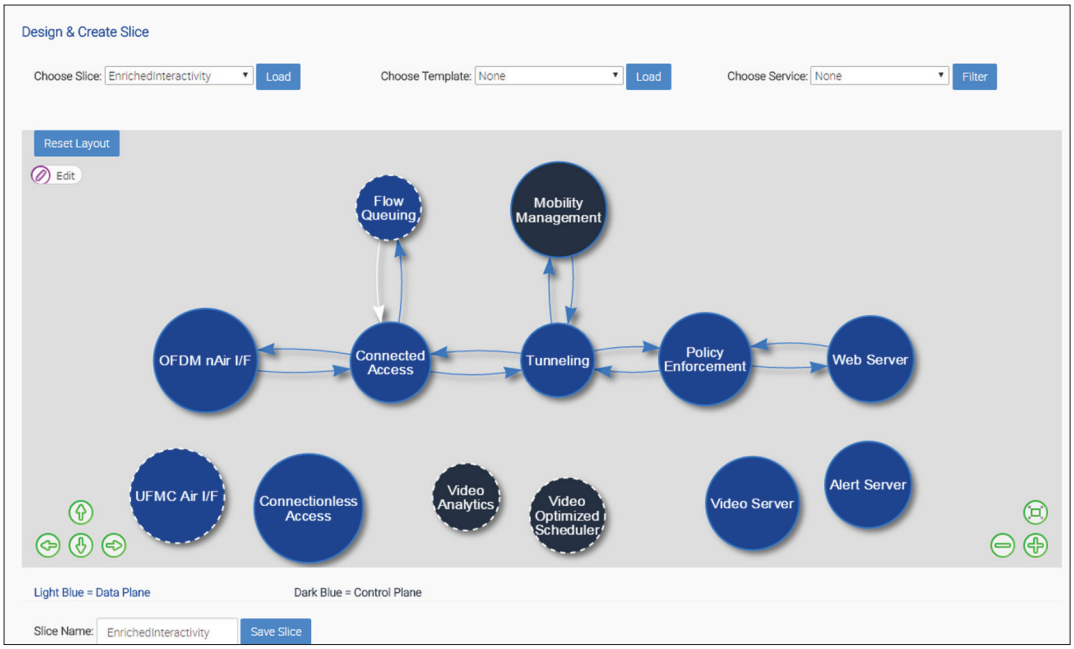


Figure 5. GUI for design and creation of a network slice.

The service-to-network-slice mapping is the final step of the slice creation phase. It consists of defining and storing a mapping between one or more service identifiers with a network slice identifier, so that when an end user requests a service, the network knows on which slice to forward the traffic.

linking individual NCUs together or by modifying an existing slice or slice template. The available NCUs can also be filtered to include only those that meet a particular set of service requirements.

The slice is created when its specification is saved into the slice repository. However, at this stage the slice and its NCUs are not yet instantiated on the distributed cloud infrastructure.

Service-to-Network-Slice Mapping

The service-to-network-slice mapping is the final step of the slice creation phase. It consists of defining and storing a mapping between one or more service identifiers with a network slice identifier so that when an end user requests a service, the network knows on which slice to forward the traffic. In the demo system, this is accomplished by a simple configuration file lookup. In a production system, the user must be authorized for the service, possibly in the subscriber database, and the service-to-network-slice mapping must be reachable during service activation.

Network Slice Orchestration and Activation

Once the network slice has been created and services have been mapped to it, the slice can be orchestrated and activated. Orchestration is the dynamic, real-time instantiation of NCU chains onto the common infrastructure, which is primarily composed of multiple distributed clouds, including edge cloud, central cloud, and application/content cloud. The activation allows services to use the slice, or more specifically allows the real-time attachment of users to newly created services on newly created network slices.

The slices make use of capabilities that can be dedicated (i.e., one per slice, as in the case of one packet scheduler instance per slice) or shared (e.g., the same air interface for multiple slices). Orchestration is performed as follows: The front-end sends a message to a back-end controller first for retrieval of the NCU from a central repository and its assignment to the appropriate place within the infrastructure (i.e., mobile edge cloud, central cloud, or application/content cloud), and then for instantiation and activation of the NCU in a container or virtual machine.

PoC Slice Instances

Figure 6 shows network slices that have been created and are ready for orchestration and activation in the PoC system. In this visualization of the GUI each slice is represented by a different color.

The blue slice provides the capabilities needed for realization of the default enhanced mobile broadband (eMBB) service. The slice chains NCUs for the orthogonal fequency-division multiple access (OFDMA) air interface, for connected access, for core connectivity (tunneling), for mobility management, and for policy enforcement. The specification of the eMBB service assigns loose ranges to performance parameters like throughput and latency for best effort support of over-the-top applications like voice, video conferencing, video streaming, and web browsing. By default, any service that is not mapped to another slice, or is mapped to a slice that is not active, uses the eMBB slice.

The red slice is designed to minimize the end-to-end latency of interactive applications such as gaming and voice over IP. This enriched-interactivity slice shares the air interface and connected access NCUs with the eMBB slice, chains dedicated instances of the tunneling, mobility management, and policy enforcement NCUs, and adds a specialized flow-queuing NCU in the radio access network (RAN) to isolate flows of concurrent applications that share the same wireless access link. This avoids the disruption of gaming or video conferencing sessions whenever the UE engages in a large data transfer with a network server (e.g., for downloading a movie or a new application). In a loaded and congested PoC system we measured reductions of the peak PING round-trip time to the web server in the application/content cloud from more than 800 ms to less than 40 ms after runtime activation of the enriched interactivity slice.

The anomaly detection algorithms can be updated in a central location without needing to retrofit a large number of surveillance cameras. Also, different algorithms can be applied to different sets of cameras at different times. Since the cameras are fixed, the slice does not include a mobility management NCU.

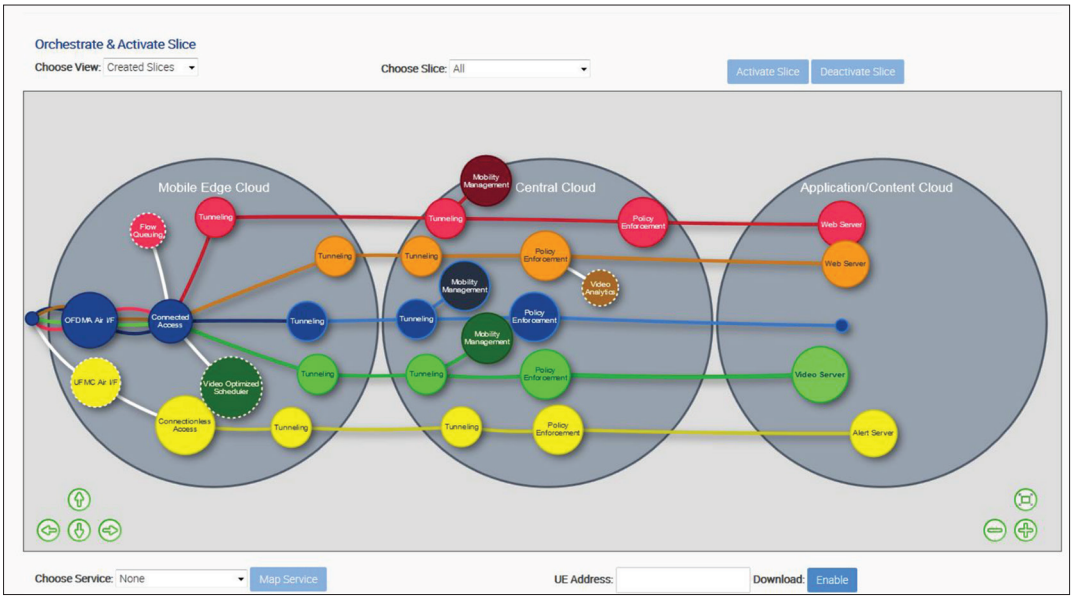


Figure 6. GUI for orchestration and activation of network slices.

The orange slice attaches a video analytics NCU to the policy enforcement NCU. The slice enables the realization of a video monitoring service with minimal consumption of radio resources. Instead of generating a continuous video stream, each camera periodically uploads only a small amount of metadata that the video analytics NCU processes for anomaly detection. When the NCU recognizes an anomaly in the metadata, it activates the corresponding camera for actual video streaming. The anomaly detection algorithms can be updated in a central location without needing to retrofit a large number of surveillance cameras. Also, different algorithms can be applied to different sets of cameras at different times. Since the cameras are fixed, the slice does not include a mobility management NCU.

The green slice includes a video-optimized scheduler NCU that refines the air interface scheduling of downlink video streaming flows based on channel conditions and on the behavior of other video flows within the slice [12]. The slice enables a mobile video streaming service that enhances the collective QoE of the video users while increasing the availability of radio resources for flows of other applications.

The yellow slice supports a fixed-location massive Internet of Things (IoT) service for sensor monitoring. It includes specialized NCUs for a universal filtered multi-carrier (UFMC) air interface, for connectionless access [13], and for alert generation. By removing the signaling overhead of connected access, the slice enables low-latency processing of short-burst messages from a large population of fixed sensors. The resulting spectral efficiency improvement ensures the scalability of this service for support of massive amounts of sensors or IoT devices.

PoC System Testbed

The PoC system is built on an LTE network with extensions for virtualized network capabilities and network slices.

A portable version of the PoC system consists of one Ettus B210 Universal Soft Radio Platform (USRP) as the radio head of the LTE radio access network (RAN), and seven Intel i7 Next Units of Computing (NUCs) with the following roles:

- Application/content cloud (one NUC), hosting web, video, and GUI servers
- Central cloud (one NUC), hosting the LTE Evolved Packet Core (EPC)
- Mobile edge cloud (one NUC), hosting the LTE radio access network (RAN)
- Four end-user devices (one NUC each, with respective USB-dongle LTE adapter)

Our NCUs run over Linux virtual machines (VMs) and dockerized containers. The life cycle management GUI is built on Linux VMs, the Django web framework, an nginx web server, and a PostgreSQL database. OpenStack services and components provide programmable networking and orchestration functions. The analytics framework leverages software from the following Apache projects: Mesos (cluster manager), Kafka (stream processing), and Cassandra (distributed database). We are now in the process of extending the PoC system to commercial Nokia products.

Conclusion

The cloud-native approach to 5G network slicing covers all phases of the slice life cycle. It leverages state-of-the art technologies and embraces advanced design principles to deliver network slices that can meet the many challenging requirements of the new services envisioned for 5G networks. The cloud-native approach allows mobile operators to devise network architectures and deployment scenarios that are tailored to the needs of every business model, use case, and service group. We have demonstrated the cloud-native approach to creating, orchestrating, and optimizing network slices in a proof-of-concept system that runs on a complete end-to-end mobile network.

Acknowledgments

The authors thankfully acknowledge the contribution of the following colleagues to the conception, realization, and demonstration of the 5G

network slicing solution presented in this article: M. L. Alberi-Morel, P. Andrews, B. Cilli, B. Erman, D. Faucher, F. Faucheux, E. Grinshpun, V. Gurbani, S. Kerboeuf, C. Payette, and C. Sartori.

References

[1] ITU-R Rec. M.2083, "IMT Vision — Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," Sept. 2015.

[2] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 3, 3rd qtr. 2016, pp. 1617–55.

[3] J. G. Andrews *et al.*, "What Will 5G Be?," *IEEE JSAC*, vol. 32, no. 6, June 2014, pp. 1065–82.

[4] J. Thompson *et al.*, "5G Wireless Communications Systems: Prospects and Challenges," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. 62–64.

[5] F. Boccardi *et al.*, "Five Disruptive Technology Directions for 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. 74–80.

[6] NGMN Alliance, "NGMN 5G White Paper," v.1.0, Feb. 2015; https://www.ngmn.org/5g-white-paper.html.

[7] ETSI NFV ISG, "ETSI GS NFV-002 Architectural Framework," v.1.2.1, Dec. 2014; http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf.

[8] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From Network Sharing to Multi-Tenancy: The 5G Network Slice Broker," IEEE Commun. Mag., vol. 54, no. 7, July 2016, pp. 32–39.

[9] "Dynamic End-to-End Network Slicing for 5G," Nokia White Paper, July 2016, available: https://insight.nokia.com/dynamic-end-end-network-slicing-unlocks-5g-possibilities.

[10] P. A. Aranda Gutiérrez and D. R. López, "Fighting Your Way through the Jungle of Intent," *IEEE Software Defined Networks Newsletter*, Sept. 2016; http://sdn.ieee.org/newsletter/september-2016/fighting-your-way-through-the-jungle-of-intent.

[11] M. Hermann, T. Pentek, and B. Otto, "Design Principles for Industrie 4.0 Scenarios," *Proc. 49th Hawaii Int'l. Conf. System Sciences*, Koloa, HI, Jan. 2016, pp. 3928–37.

[12] D. De Vleeschauwer *et al.*, "Optimization of HTTP Adaptive Streaming over Mobile Cellular Networks," *Proc. 32nd IEEE INFOCOM 2013*, Turin, Italy, Apr. 2013, pp. 989–97.

[13] C. Kahn and H. Viswanathan, "Connectionless Access for Mobile Cellular Networks," *IEEE Commun. Mag.*, vol. 53, no. 9, Sept. 2016, pp. 26–31.

Biographies

Sameerkumar Sharma (sameer.sharma@nokia-bell-labs.com) is head of Autonomic Networks and Mobile Services research in Nokia Bell Labs. He leads a global team spearheading breakthrough technologies and innovations. He has held various leadership positions in innovation, technology, and product teams, and has worked across Asia, Europe, and the United States. His current focus areas are end-to-end mobile/IP networks/services, cloud computing, analytics, machine learning, SDN, NFV, IoT, and security. He has pioneered multiple new product concepts, holds numerous patents, and has published many papers.

Raymond Miller (ray.miller@nokia-bell-labs.com) is a researcher in the Autonomic Networks and Mobile Services research department at Nokia Bell Labs. He holds a degree in electrical engineering from Rutgers University. He has 30 years of experience in research and development of network and wireless-communication systems, including core optical systems, metro Ethernet systems, and 3G/4G wireless systems. He is currently engaged in research pertaining to 5G end-to-end services and network architectures.

Andrea Francini (andrea.francini@nokia-bell-labs.com) has been with Nokia Bell Labs since 1997. He holds a Ph.D. in electrical engineering and communications from the Politecnico di Torino, Italy. He is a traffic management expert with extensive experience designing quality-of-service architectures for packet switching chipsets, broadband access platforms, and mobile wireless networks. His current research focus is on congestion control solutions that fit every application with the ideal balance between data throughput and end-to-end packet delay.

The cloud-native approach to 5G network slicing covers all phases of the slice life cycle. It leverages state-of-the art technologies and embraces advanced design principles to deliver network slices that can meet the many challenging requirements of the new services envisioned for 5G networks.

5G-Crosshaul Network Slicing: Enabling Multi-Tenancy in Mobile Transport Networks

Xi Li, Ramon Casellas, Giada Landi, Antonio de la Oliva, Xavier Costa-Pérez, Andres Garcia-Saavedra, Thomas Deiß,Luca Cominardi, and Ricard Vilalta

The authors present the 5G transport network architecture designed in the 5G-Crosshaul project. An SDN/NFV-based control plane has been designed that enables multi-tenancy through network slicing. The proposed solution allows for flexible and efficient allocation of transport network resources to multiple tenants by leveraging widespread architectural frameworks for NFV and SDN.

ABSTRACT

5G requires a redesign of transport networks in order to feed the increasingly bandwidth hungry radio access networks and to benefit from the performance/cost efficiency provided by the integration of both backhaul and fronthaul segments over the same transport substrate as well as the incorporation of cloud RAN architectures. In addition, to increase its usage and cost efficiency, this new transport network should allow simultaneous use by different tenants (e.g. MVNOs, OTTs, and vertical industries). This article presents the 5G transport network architecture designed in the 5G-Crosshaul project to address this challenge. An SDN/NFV-based control plane has been designed that enables multi-tenancy through network slicing. The proposed solution allows for flexible and efficient allocation of transport network resources (networking and computing) to multiple tenants by leveraging on widespread architectural frameworks for NFV (ETSI NFV) and SDN (e.g., Open Daylight and ONOS).

INTRODUCTION

Fifth generation (5G) mobile transport networks will support multiple cloud radio access network (RAN) functional splits in a flexible and unified manner. This will allow for various degrees of RAN centralization, varying from distributed RAN (D-RAN) to fully centralized RAN (C-RAN). Thus, 5G transport networks will flexibly distribute and move base station functions across data centers, introducing another degree of freedom for resource management. In this context, the division between *fronthaul*, which is the interface between the remote radio heads (RRHs) and their associated centralized processing units (baseband units, BBUs), and *backhaul* will blur, since varying portions of functionality of the base stations will be moved flexibly across the transport network, as required for cost efficiency/performance reasons. In order to fulfill these requirements, we propose a new generation of transport networks for 5G integrating both fronthaul and backhaul segments into a common transport infrastructure, defined as **5G-Crosshaul** [1]. This 5G transport network aims to enable a flexible and software-defined reconfiguration of all networking elements in a multi-tenant and service-oriented unified management environment, through unified data and control planes interconnecting distributed 5G radio access and core network functions, hosted on in-network cloud infrastructure.

One of the most important and desired features of 5G-Crosshaul is *multi-tenancy*, that is, the ability to support multiple tenants while enabling flexible sharing of the 5G-Crosshaul physical infrastructure, so that each tenant can operate, independently, a subset of such resources. The aim of multi-tenancy is to maximize the degree of utilization of infrastructure deployments and to minimize the costs of rollout, operation, and management — reducing both the capital (CAPEX) and operational (OPEX) expenditures — and to reduce energy consumption, which are essential goals of 5G [2]. In our context, a tenant can be associated with an administrative entity or a user of a given service and implies a notion of ownership of one or more service instances and isolation between these instances.

Multi-tenancy is enabled by technologies such as network virtualization and network slicing, both covering the processes by which an infrastructure is physically or logically partitioned, segmented and assigned to different users. More formally, in line with related work (e.g., [3]), we define a *network slice* as *a self-contained, coherent set of functions along with the infrastructure required to support such functions, offering one or more services for end users*.

Although multi-tenancy is a concept that has been developed in many contexts, its applicability and benefits within transport networks has been addressed more recently. In the scope of the Fifth Generation Public Private Partnership (5GPPP), projects like 5G-NORMA and SESAME are addressing RAN multi-tenancy [4] while CHARISMA covers 5G access networks. The work in this article complements related work by focusing on the transport network aspects directly related to the combined fronthaul and backhaul, targeting per-tenant services that combine computing, storage, switching and transmission resource management. This article presents a novel architecture unifying the aspects of resource virtualization, virtual infrastructure, and network service management, combining the European Telecommunications Standards Institute (ETSI) network functions virtualization (NFV) management and

Xi Li, Xavier Costa-Pérez, and Andres Garcia-Saavedra are with NEC Laboratories Europe; Ramon Casellas and Ricard Vilalta are with CTTC/CERCA; Giada Landi is with Nextworks; Antonio de la Oliva is with Universidad Carlos III de Madrid; Thomas Deiß is with Nokia; Luca Cominardi is with Interdigital Europe.

Digital Object Identifier:
10.1109/MCOM.2017.1600921

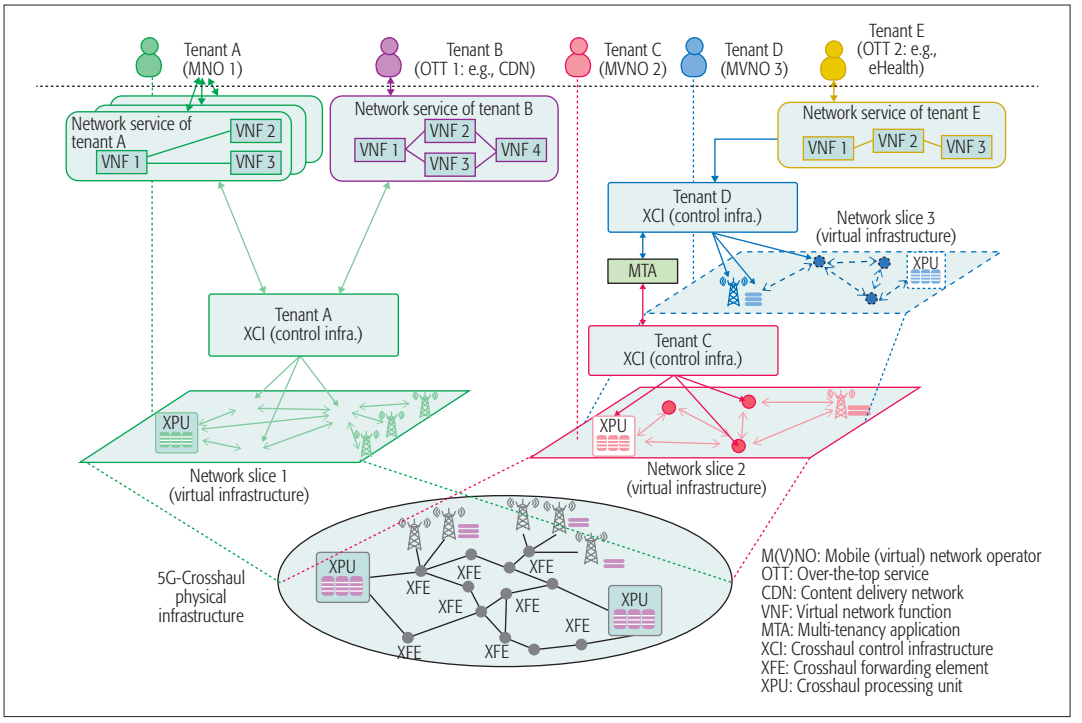


Figure 1. Network Slicing in 5G-Crosshaul for multi-tenancy support.

network orchestration (MANO) framework with integrated software defined networking (SDN)-based control. Note that the general concepts proposed in this article also can be applied to other segments of a mobile system (i.e., the core network and the RAN) to constitute an end-to-end (E2E) system. E2E network slicing relies on E2E orchestration (in some cases federation) between different network domains.

Our final target is to enable *slicing as a service* addressing the dynamic allocation of slices over a shared 5G-Crosshaul. The allocation of a slice involves the selection of the functions, their constrained placement, and the composition and configuration of the underlying infrastructures (either physical or virtual) fulfilling the services' requirements, in terms of latency, bandwidth, processing capacity, and so on. We consider two main network slicing services that enable different degrees of explicit control and are characterized by different levels of automation of network slice management:

- The provisioning of virtual infrastructures (VIs) under the control and operation of different tenants — in line with an infrastructure-as-a-service (IaaS) model
- The provisioning of a tenant's owned network services (NSs) as defined by the ETSI NFV architecture [5]

In the former, detailed later, a VI is defined as a logical construct composed of virtual links and nodes, which, as a whole, behaves as and can be operated as a physical infrastructure, enabling different degrees of internal control (i.e., can be operated by the tenant via different SDN control models). The service involves dynamic allocation of a VI, and its operation and deallocation. The actual realization of a VI combines many aspects like partitioning and bookkeeping of resources, and the instantiation of connections supporting virtual links. The provisioning of a VI commonly requires direct hardware element support or its emulation via software for multiplexing over the shared infrastructure.

In the latter, described later, an NS is instantiated directly over a shared infrastructure, and as a set of interrelated virtual network functions (VNFs). An NS corresponds to a set of endpoints connected through one or more VNF forwarding graphs (VNF-FGs). Note that whether the allocation of a NS is implemented in terms of the allocation of an underlying VI and the subsequent instantiation of the VNFs over the containing virtual machines (VMs) is an implementation choice.

Multi-tenancy is an orthogonal characteristic of both services, guaranteeing separation, isolation, and independence between different slices coupled with efficient sharing of the underlying resources. Consequently, 5G-Crosshaul defines the term *tenant* as a logical entity owning and operating either one or more VIs or one or more NSs, ultimately controlling their life cycle. The concept is illustrated in Fig. 1, where the owner of the physical infrastructure allocates VIs over its substrate network, providing multiple network slices to offer different tenants. Each tenant, such as a mobile (virtual) network operator (MNO or MVNO), owns and operates a network slice. In this example, tenants A, C, and D own network slices 1, 2, and 3, respectively. Moreover, tenant A itself can also allow sharing of its infrastructure by other tenants. The M(V)NO tenants can further deploy their own NSs or allow multiple third party tenants (e.g. over-the-top, OTT, service providers) to instantiate their NSs on top of the VI (e.g., tenant B deploying its NS over the VI of tenant A). It is possible to instantiate a VI on top of another one following a recursive approach (e.g., the VI of tenant D is instantiated over the one of tenant C.)

Although multi-tenancy is a concept that has been developed in many contexts, its applicability and benefits within transport networks has been addressed more recently. In the scope of 5GPPP, projects like 5G-NORMA or SESAME are addressing RAN multi-tenancy while CHARISMA covers 5G access networks.

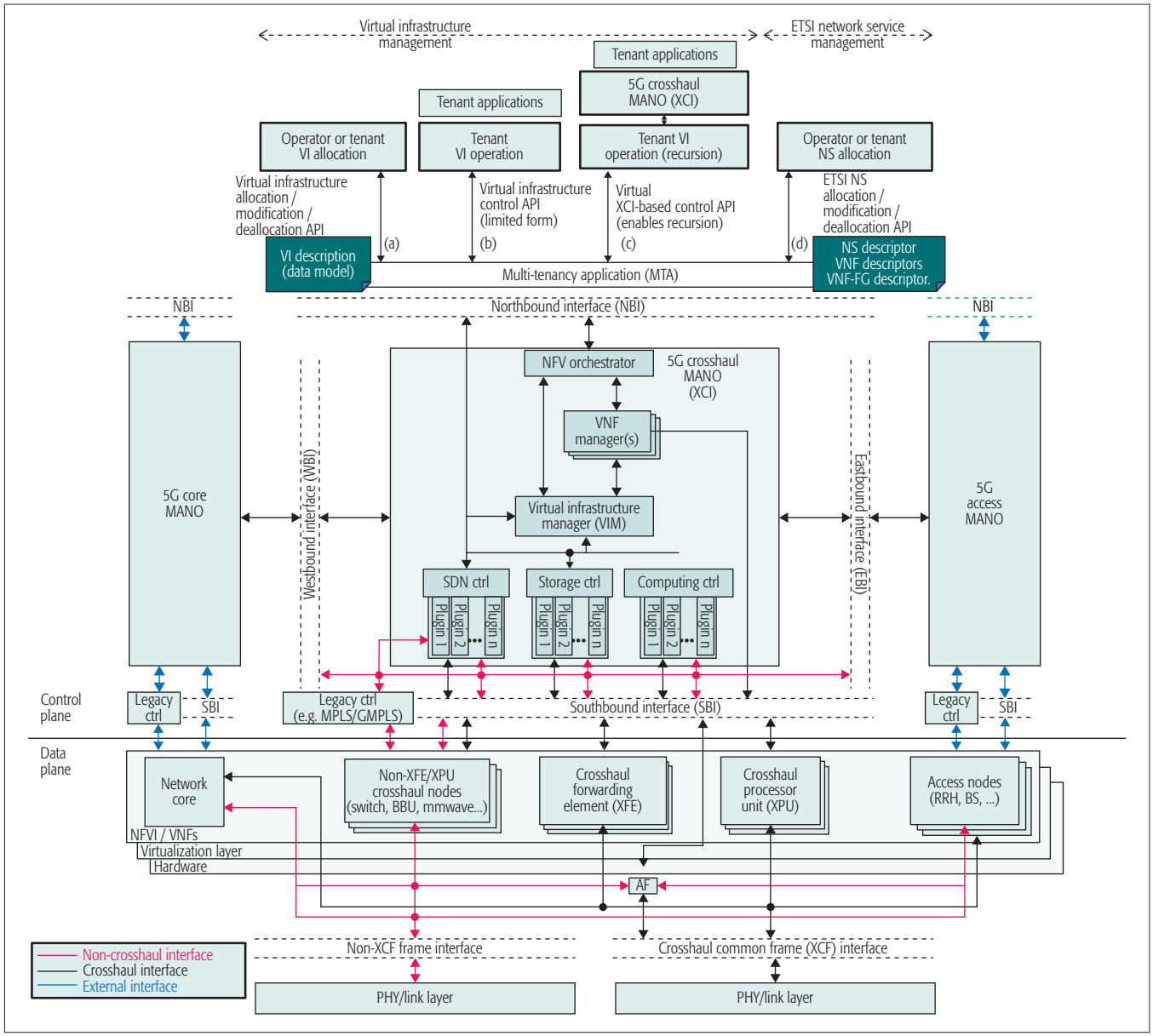


Figure 2. 5G-Crosshaul architecture for multi-tenancy.

From the point of view of business models, network slicing allows MNOs to open their physical transport network infrastructure to the concurrent deployment of multiple logical self-contained networks. The availability of this vertical market multiplies the monetization opportunities of the network infrastructure as:

- New players may come into play (e.g., automotive industry, e-health).
- Higher infrastructure capacity utilization can be achieved by exploiting multiplexing gains.

For the particular 5G-Crosshaul services, VI deployments are oriented to the business-to-business (B2B) market, targeting customers like MVNOs and cloud providers specializing in customizable IaaS services, since they need deep control of the network segment between distributed data centers. VIs also can be deployed by network operators to create virtualized and highly controlled environments to test and validate services before their rollout. Conversely, NSs target customers operating in the B2C segment, like application or service providers that offer services to end users (e.g., content providers specializing in streaming services).

5G-Crosshaul Architecture

The extended 5G-Crosshaul architecture based on the baseline design in [6], supporting several use cases of multi-tenancy, is depicted in Fig. 2. It follows the SDN principles:

- The data and control planes are fully decoupled.
- Control is logically centralized.
- Applications have an abstracted view of resources and states.

Our design approach leverages state-of-the-art SDN and NFV architectures to maximize the compatibility and integration of the system design with the existing standard frameworks and reference specifications, and to allow the reuse of open source projects to facilitate its deployability while minimizing the implementation costs. The extensions we proposed on top of the baseline archi-

tecture are the multi-tenancy application (MTA) and a set of application programming interfaces (APIs) to support the various multi-tenancy services, as shown in Fig. 2, for the control of a VI or NS lifetime, instantiation, modification, and deletion (API classes a and d in the figure), and for the control of the VI in its limited or full-featured form (API classes b and c, respectively).}

The **data plane** comprises Crosshaul forwarding elements (XFEs) and Crosshaul processing units (XPUs). XFEs are switching units, based on packet or circuit technologies, that interconnect a broad set of link and PHY technologies using a common framing (Crosshaul common frame, XCF) to transport both backhaul and fronthaul traffic. XPUs take care of most of the computational burden including BBUs or medium access control (MAC) processors, virtual network functions (VNFs), and other virtualized services. To this aim, the data plane makes use of an NFV infrastructure (NFVI) relying on generalized hardware components.

The **control plane** is divided into two layers: an application layer at the top and the 5G-Crosshaul control infrastructure (XCI) below. The XCI is our 5G transport MANO platform, compliant with the NFV MANO reference architecture, and provides an abstracted view of available resources, states, and control and management functions to an ecosystem of applications via a northbound interface (NBI). The XCI is connected to the data plane elements via southbound interfaces (SBIs) to execute control and management functions on the actual hardware components. The NFV orchestrator (NFVO) manages an NS life cycle. It coordinates the VNF's life cycle and the resources available at the NFVI in the data plane (supported by the virtual infrastructure manager, VIM) to ensure an optimized allocation of the necessary resources and connectivity to provide the requested virtual network functionality. The VNF managers (VNFMs) are responsible for the life cycle management of VNF instances. Finally, the VIM is responsible for controlling and managing the NFVI computing (via computing controllers), storage (via storage controllers), and network resources (via SDN controllers).

Although the scope of the XCI is limited to the transport network, it is essential to also consider the end-to-end coordination with other network segments (notably the 5G access and core segments). As shown in Fig. 2, our design includes westbound and eastbound Interfaces (WBI/EBI) to communicate with the 5G core MANO and the 5G access MANO. They can be used for functions like reachability dissemination or (abstracted) topology and provisioning information to help achieve system-wide optimization, enabling either a purely hierarchical architecture or a distributed/peer model for the orchestration of all involved segments. That said, the 5G access and core are out of the scope of 5G-Crosshaul. Work in complementary projects like 5G-Exchange can be leveraged for multi-domain orchestration and federation [7].

The MTA is the application that implements the support for multi-tenancy, by coordinating and managing tenants' access to the shared infrastructure, driving resource allocation for instances assigned to different tenants, and delivering multi-tenancy related services by means of dedicated APIs.[1] A high-level requirement is resource isolation, understood as the function of partitioning, separating and book-keeping of resources such that a tenant has no visibility of or access to the resources associated to another tenant. To perform this function, the MTA uniformly wraps and complements the infrastructure elements' (SDN controllers, cloud management systems, network elements, etc.) capabilities to provide multi-user and resource isolation support, offering uniform and abstracted views to tenants. Regarding mechanisms for isolation, our approach is to rely on existing ones, with the MTA acting as middleware and hypervisor. Full resource isolation requires system/infrastructure support, and it is not straightforward or may not even be achieved, for example, without hardware redundancy. 5G-Crosshaul provides soft resource isolation including, notably, driving the SDN controllers capabilities to create per-tenant networks, allocating software switches within XPUs dedicated to per-tenant traffic, defining security groups and per-tenant addressing, switching and routing within XPUs, and logically separating traffic within XPEs. Similarly, from the ETSI NFV/MANO perspective, the MTA manages state regarding allocation of NSs mapping tenants to actual instances and relying on implementations support.

5G-Crosshaul Virtual Infrastructure Services

The allocation of a VI can be triggered by a tenant (e.g., a VNO), either directly consuming the MTA API — Fig. 2, API a — or via the intervention of the infrastructure operator in a less dynamic environment, after an offline service level agreement (SLA). The VI concept is quite generic and can be extended to incorporate infrastructure elements beyond the ones considered herein. As part of the deployment of a VI, network, computing, and storage resources need to be partitioned and aggregated, eventually recursively if a hierarchy is enabled. This partitioning can be committed in full at the time of instantiation (hard allocation) or reflected in terms of predefined quotas that are enforced at the time of use (soft allocation).

It is noteworthy that VI allocation follows an IaaS model, so the actual use of the VI (including the functions and related business logic) is defined by the tenant. The infrastructure owner is agnostic to the VI end use. Once a given VI has been allocated, the 5G-Crosshaul MTA empowers the tenants with different degrees of control to be exerted over it, with different operational models of control and management. In simple terms, this ranges between either of the following:

- The control and management are restricted to the operational management and integration with the tenant operation support system (OSS)/base station support (BSS), and the operation of VI is mostly autonomous, with limited involvement of the tenant, such as monitoring and SLA validation.
- Each tenant is free to deploy their choice of the infrastructure operating system and control plane, allowing the optimization of the resource usage within each VI.

The infrastructure owner is agnostic to the VI end use. Once a given VI has been allocated, the 5G-Crosshaul MTA empowers the tenants with different degrees of control to be exerted over it, with different operational models of control and management.

[1] In the considered model, a single tenant entity owns one or more instances of each service in a 1:*N* relationship.

The tenant has access to application-level interfaces only and the NS provisioning API follows an "intent-based" modeling approach where the tenant asks just for the composition of some network functions, without caring about how they should be deployed and delivered.

The former model involves the MTA offering an API that enables the tenant to have a limited form of control over the (abstracted) elements that constitute the VI — Fig. 2, API b — including a set of operations and policies that can be applied (e.g., retrieve an aggregated view of the virtual infrastructure topology and resource state, and apply rules that affect element configuration and behavior). Low-level operations such as the actual configuration and monitoring of individual flows at the nodes may not be allowed. The latter implies per-tenant controller — Fig. 2, API c — or per-tenant MANO (XCI), including, most importantly, the ability to offer network services over its allocated virtual infrastructure. This approach ultimately enables recursion.

5G-Crosshaul ETSI/NFV Network Services

The allocation of an NS extends and complements the concept of VI deployment — Fig 2, API d — to deliver isolated chains of virtual services composed of specific VNFs in an automated manner. The tenant request usually specifies the type of VNFs (i.e., the desired virtual application components) in the NS Descriptor, their capabilities and dimensions through one or more VNF Descriptors, and how they must be interconnected through a VNF-FG Descriptor. Templates for the unified description of these information elements are currently under the standardization process in the ETSI NFV Interest Study Group (ISG) and OASIS TOSCA standards [8].

In the VI case, the tenant is responsible for the low-level deployment and configuration of its own applications over the allocated VI, while maintaining a certain level of control on the operation of the virtual resources. In the NS case, the tenant is interested in operating the applications that run in these virtual resources and expects that the needed level of resource capacity is seamlessly available in real time without any further configuration effort. The deployment and continuous management of the whole service is completely automated and totally delegated to the MTA and the NFVO within the XCI. The tenant has access to application-level interfaces only, and the NS provisioning API follows an intent-based modeling approach where the tenant asks just for the composition of some network functions, without caring about how they should be deployed and delivered.

In this scenario, the MTA is responsible for maintaining and coordinating the logical mapping between tenants, assigned services (in terms of NS and VNFs instances), and underlying virtual resources, in compliance with the SLAs established. Multi-tenancy is handled at different levels: at the lower level, a tenant has assigned physical and/or virtual resources in the domain of a VIM; at the upper levels, tenants have assigned VNFs and NSs. These different kinds of tenants can overlap and be merged in a single entity or be mapped over separate entities. For example, a VNO can further virtualize the rented VI to serve different kinds of business customers, like CDN providers, delivering dedicated VNFs and NSs. The management of these tenants' relationships, together with the correlated authorization and SLA validation and assurance procedures are under the responsibility of the MTA. Moreover, in these scenarios, NSs are not built directly on top of physical resources, but over VIs through the allocation of VNFs and VNF-FGs in VMs and virtual network nodes, following a recursive approach. This involves the operation of multiple MTA instances deployed at different levels and requires the mediation of XCI components deployed over the VI itself (further details are provided later).

At a lower level of service coordination, the NFVO in the XCI is responsible for the instantiation of the different NS components, based on the descriptors and metadata provided at the instantiation stage by the tenant. The NFVO, with the optional cooperation of the MTA, makes decisions about the most convenient usage of infrastructure resources, and allocates the required VMs and network connections accordingly. Moreover, during the NS life cycle, the NFVO is also responsible for the continuous monitoring of resource failures or infrastructure and application performance, coordinating the automated reactions for up/downscaling and self-healing procedures at the single VNF and global NS levels.

Requirements and Enabling Technologies for Multi-Tenancy

Multi-tenancy support requires a coordinated, holistic approach from the hardware to the XCI controllers up to the application layer, where the MTA acts as a global orchestrating entity. In this section we present the main requirements to support multi-tenancy at all these layers, analyzing the approaches that can be adopted to meet them.

Data Plane

When carrying the data of several tenants through the network, several requirements have to be considered:

- Traffic *separation*. One tenant should not be able to listen to the traffic of other tenants or of the network provider.
- Traffic *isolation*. The network has to provide guaranteed quality of service (QoS) to traffic of different tenants. Traffic of one tenant should not impact the QoS of the traffic of other tenants.
- Traffic *differentiation*. The traffic of different tenants may be forwarded differently, even when entering or exiting the network at the same points of attachment.
- *Statistical multiplexing*. Multiplexing gains should be possible among the traffic of different tenants.

The technical solution for traffic *separation and isolation* depends on the specific data plane technology adopted for the XFE, circuit or packet switched forwarding. For circuit switched forwarding, traffic separation, isolation, and differentiation can be achieved by creating different circuits per tenant. Although this is beneficial to achieve low and deterministic latency, for example, it does not provide *statistical multiplexing* gains among the traffic of different tenants, which are instead enabled with packet switching technologies.

For packet switched forwarding, the multi-ten-

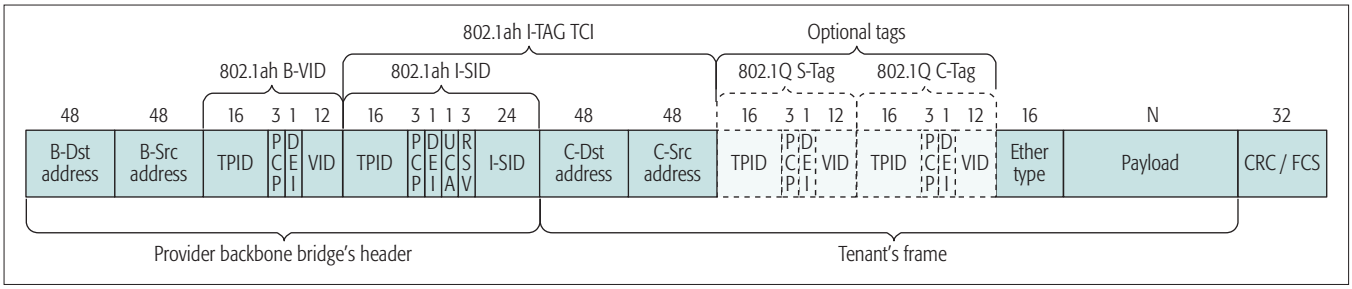


Figure 3. Provider backbone bridge — traffic engineering header.

ancy requirements are supported by using a common frame format across the network and different transmission technologies: the 5G-Crosshaul XCF. We propose provider backbone bridge — traffic engineering (PBB-TE) [9] as a common format to encapsulate the tenants' traffic, but other frame formats such as multiprotocol label switching — transport profile (MPLS-TP) can be used alternatively (for a comparison of PBB-TE and MPLS-TP see [10]).

In our solution, the fields in the PBB-TE header (Fig. 3) are used to achieve the multi-tenancy requirements as follows. Traffic *separation* is based on the backbone VLAN ID (B-VID) and the service ID (I-SID), used to identify the traffic for different tenants by using unique identifiers per tenant or even per service of the tenants. This allows the creation of different virtual networks and keeping the traffic separate at the XFEs. Independent forwarding decisions are also made at the level of these separate traffic flows, thus achieving traffic differentiation on a per-tenant basis. Traffic *isolation* regarding QoS is based on the three priority-code-point bits within the header, used to distinguish different types of service within the network and to schedule the packets for forwarding based on this priority information. At the ingress of the network, this priority has to be set appropriately and consistently across the different tenants to simplify the rules within the network.

Per-tenant XCF forwarding decisions are elaborated at the control plane and configured on the data plane following a forwarding abstraction model common to all the XFEs, either circuit- or packet-based. Such models are defined by the southbound protocols that define the interaction between the data and control planes. We propose the use of the OpenFlow protocol suite as the SBI for controlling the forwarding of XCF frames.

Control Plane

Support of multi-tenancy has a strong impact on the XCI components, from the network controller to the VIM and MANO components for the orchestration and delivery of VNFs and NSs.

At the SDN controller level, multi-tenancy requirements are related to the following aspects:

- *Delivery of per-tenant virtual network infrastructures*, providing the user with a uniform, abstract, and data-plane-independent view of its own logical elements, while hiding the visibility of other coexisting virtual networks
- Logical *partitioning of physical resources* to allocate logical and isolated network elements handling per-tenant traffic
- *Configuration of traffic forwarding* at the data plane level compliant with per-tenant traffic separation, isolation, and differentiation in the data plane

Tenant-based *virtual networks delivery* is handled through a dedicated SDN controller service. Its northbound APIs allow authorized tenants to request and operate their own network instances following abstract specifications (e.g., based on intent-based network models). Access to virtual resources is wrapped by the SDN controller and regulated at the northbound APIs based on tenants' profiles. *Physical resource partitioning* is managed within the SDN controller service through resource allocation algorithms combined with procedures to map logical network concepts with their corresponding entities or traffic configurations at the physical level. *Traffic separation* is achieved through the creation of tagged connections, exploiting the XCF multi-tenant features as explained earlier. Forwarding rules for the resulting traffic flows are then installed across the physical network following the paths computed by the resource allocation algorithms on a per-tenant basis (*traffic differentiation*), while QoS is handled through the creation of meters or queues (*traffic isolation*).

An example of SDN application for provisioning of multi-tenant virtual network infrastructures is the OpenDaylight Virtual Tenant Network (VTN) project [11]. The VTN application allows a tenant to request a virtual network. The mapping between network packets exchanged between OpenFlow switches at the data plane and instances of virtual networks defined at the logical level is based on ports and/or VLANs (Fig. 4). Each virtual network entity implements the typical functions of a corresponding physical element; for example, virtual routers provide routing, Address Resolution Protocol (ARP) learning, and Dynamic Host Configuration Protocol (DHCP) relay agent functions. Moreover, the tenant has the possibility to control the network behavior, defining a set of actions for flows matching layer 2–3 (L2–L3) filters.

At the VIM and VNF MANO level, beyond similar considerations of virtual resource allocation and isolation extended to computing elements, suitable modeling of the tenant and its capabilities needs to be supported. *Resource allocation* is handled through the creation of VMs and software switches assigned to specific tenants within the XPU, with isolation managed allocating specific addressing spaces and configuring proper routing rules and security groups. *Tenant profiles* are defined at the VIM and at the NFV orchestrator. At the VIM, each tenant has its own view of the VIM capacity, policies to regulate the access to the resources (e.g., a quota of dedicated resourc-

Our MTA approach is based on virtualization, and this usually involves refinements in the components architecture, enabling one-to-many and many-to-many relationships of software components and implementing the required mechanisms to guarantee security and isolation.

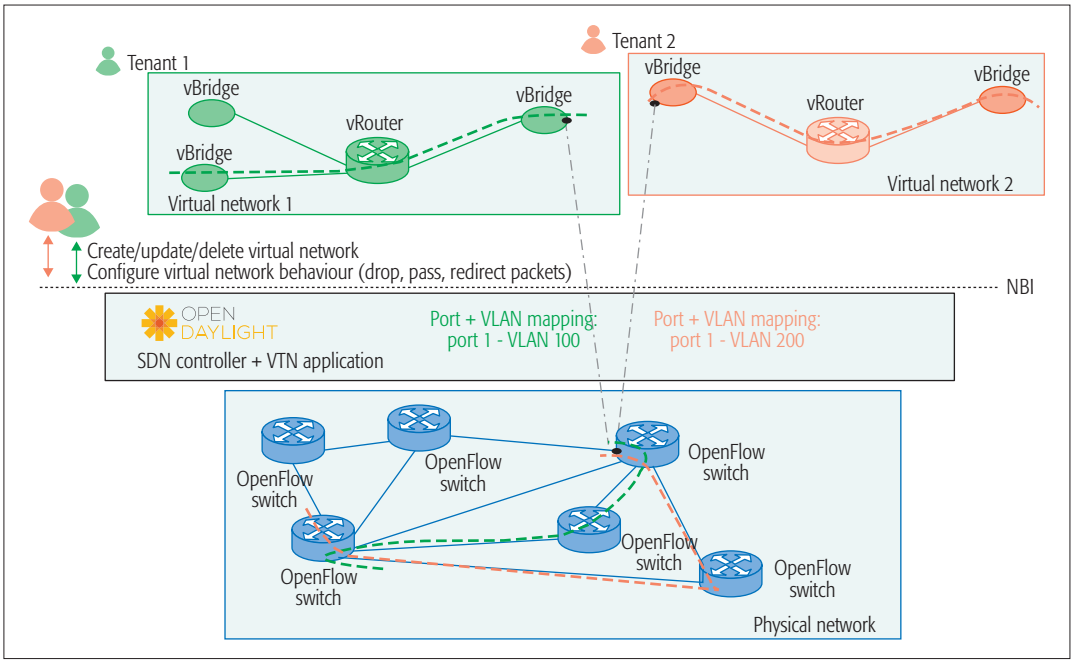


Figure 4. Virtual networks mapping in the OpenDaylight Virtual Tenant Network application.

es), and, optionally, custom resource flavors and VM images [12]. Requests for new VI must be authenticated and authorized, and they are evaluated based on the resources still available in the tenant's quota. Finally, access to the instantiated VI is strictly limited to the tenant owning the specific instance. Most cloud computing platforms (e.g., VMware, OpenStack) support multi-tenancy.

A similar approach, based on per-tenant profiles and policies, needs to be adopted at the NFV orchestration level, extending the virtual resources concept to VNF and NS entities. Each tenant must have a view and control of its own VNFs and NSs only; they must be maintained fully isolated from other entities belonging to different tenants, to guarantee their security and their desired key performance indicator (KPI) level independent of the load of other VNFs. New service requests must be granted depending on the tenant's profile, in combination with the tenant-related policies at the VIM level. Currently, this implies extending the functions of the NFVOs such as Open Source Mano and OpenBaton to manage tenant separation and mapping between tenants and NSs.

In general, our MTA approach is based on virtualization, and this usually involves refinements in the components architecture, enabling one-to-many and many-to-many relationships of software components and implementing the required mechanisms to guarantee security and isolation. From the point of view of performance, the overhead strongly depends on the underlying infrastructure and technology support (VLAN tagging, separate switching instances, compute resource quotas, etc.) and the need or not to emulate such features purely in software. In our considered use cases it is largely within acceptable operational ranges.

Application Plane

Coherent management of multi-tenancy is required horizontally for unifying the concepts of infrastructure virtualization and multi-tenancy in all involved segments and resources. The MTA at the application level provides such management, becoming the logical decision entity and serving as an optimizer to decide the allocation/modification/deallocation of network, compute, and storage resources. Essentially, the application decides an optimum subset of nodes (node mapping) and links (link mapping) in the substrate network to build a VI for a tenant that satisfies its resource demand and SLAs, by solving classical virtual network embedding (VNE) problems.

A VNE process consists of two coupled subproblems: node mapping and link mapping. The node mapping problem consists of reserving, for each virtual node, enough computational resources of a substrate node without exceeding capacity. Analogously, the link mapping phase consists of finding, for each pair of virtual nodes, a path (a collection of substrate links) to connect them. The selected paths must satisfy the networking requirements of each virtual link without exceeding network capacity on the physical links. The problem is recognized as NP-hard, and several approaches (e.g., [13]) have been proposed, which compromise optimality to find feasible solutions.

To deploy and enforce the computed mapping, the MTA needs to interact/coordinate with several functional entities inside the XCI — the SDN controller, the NFVO, and the VIM — either to collect information (GET command) or to provide commands (PUT command) (Fig. 5). The MTA covers both network- and computing- related functions. The actual workflows are strongly dependent on each use case. For the network-related services, the MTA first collects information on physical topology, traffic paths, and link load through the XCI, then computes the optimum allocation of networking resources and commands the XCI to perform the required configuration. This may involve direct requests to the SDN controller (to provision network paths and/or allocate virtual nodes providing the desired mapping between physical and virtual ports). For the computing-related services, the MTA may ask

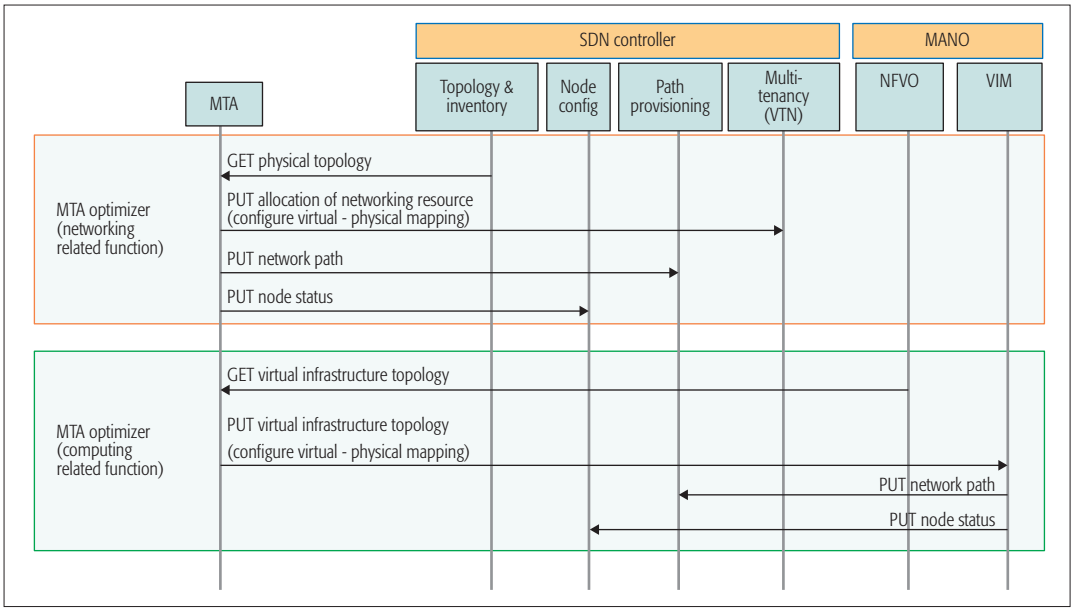


Figure 5. Workflow of the multi-tenancy application: interaction with the control plane.

The 5G-Crosshaul architecture has been designed to not only support sharing of the common transport infrastructure by multiple tenants, but also to allow each tenant to own and deploy its own MANO system. We refer to this case as multi-MANO, building a hierarchy of tenants operating on top of slices of VI.

the NFVO to provide a VI topology specifying where the VNFs must be placed or to directly instruct the VIM to enforce the mapping between virtual infrastructures and corresponding physical resource. The VIM itself will in turn request the SDN controller for the provisioning of required network paths and related node configurations.

Multi-Tenancy Recursion

The 5G-Crosshaul architecture has been designed to not only support sharing of the common transport infrastructure by multiple tenants, but also to allow each tenant to own and deploy its own MANO system. We refer to this case as *multi-MANO*, building a hierarchy of tenants operating on top of slices of VI. This concept requires support for XCI recursion to allow multiple instances of the 5G-Crosshaul MANO operating on top of the set of services provided by the XCI instance below. The 5G-Crosshaul architecture enables this functionality, on one hand, by providing support and bookkeeping of resources, maintaining a consolidated state of the virtual resources provided to each tenant, and, on the other hand, by providing a homogeneous API for controlling the underlying virtual resources which is transparent to the level of the hierarchy where the tenant is operating.

Figure 6 shows the recursive architecture. In the lower layer, the owner of the physical resources (MNO), instantiates its XCI. Different tenants request the provisioning of VIs to the MTA. By means of a template, blueprint, or SLA, each tenant specifies not only the slice characteristics (topology, QoS, etc.) but also some extended attributes such as the level of resiliency desired. The provider must take care of meeting the requirements and managing the available resources. Through the use of the MTA application, the resources at the MNO are hidden to the MVNOs, providing a layer of abstraction easing the management of each slice.

In a recursive and hierarchical manner, each tenant can operate its VI as the MNO operates on the physical one, allocating and reselling part of the resources to other MVNOs. Figure 6 shows this practice between Tenant#1 and Tenant#2. The infrastructure of MVNO#2 operates over the virtual network offered by MVNO#1, which operates on top of the MNO infrastructure (the physical one).

The multi-tenant architecture presented in this section is very challenging and one of the central points of innovation of the project. To devise a feasible and flexible framework, we have followed the recursion principles of the ONF architecture [14]. Although here we have presented mainly the control plane related issues, enabling multi-tenancy in such an architecture also requires modifications in the data plane. For example, isolation of resources/traffic is required, as described earlier. In addition, we have designed a specific OpenFlow-based pipeline to deal with the forwarding of traffic with different requirements and resources per tenant.

Summary and Conclusions

5G requires a new generation multi-tenant transport network integrating fronthaul and backhaul segments into a single transport infrastructure. In this article we have presented the 5G transport network architecture designed in the 5G-Crosshaul project that enables multi-tenancy through network slicing.

We have considered two main network slicing services that enable different control and automation levels of network slices management:

- Provisioning of virtual infrastructures under the control and operation of different tenants
- Provisioning of tenant-owned network services as defined by ETSI NFV

The former deals with the allocation and deallocation of VIs, logical entities encompassing a set of compute and storage resources interconnected by a virtual, logical network. In the latter, NSs are instantiated directly over a shared infrastructure, and as a set of interrelated virtual network Functions.

A multi-tenancy application (MTA) building on the network slicing services has been described that coordinates and manages the tenants' access to the shared infrastructure, performs resource isolation

To devise a feasible and flexible framework we have followed the recursion principles of the ONF architecture. Although here we presented mainly the control plane related issues, enabling multi-tenancy in such an architecture also requires modifications in the data plane.

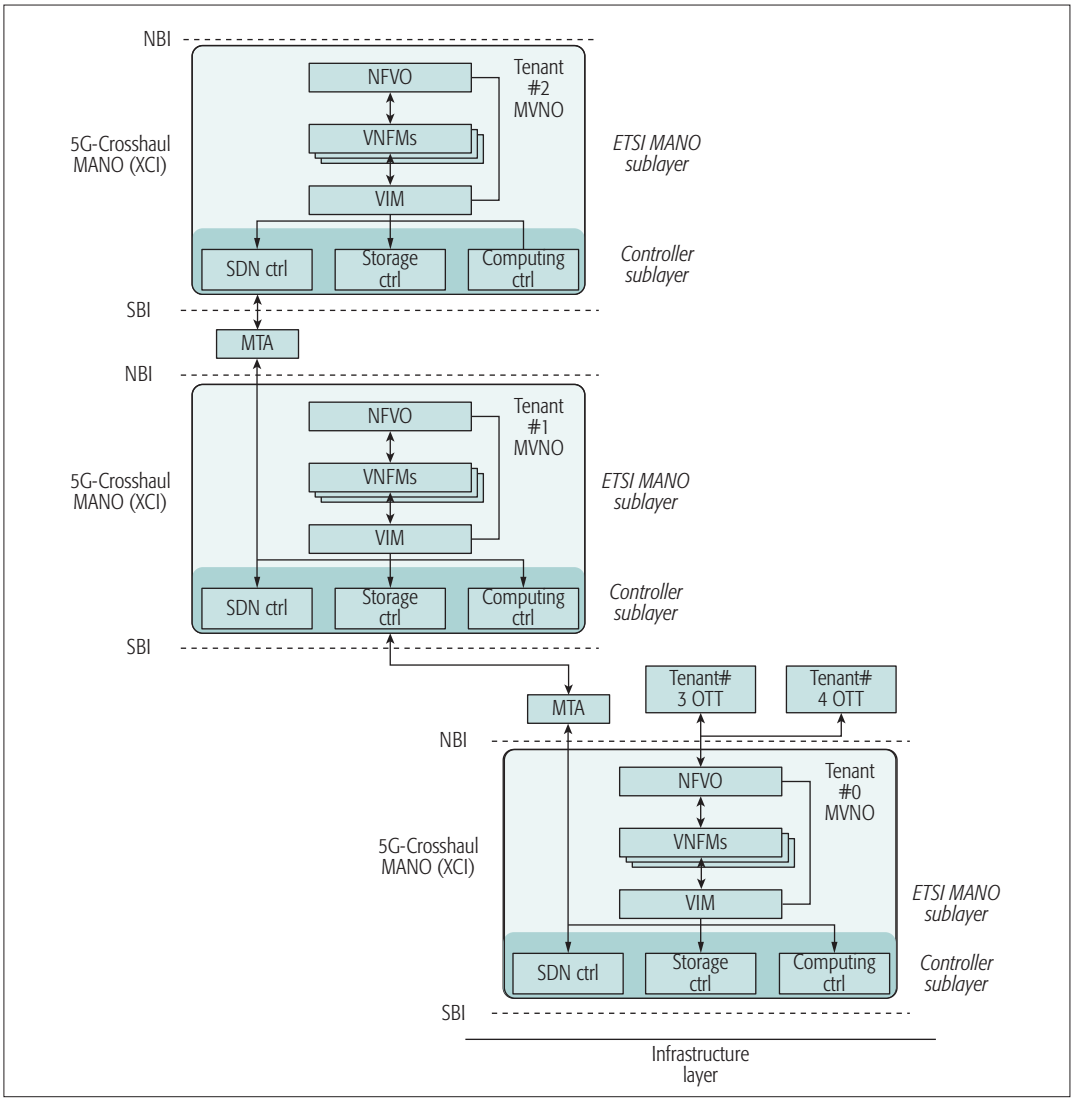


Figure 6. Crosshaul Control Infrastructure (XCI) Recursion: Multi-MANO.

between instances assigned, and delivers related services, such as the allocation and operation of VIs or NSs, by means of a set of proposed APIs.

Finally, the multi-tenancy recursion case (multi-MANO) has been considered, which requires support for multiple instances of the 5G-Crosshaul MANO simultaneously.

Acknowledgment

This work was partially funded by the European Commission through the EU H2020 5G-Crosshaul Project (grant no. 671598).

References

[1] S. Gonzlez *et al.*, "5G-Crosshaul: An SDN/NFV Control and Data Plane Architecture for the 5G Integrated Fronthaul/Backhaul," *Trans. Emerging Telecommun. Technologies*, vol. 27, no. 9, 2016, pp. 1196–1205.
[2] 5G PPP Architecture W G, "View on 5G Architecture," July 2016.
[3] NGMN, "5G White Paper and Description of Network Slicing Concept," 2015/2016.
[4] K. Samdanis, X. Costa-Pérez, and V. Sciancalepore, "From Network Sharing to Multi-Tenancy: The 5G Network Slice Broker," *IEEE Commun. Mag.*, vol. 54, no. 7, July 2016, pp. 32–39.
[5] ETSI, "Network Functions Virtualisation, Network Functions Virtualisation (NFV); Management and Orchestration," Dec. 2014.
[6] X. Costa-Pérez *et al.*, "5G-Crosshaul: An SDN/NFV Integrated Fronthaul/Backhaul Transport Network Architecture," *IEEE Wireless Commun.*, Feb. 2017.
[7] C. J. Bernardos *et al.*, "5GEx: Realising a Europe-Wide Multi-Domain Framework for Software-Defined Infrastructures," *Trans. Emerging Telecommun. Technologies*, vol. 27, no. 9, 2016, pp. 1271–80.
[8] OASIS, "TOSCA Simple Profile for Network Functions Virtualization (NFV)," v. 1.0, Mar. 2016.
[9] IEEE 802.1 Task Group, IEEE 802.1ah-2008, "IEEE Standard for Local and Metropolitan Area Networks — Virtual Bridged Local Area Networks Amendment 7: Provider Backbone Bridges."
[10] R. Vaishampayan *et al.*, "Application Driven Comparison of T-MPLS/MPLS-TP and PBB-TE — Driver Choices for Carrier Ethernet," *IEEE INFOCOM Wksps. 2009*, Apr. 2009.
[11] "OpenDaylight Virtual Tenant Network (VNT)," https://wiki.opendaylight.org/view/VTN:Main, accessed Feb. 10, 2017.
[12] R. Vilalta *et al.*, "Experimental Demonstration of Distributed Multi-Tenant Cloud/Fog and Heterogeneous SDN/NFV Orchestration for 5G Services," *Euro. Conf. Networks and Commun.*, 2016.
[13] L. Gong *et al.*, "Toward Profit-Seeking Virtual Network Embedding Algorithm via Global Resource Capacity," *Proc. IEEE INFOCOM*, Apr. 2014, pp. 1–9.
[14] ONF, "SDN Architecture, Issue 1.1," 2016.

Biographies

Xi Li received her M.Sc. in 2002 from TU Dresden and her Ph.D. in 2009 from the University of Bremen, Germany. From 2003 to 2014 she worked as a research fellow and lecturer in the Communication Networks Group at the University of Bremen,

leading several industrial and European research projects on mobile networks. In 2014 she worked as a solution designer at Telefonica, Germany. Since 2015 she has been with NEC Laboratories Europe, working as a senior researcher on 5G networks.

RAMON CASELLAS graduated in telecommunications in 1999 from UPC and ENST. He worked as an undergraduate researcher at France Telecom and BT Labs, completed a Ph.D. in 2002, and worked as an associate professor (ENST) until joining CTTC in 2006. He is a senior researcher, involved in research and technology transfer projects. His research interests include network control, GMPLS/PCE, and SDN/NFV. He has co-authored over 150 papers, 4 book chapters, and 4 IETF RFCs.

GIADA LANDI holds an Italian Laurea degree cum laude in telecommunication engineering from the University of Pisa. She holds 10+ years experience in telecommunication networks, with focus on control plane architectures and protocols. Currently, she is an R&D project manager at Nextworks. Her main research areas include SDN/NFV, cloud computing and orchestration, ASON/GMPLS, and PCE architectures. She has participated in industrial projects and consultancies on PCE, SDN, and NFV topics, and is active in European research projects.

ANTONIO DE LA OLIVA obtained his degree in telecommunication engineering from UC3M in December 2004 and his Ph.D. on telematics engineering in July 2008. He has served as Vice-Chair of the IEEE 802.21b task group and Technical Editor of IEEE 802.21d, and is now serving as Rapporteur of the ETSI WP on Crosshauling. He is currently working as Deputy Project Manager of the H2020 5GPPP 5G-Crosshaul project.

XAVIER COSTA-PÉREZ is head of 5G Networks R&D at NEC Laboratories Europe, where he manages several projects focused on 5G mobile core, backhaul/fronthaul, and access networks. He is a 5GPPP Technology Board member and Technical Manager of the 5G-Crosshaul project. His team contributes to projects for NEC products roadmap evolution, European Commission research collaborative projects, and related standardization bodies. He received his M.Sc. and Ph.D. in telecommunications from the Polytechnic University of Catalonia (UPC-BarcelonaTech).

ANDRES GARCIA-SAAVEDRA received his M.Sc. and Ph.D. from University Carlos III of Madrid in 2010 and 2013, respectively. He then joined the Hamilton Institute at Trinity College Dublin, Ireland, as a research fellow in 2014. Since July 2015 he has worked as a research scientist at NEC Laboratories Europe. His research interests lie in the application of fundamental mathematics to real-life computer communications systems and the design and prototyping of wireless communication systems and protocols.

THOMAS DEIß received his degree in computer science in 1990 and his Ph.D. in 1999 from the University of Kaiserslautern. He joined Nokia in 1999. He has contributed to standardization in the area of automated testing and worked in requirements engineering for backhaul functionality of WCDMA and LTE base stations with a focus on backhaul sharing among radio technologies.

LUCA COMINARDI received his B.Sc. and M.Sc. degrees in computer science from the University of Brescia, Italy. He also received an M.Sc. degree in telematics engineering from University Carlos III Madrid, where he is currently pursuing a Ph.D. in the same field. He has six years of experience in European research projects, such as FP7 FLAVIA, FP7 ICT iJOIN, and H2020 5G-Crosshaul, and he is now with InterDigital Europe as 5G Radio Access Network researcher.

RICARD VILALTA has a telecommunications engineering degree (2007) and a Ph.D. degree (2013), from UPC, Spain. Since 2010, he has been a researcher at CTTC in the Communication Networks Division. He is currently a research associate at the Open Networking Foundation. His research is focused on SDN/NFV, network virtualization, and network orchestration. He has been involved in international, EU, national, and industrial research projects, and published more than 100 journal and conference papers and invited talks.

Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges

Haijun Zhang, Na Liu, Xiaoli Chu, Keping Long, Abdol-Hamid Aghvami, and Victor C. M. Leung

The authors introduce a logical architecture for network-slicing-based 5G systems, and present a scheme for managing mobility between different access networks, as well as a joint power and subchannel allocation scheme in spectrum-sharing two-tier systems based on network slicing, where both the co-tier interference and cross-tier interference are taken into account.

ABSTRACT

5G networks are expected to be able to satisfy users' different QoS requirements. Network slicing is a promising technology for 5G networks to provide services tailored for users' specific QoS demands. Driven by the increased massive wireless data traffic from different application scenarios, efficient resource allocation schemes should be exploited to improve the flexibility of network resource allocation and capacity of 5G networks based on network slicing. Due to the diversity of 5G application scenarios, new mobility management schemes are greatly needed to guarantee seamless handover in network-slicing-based 5G systems. In this article, we introduce a logical architecture for network-slicing-based 5G systems, and present a scheme for managing mobility between different access networks, as well as a joint power and subchannel allocation scheme in spectrum-sharing two-tier systems based on network slicing, where both the co-tier interference and cross-tier interference are taken into account. Simulation results demonstrate that the proposed resource allocation scheme can flexibly allocate network resources between different slices in 5G systems. Finally, several open issues and challenges in network-slicing-based 5G networks are discussed, including network reconstruction, network slicing management, and cooperation with other 5G technologies.

INTRODUCTION

With the rapid development and innovations of mobile networking technologies, an entirely new era of mobile communications, the fifth generation (5G) of mobile communication systems, is coming. There is a consensus that 5G systems can be rolled out around 2020. 5G systems are expected to provide society with full connection, which can break through the limitations of time and space to create all-dimensional user-centered or service-centric interconnections between people and things [1].

5G networks aim to meet various user quality of service (QoS) requirements in different application scenarios (e.g., in terms of data transmission rate and latency) [2]. In scenarios where seamless wide-area coverage is needed, 5G systems should provide users with seamless high-data-rate services anytime and anywhere, even at cell edges or with high-speed (up to 500 km/h) mobility. In metropolitan areas where the density and volume of wireless traffic demand are both very high, 5G networks should provide dense hotspot coverage with high capacity. In scenarios where reliable connections of a large number of widespread low-power nodes (e.g., wireless sensors) are needed, 5G networks should be able to connect millions of devices under the constraints of low power consumption and low cost per device. Extremely low latency and high reliability of 5G networks are required to meet the performance requirements of real-time, reliable, and secure communications in some vertical industries such as interconnected vehicles and industrial production control.

Faced with the abundant, distinct, customized service requirements, and in the new application scenarios mentioned above, the network architecture and networking technologies need to be revisited for 5G systems [3]. This has become the focus of research and development activities of operators, equipment vendors, and research institutes all over the world. In order to provide customized reliable services using limited network resources while reducing capital expenditure and operating expense of 5G networks, network slicing has recently been proposed by the wireless industry as a main enabler of network service convergence and on-demand customized services [4–6]. By slicing a physical network into several logical networks, network slicing can support on-demand tailored services for distinct application scenarios while using the same physical network. Supported by network slicing, network resources can be dynamically and efficiently allocated to logical network slices according to the corresponding QoS demands.

Network slicing has also attracted a lot of research interest in academia. In [7] a user-centric service slicing strategy considering different QoS requirements was proposed based on software defined networking (SDN), and a genetic algorithm was devised to optimize the virtualized radio resource management based on resource pooling. In [8], a network slicing mechanism was introduced for network edge nodes to offer low-la-

Digital Object Identifier:
10.1109/MCOM.2017.1600940

Haijun Zhang and Keping Long are with the Beijing Engineering and Technology Research Center for Convergence Networks and Ubiquitous Services, University of Science and Technology Beijing; Victor C. M. Leung is with the University of British Columbia; Na Liu is with Beijing University of Chemical Technology; Xiaoli Chu is with the University of Sheffield; Abdol-Hamid Aghvami is with King's College London. Keping Long is the corresponding author.

0163-6804/17/$25.00 © 2017 IEEE

tency services to users, where the centralized core network (CN) entities and related applications are shifted to the network edge to reduce delays and burdens on the backhaul. The authors of [8] also proposed mobility management schemes and an optimal gateway selection algorithm to support seamless handover. A resource allocation scheme with consideration of interference management was presented in [9], where heterogeneous QoS requirements were guaranteed by optimizing power and subchannel allocation jointly. In [10], an agile and flexible SDN-based 5G network architecture was proposed to allocate physical network resources to virtual slices within a local area and to perform scheduling among slices. The SDN-based network architecture features a unified control plane, where hierarchical controllers are used to achieve differentiated services in user access layers close to the base stations, radio access network (RAN), and CN, respectively. The research on mobility management in network slicing systems has mainly been focused on an SDN-based control and handover procedure [10–12]. In the existing literature, mobility management and virtualized resource allocation have not been sufficiently studied for network-slicing-based 5G networks.

In this article, we present a logical architecture for network-slicing-based 5G systems, including an introduction to the fundamental concepts of network slicing. Based on the proposed network architecture, we investigate mobility management and virtualized radio resource allocation technologies in network-slicing-based 5G systems. Due to the diversity and complexity of 5G scenarios, it is vital to study proper mobility management for different mobility scenarios. Accordingly, we present a handover management scheme for handovers between different access networks. Virtualized resource management is responsible for inter-slice and intra-slice allocation of network resources in a dynamic and efficient manner. We propose a joint power and subchannel allocation scheme for network-slicing-based spectrum-sharing two-tier networks, where both the co-tier interference and cross-tier interference are taken into account. Simulation results show that the proposed resource allocation scheme can flexibly allocate network resources between different slices, thereby realizing efficient sharing of network resources in 5G systems. Finally, we highlight the future challenges and open issues on network slicing in 5G systems.

The remainder of this article is arranged as follows. The network-slicing-based 5G network architecture is given, and network slicing management is described in detail. Next, mobility management in 5G networks based on network slicing is briefly discussed. A joint power and subchannel allocation scheme in spectrum-sharing two-tier systems based on network slicing is formulated, and the simulation results are given. Several open issues and challenges in network-slicing-based 5G networks are discussed. Lastly, the article is summarized.

Network-Slicing-Based 5G System Architecture

The design of 5G network architectures should be based on comprehensive consideration of software control and hardware infrastructure and the interworking between them. Network slicing, which can fulfil diverse network requirements based on the unified physical infrastructure and sharing network resources, is considered as a key paradigm to provide several independently operating instances for a specific network function [5]. SDN has been widely accepted as a promising technique to implement network slicing on the basis of network functions virtualization (NFV) [10]. NFV replaces the traditional network elements, such as mobility management entity (MME), policy and charging rules function (PCRF), and packet/service gateway (P/S-GW), in the CN and RAN with commercial off-the-shelf servers, which also host the functions of dedicated physical infrastructures. Each such server can be considered as a pool of virtual machines (VMs) running on commercial off-the-shelf hardware and software. The traditional RAN is divided into centralized processing units, such as baseband units (BBUs) in cloud RAN (C-RAN)) and radio access units. The centralized processing units are largely virtualized, where resource pooling is introduced to perform service slicing in accordance with different QoS requirements [13].

The logical architecture of a 5G system based on network slicing is given in Fig. 1. In the radio access plane of the 5G system, a heterogeneous network accommodates multiple radio access technologies (RATs) and supports efficient cooperation between them. Small cells and WiFi access points are densely deployed to meet the increasing data traffic demand in 5G systems [14]. Furthermore, device-to-device (D2D) communications are used to increase system capacity and improve energy and spectrum efficiency while reducing communication delays and relieving the backhaul burden of macrocells [10]. D2D communications will play a critical role in network-slicing-based 5G systems, especially for improving quality of local services, emergency communications, and the Internet of Things (IoT).

As shown in Fig. 1, the traditional centralized architecture of the CN has evolved into a core cloud, which separates the control plane from the user plane so as to reduce control signaling and delays of data transmissions. The core cloud provides some important functions of the control plane, including mobility management, virtualized resource management, interference management, and so on. The servers and other functions of the RAN are located in the edge cloud, which is a centralized pool of virtualized functionalities. The edge cloud mainly performs data forwarding and control plane functions such as baseband processing. The user plane functions in the P/S-GW are also shifted to the edge cloud, to provide low-latency services and to reduce the burden on the backhaul. Mobile edge computing platforms are also deployed in the edge cloud, in conjunction with data forwarding and content storage servers, which can collaboratively execute the storage, computing, and transmission of massive data in a real-time and efficient way. The corresponding VMs will be distributed in the core cloud and edge cloud to execute virtualized network functions. By utilizing SDN, 5G networks can connect the VMs distributed in the core cloud and edge cloud, creating the mapping between them. Furthermore, the SDN controllers can control network slicing in a centralized fashion.

There is a consensus that 5G systems can be rolled out around 2020. 5G systems are expected to provide society with full connection, which can break through the limitations of time and space to create all-dimensional, user-centered, or service-centric interconnections between people and things.

By utilizing SDN, 5G networks can connect the VMs distributed in the core cloud and edge cloud, creating the mapping between them. Furthermore, the SDN controllers can control network slicing in a centralized fashion.

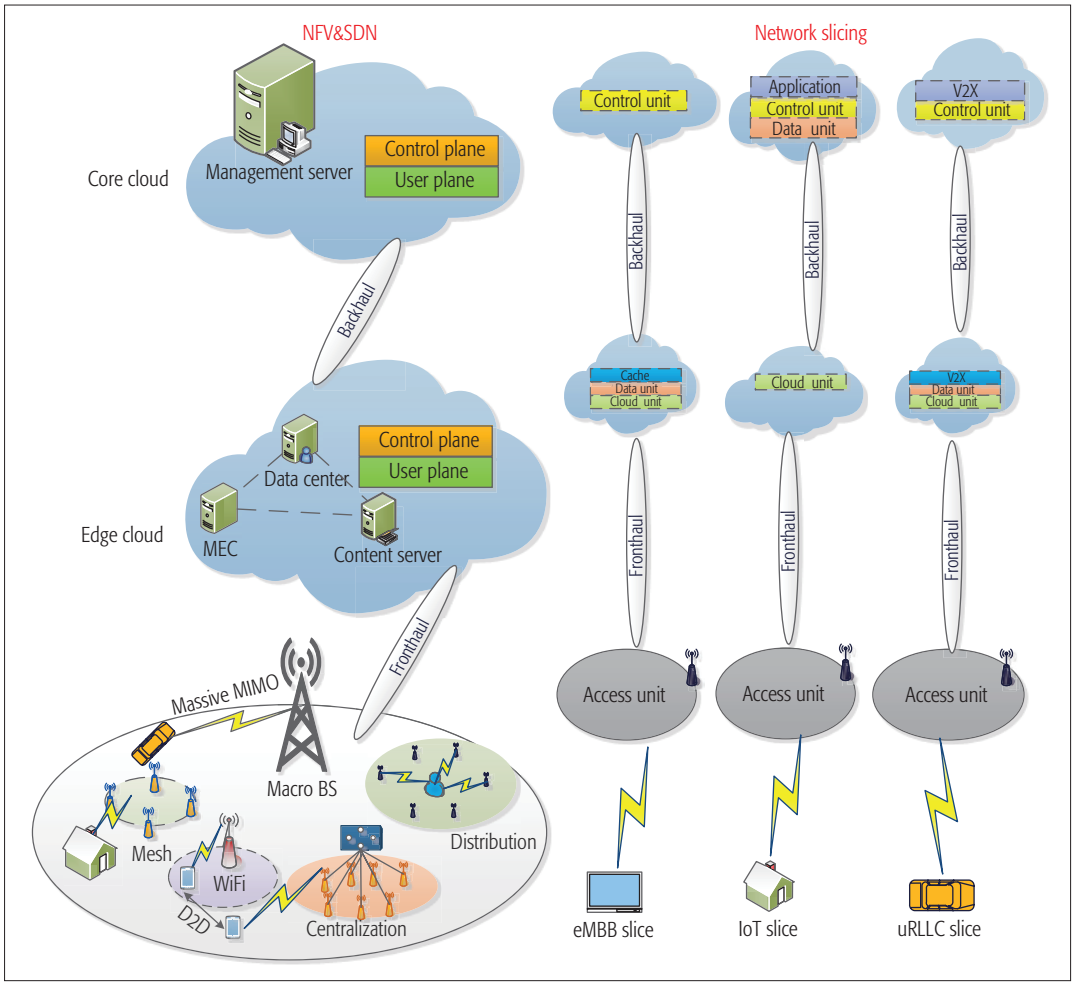


Figure 1. Network-slicing-based 5G system architecture.

After the virtualization and software redefinition of system architecture as described above, network slicing can be implemented. An example of network slicing operating on a set of generic physical infrastructures is illustrated in Fig. 2. An end-to-end network slice is a specific collection of network functions and resource allocation modules isolated from other network slices [5]. For example, the enhanced mobile broadband (eMBB) slice requires a large bandwidth to support high-data-rate services, such as high-definition video streaming and augmented reality. A caching function, data unit, and cloud unit are also needed to assist control functions in implementing eMMB slicing services. Reliability, low latency, and security will be critical for the ultra-reliable and low-latency communication (uRLLC) slice to provide services that are extremely sensitive to latency, such as autonomous driving and Internet of Vehicles (vehicle-to-everything, V2X). For uRLLC slice, all dedicated functions should be instantiated at the edge cloud. For the IoT slice, which serves a large number of static or dynamic machine type devices (e.g., sensors and monitors), the vertical applications will be placed on the upper layer to support the external services demanded by different commercial tenants.

In network slicing management, the control parts interact with each other through controllers or some kind of interfaces. The virtualized network function manager is responsible for the mapping of physical network functions to VMs. Coordinated with virtualized network function management (VNFM), the SDN controller operates and controls the entire virtual network by connecting the data layer and vertical applications through the interface protocols. Virtualized infrastructure management (VIM), as the center of the virtualized infrastructure, allocates virtualized resources to VMs by monitoring their resource utilization status. The network management and orchestration unit is the core part of slicing management, because it is responsible for creating, activating, and deleting network slices according to customized service requirements.

The network-slicing-based 5G network architecture will radically change the traditional network planning and deployment patterns. Network slicing is driven by and tailored for the network applications and user requirements. By avoiding mapping each application to a single pipeline in the physical network, 5G networks can provide end-to-end tailored services according to customized application requirements.

Mobility Management in Network-Slicing-Based 5G Systems

Mobility management in mobile communications has evolved from handling simple and single-RAT handover cases to managing complex, multi-RAT mobility scenarios. Based on SDN, the control

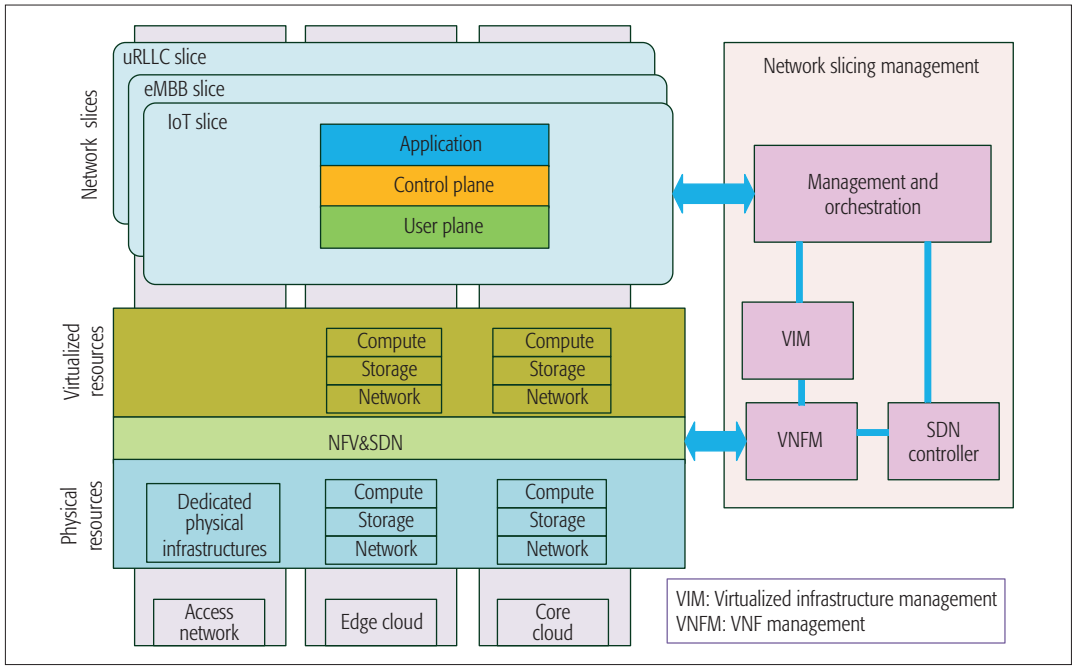


Figure 2. Network slicing management.

In conventional cellular networks, handovers are mainly event-triggered. The base station controls the user terminals to execute the measurement and report the measured network status information to serving base station. However, in our proposed network slicing based 5G systems, mobility related events need to be redefined.

plane and the user plane are split and decoupled at the gateway in the CN, and the integrated control functions can reduce control signaling even for a large number of distributed network nodes. However, network-slicing-based 5G systems will still face mobility management challenges caused by the potentially ultra high density of 5G networks combined with high mobility and high density of end devices. Consequently, new mobility management schemes need to be developed for network-slicing-based 5G systems to support seamless user experience with quality, continuity, and scalability [12].

Different network slices have different characteristics and requirements in terms of mobility, latency, and reliability. For instance, in railway communications, many handovers could be triggered by a high-speed train during a short time [11]; while in IoT applications, reliable and/or low-latency communications should be guaranteed for many devices with low or no mobility. In the following, we study the on-demand and scalable mobility management mechanism under network slicing for customized service scenarios.

There are two main procedures in mobility management: location registration and handover management.

Location Registration

Mobile devices register their locations when they first connect to the network, and then report their location information to the network periodically. In 5G networks, the home subscriber servers will be distributed into the edge cloud, making them closer to end devices to shorten registration delays and reduce backhaul burdens. 5G networks will aggregate multiple heterogeneous RATs. To achieve unified multi-RAT access and seamless mobility in 5G networks, multi-RAT coordination is needed for different RATs to share location information of their mobile devices.

Handover Management

In conventional cellular networks, handovers are mainly event-triggered. The base station controls the user terminals to execute the measurement and report the measured network status information to the serving base station. However, in our proposed network-slicing-based 5G systems, mobility related events need to be redefined. For instance, handovers may occur in different slicing scenarios. Flexible handover mechanisms and adaptive handover thresholds should be exploited to support mobility management in service-tailored scenarios.

In the proposed mobility management scheme for network-slicing-based 5G systems, the SDN is introduced into the RAN, generating the software-defined wireless network (SDWN). In SDWN, the single or hierarchical control plane is deployed close to the edge cloud to support centralized control plane handover decisions. One SDN controller can handle handovers in a single network slice. In a hierarchical control plane within SDN, it is necessary for controllers to cooperate [10]. A handover signaling procedure in network-slicing-based 5G systems is given in Fig. 3. The user supported by one of the slices is communicating with other terminals through the core cloud when the handover is triggered. After handover is executed successfully, the data will be transmitted through the target edge cloud and target access unit to the user from the core cloud. Due to virtualization, physical network elements are replaced by corresponding logical servers in the core cloud and edge cloud. Moreover, in order to simplify multi-RAT cooperation, only IP protocols are used to support signaling interactions in the control plane. Existing interfaces are made open so that a unified interface protocol can operate flexibly. The SDN controllers located in the core cloud, the edge cloud, and the access plane cooperatively carry out handover management in complex application scenarios.

Virtualized Resource Allocation with Interference Management

Network slicing facilitates dynamic and efficient allocation of network resources to meet diverse QoS requirements [5]. In SDN and NFV enabled network slicing systems, network resources are virtualized and managed in the centralized resource pools [7]. Due to limited network resources and increasingly diversified network services, it is challenging to efficiently provision network resources to network slices with different QoS requirements. Moreover, the heterogeneous nature of 5G networks (e.g., different RATs, different cell sizes) also adds complexities to resource allocation [9]. Especially for densely deployed spectrum-sharing small cells, efficient and flexible resource allocation schemes with interference awareness are needed [15].

In this section, we present a resource allocation scheme tailored for different QoS requirements of the uRLLC slice, IoT slice, and eMBB slice, which are the three fundamental categories

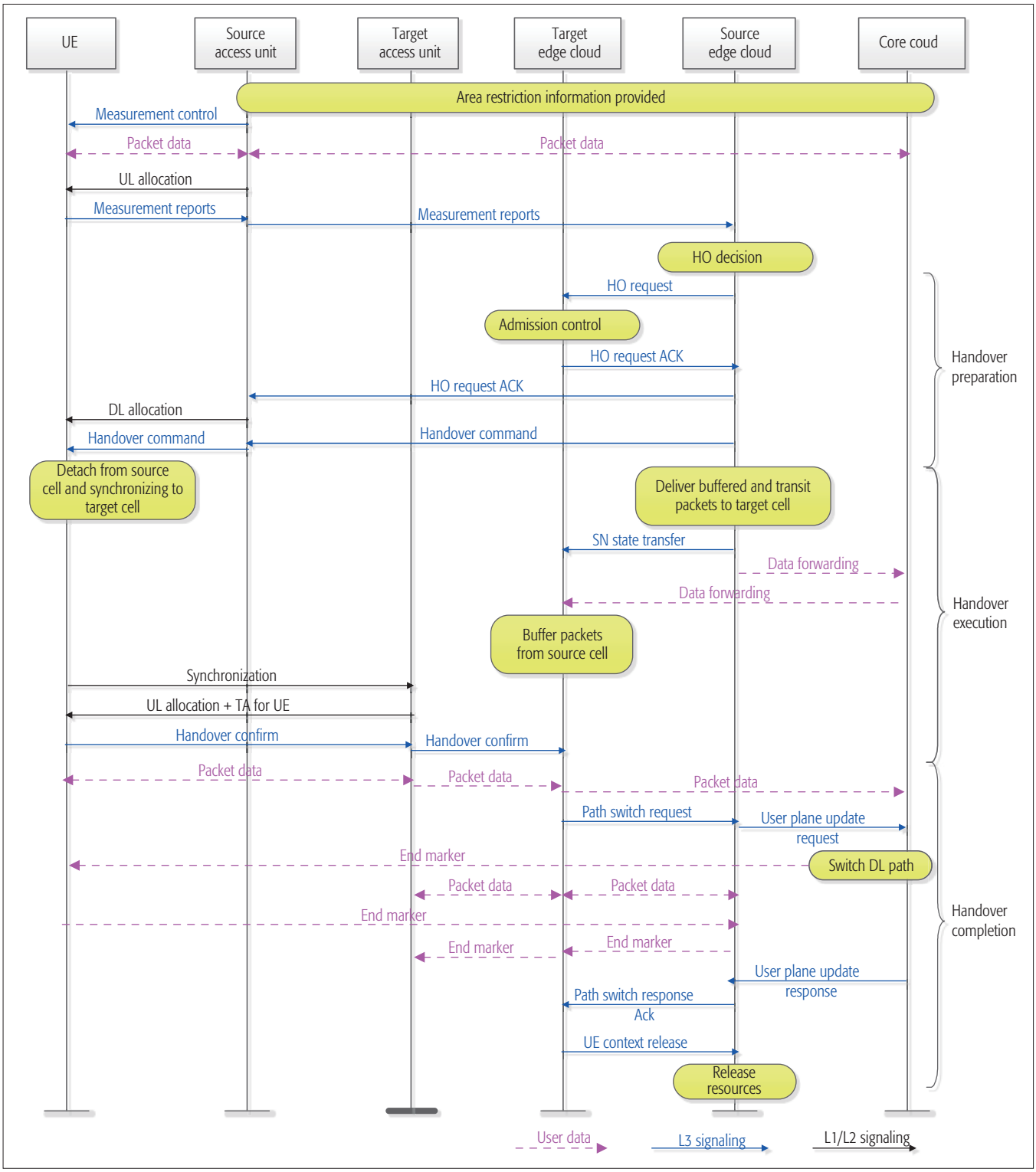


Figure 3. Handover procedure based on 5G network slicing systems.

of network slicing in 5G systems. For example, in uRLLC slicing scenarios, communication devices are more sensitive to time delay and require lower transmission rate than those in other slices. There could be mutual interference between small cells and macrocells, which provide services (e.g., video streaming) for the eMBB slice and IoT slice, respectively.

Modeling and Formulation

As shown in Fig. 1, the collocated small cells and macrocell compose a two-tier system in the radio access plane. Small cells receive two kinds of interference: cross-tier interference from the macrocell and co-tier interference from neighboring small cells. In this scenario, we model the uplink resource allocation problem as the maximization of uplink capacity on each subchannel for small cells considering the following constraints:

1. The maximum transmit power of each small cell user
2. The minimum data rate requirement of each uRLLC user
3. The threshold of total interference power received by the macrocell from small cell users
4. A subchannel that can be allocated to at most one user in each small cell during one transmission interval

Solution Based on the Lagrangian Dual Decomposition Method

The above formulation results in a non-convex discrete objective function. By relaxing the binary subchannel allocation indicators into continuous real variables, we transform it into a convex continuous function, which can be solved using the Lagrangian dual decomposition method. To simplify the solution, we decompose the objective function into a master problem and $K \times N$ sub-problems (for K small cells and N subchannels). The Karush-Kuhn-Tucker (KKT) conditions are used to get the optimal power allocation, and the sub-gradient method is exploited to update the Lagrangian multipliers to obtain the optimal subchannel allocation.

Simulation Results

We present simulation results to demonstrate the performance of a network-slicing-based 5G network (in conjunction with the proposed subchannel and power allocation scheme), where a suburban environment is considered with small cells randomly distributed in the macrocell coverage area. The macrocell coverage radius is 500 m and that of a small cell is 10 m. Other system parameters are set as follows: the carrier frequency is 2 GHz, the 10 MHz channel is divided into 50 subchannels, the minimum inter-small-cell distance is 20 m, the maximal transmission power (of small cell and macrocell users) is 23 dBm, the threshold of interference per subchannel (received by the macrocell) is –101.2 dBm, and the power spectral density of additive white Gaussian noise (AWGN) is –174 dBm/Hz. There are 50 users (requesting IoT services) distributed randomly in the macrocell, and 2 or 4 users (requesting uRLLC or eMBB services) camping on each small cell. The channel model includes path loss (indoor and outdoor) and frequency-selective fading. Round-robin scheduling is used in each cell, and uniform power allocation is adopted for macrocell users.

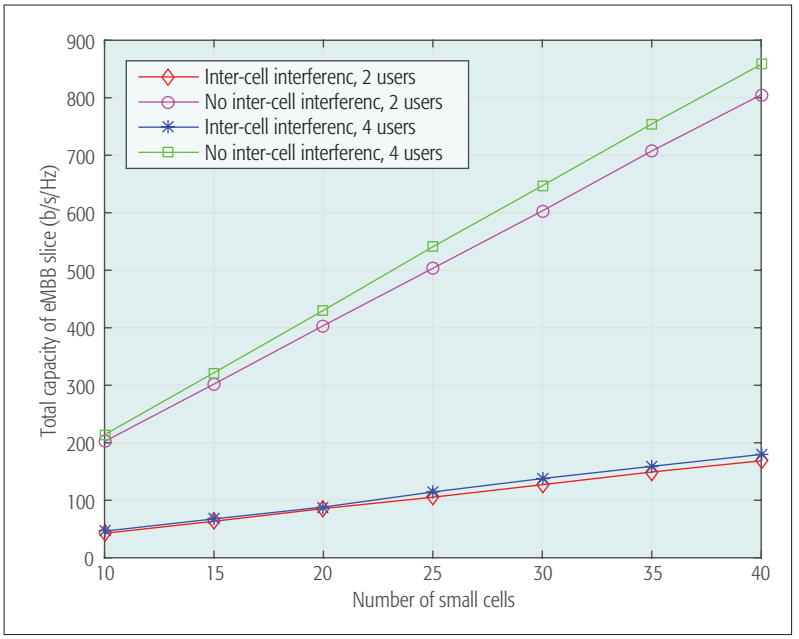


Figure 4. Total capacity of an eMBB slice vs. the number of small cells.

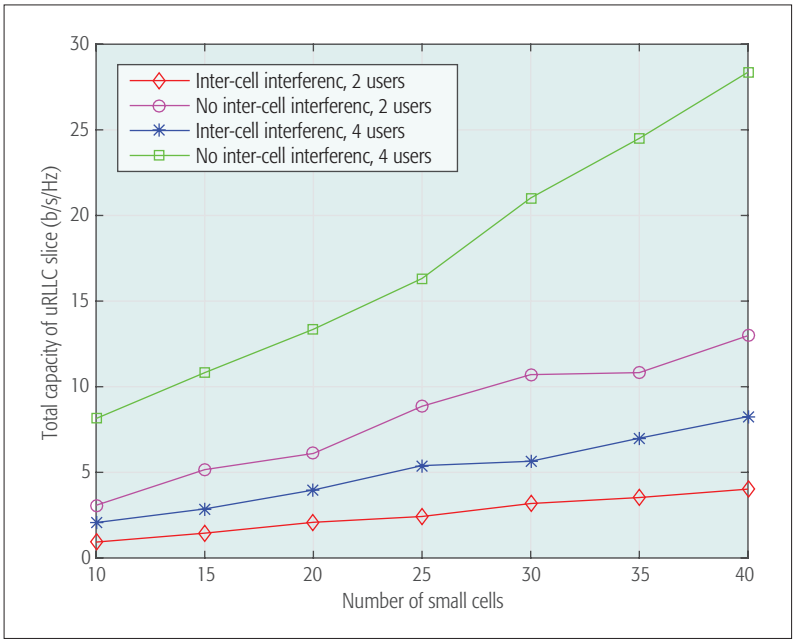


Figure 5. Total capacity of a uRLLC slice vs. the number of small cells.

Figure 4 shows the total capacity of the eMBB slice vs. the number of small cells per macrocell. We can see that the eMBB slice capacity rises nearly linearly with the density of small cells and increases slightly with the number of users per small cell. However, the eMBB slice capacity decreases significantly due to the inter-cell interference between small cells, especially at high small cell densities.

Figure 5 shows that the total capacity of the uRLLC slice also increases with the number of small cells, but the capacity of the uRLLC slice is 20 times less than that of the eMBB slice. This is because the eMBB slice uses large bandwidths to

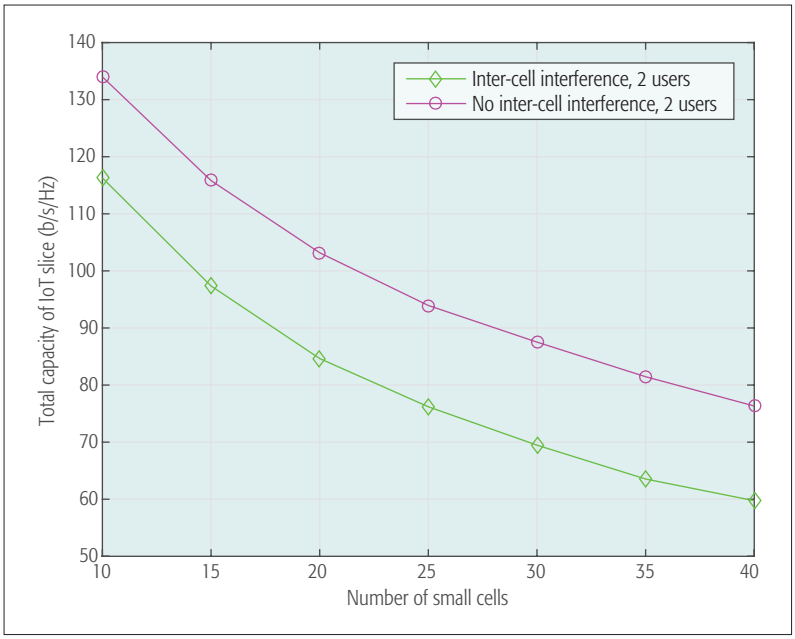


Figure 6. Total capacity of the IoT slice vs. the number of small cells.

transmit massive data, while the uRLLC slice only transmits low-volume control messages or data under low-latency constraints.

Figure 6 shows the total capacity of the IoT slice supported by the macrocell, which suffers from cross-tier interference from small cells supporting the eMBB and uRLLC slices. The total capacity of the IoT slice decreases with the number of small cells due to the increasing cross-tier interference. The capacity of the IoT slice will further decrease due to co-tier interference between macrocells and between small cells. This is because with channel quality affected by increased inter-small-cell interference, small cell users will adaptively increase their transmit power, leading to an increase of cross-tier interference from small cells.

The simulation results have shown that in both latency-sensitive and latency-tolerant network slicing scenarios, the proposed resource allocation scheme can allocate network resources properly and efficiently, and can improve system capacity of dense heterogeneous networks. Due to space limitations, we will discuss other metrics (e.g., latency) in future works.

Challenges and Open Issues

Network slicing is a promising paradigm in future 5G mobile networks, but realizing it is not without challenges [13]. In the following, we discuss major challenges and open issues on network slicing in terms of network reconstruction, slicing management, and cooperation with other 5G technologies.

Network Reconstruction

Since 5G networks provide wireless connection for everything, both the RAN and CN need reconstruction to support end-to-end network slicing. Especially in dense heterogeneous networks, not only should the cooperation of macrocells and small cells be designed to meet the customized slicing demands, but also the cooperation of multiple RATs should be considered to provide seamless mobility and high transmission throughput.

Network Slicing Management

Network slicing supports customized configuration of resources, management models, and system parameters for various use cases in an isolated or abstract way [5]. Although service providers and mobile operators have started developing industrial solutions for network slicing, the management of network slicing is still a hard nut to crack. There are many dimensions and technologies included in network slicing: to create, activate, maintain, and deactivate network slicing at the service level; to adjust load balance, charging policies, security, and QoS at the network level; to abstract and isolate virtualized network resources; and inter-slice and intra-slice resource sharing. Moreover, the complexity and difficulty of network slicing management may increase with the continued boom of applications and services.

Cooperation with Other 5G Technologies

In future 5G systems, network slicing needs to coexist and cooperate with traditional technologies, such as broadband transmission, mobile cloud engineering (MCE), SDN, and NFV, evolved from LTE/LTE-A systems. The virtualized cloud of access networks and CN have the advantages of physical resource pooling, distribution of software architectures, and centralization of management. However, there is still no proper approach to integrate network slicing with C-RAN, SDN, and NFV to provide point-to-point connection between physical radio equipment and radio equipment controller. Cooperation between network slicing and other 5G technologies is necessary to enable more network slices in future 5G networks.

Conclusion

In this article, we have presented a logical architecture for network-slicing-based 5G systems, and discussed the evolution of network architecture based on SDN and NFV technologies, as well as the implementation of network slicing. Based on the network slicing architecture, we have revised handover procedures in mobility management, and discussed mobility management mechanisms to offer flexible and agile customized services in network-slicing-based 5G systems. Moreover, considering various network slicing scenarios, we have introduced a resource allocation mechanism tailored for QoS requirements and interference constraints of uRLLC, eMBB, and IoT service slices. The promising performance of network-slicing-based 5G networks has been demonstrated through computer simulations.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant 61471025), the Young Elite Scientist Sponsorship Program by CAST (2016QNRC001), and the Fundamental Research Funds for the Central Universities.

References

[1] H. Zhang *et al.*, "Fronthauling for 5G LTE-U Ultra Dense Cloud Small Cell Networks," *IEEE Wireless Commun.*, vol. 23, no. 6, Dec. 2016, pp. 48–53.
[2] A. Osseiran *et al.*, "Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project," *IEEE Commun. Mag.*, vol. 52, no. 5, May 2014, pp. 26–35.
[3] C. L. I *et al.*,"New Paradigm of 5G Wireless Internet," *IEEE JSAC*, vol. 34, no. 3, Mar. 2016, pp. 474–82.

[4] P. Rost *et al.*, "Mobile Network Architecture Evolution toward 5G," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 84–91.
[5] M. Jiang, M. Condoluci, and T. Mahmoodi, "Network Slicing Management & Prioritization in 5G Mobile Systems," *Euro. Wireless 2016*, Oulu, Finland, 2016, pp. 1–6.
[6] Ericsson, "Ericsson White Paper: 5G System," Jan. 2015.
[7] X. Xu *et al.*, "SDN Based Next Generation Mobile Network with Service Slicing and Trials," *China Commun.*, vol. 11, no. 2, Feb. 2014, pp. 65–77.
[8] J. Heinonen *et al.*, "Mobility Management Enhancements for 5G Low Latency Services," *2016 IEEE ICC Wksps.*, Kuala Lumpur, Malaysia, 2016, pp. 68–73.
[9] H. Zhang *et al.*, "Resource Allocation in Spectrum-Sharing OFDMA Femtocells with Heterogeneous Services," *IEEE Trans. Commun.*, vol. 62, no. 7, July 2014, pp. 2366–77.
[10] V. Yazici, U. C. Kozat, and M. O. Sunay, "A New Control Plane for 5G Network Architecture with a Case Study on Unified Handoff, Mobility, and Routing Management," *IEEE Commun. Mag.*, vol. 52, no. 11, Nov. 2014, pp. 76–85.
[11] H. Song, X. Fang, and L. Yan, "Handover Scheme for 5G C/U Plane Split Heterogeneous Network in High-Speed Railway," *IEEE Trans. Vehic. Tech.*, vol. 63, no. 9, Nov. 2014, pp. 4633–46.
[12] S. Kuklinski, Y. Li, and K. T. Dinh, "Handover Management in SDN-Based Mobile Networks," *2014 IEEE GLOBECOM Wksps.*, Austin, TX, 2014, pp. 194–200.
[13] M. Peng *et al.*, "Fronthaul-Constrained Cloud Radio Access Networks: Insights and Challenges," *IEEE Wireless Commun.*, vol. 22, no. 2, Apr. 2015, pp. 152–60.
[14] H. Zhang *et al.*, "Coexistence of Wi-Fi and Heterogeneous Small Cell Networks Sharing Unlicensed Spectrum," *IEEE Commun. Mag.*, vol. 53, no. 3, Mar. 2015, pp. 158–64.
[15] H. Zhang *et al.*, "Cooperative Interference Mitigation and Handover Management for Heterogeneous Cloud Small Cell Networks," *IEEE Wireless Commun.*, vol. 22, no. 3, June 2015, pp. 92–99.

Biographies

Haijun Zhang [M'13, SM'17] (haijunzhang@ieee.org) is currently a full professor at the University of Science and Technology Beijing, China. He was a postdoctoral research fellow in the Department of Electrical and Computer Engineering, University of British Columbia (UBC), Vancouver, Canada. He received his Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT). From 2011 to 2012, he visited the Centre for Telecommunications Research, King's College London, United Kingdom, as a visiting research associate. He has published more than 90 papers and authored 2 books. He serves as an Editor of *IEEE 5G Tech Focus*, the *Journal of Network and Computer Applications*, *Wireless Networks*, *Telecommunication Systems*, and *KSII Transactions on Internet and Information Systems*, and serves/has served as a leading Guest Editor for *IEEE Communications Magazine*, *IEEE Transactions on Emerging Topics in Computing*, and *ACM/Springer MONET*. He serves/has served as General Co-Chair of GameNets '16 and 5GWN '17, Symposium Chair of GameNets '14, Track Chair of ScalCom '15, and Co-Chair of the Workshop on 5G Ultra Dense Networks at IEEE ICC 2017 and GLOBECOM 2017. He received the IEEE ComSoc Young Author Best Paper Award in 2017.

Na Liu (eeliuna@gmail.com) received her B.S. degree in electronic information engineering from Beijing University of Chemical Technology, China, in 2016. She is currently pursuing an M.S. degree at the Laboratory of Wireless Communications and Networks from the College of Information Science and Technology, Beijing University of Chemical Technology. Her research interests include resource allocation, power control, energy efficiency in wireless communications, software-defined wireless networks, and visible light communications.

Xiaoli Chu (x.chu@sheffield.ac.uk) is a senior lecturer in the Department of Electronic and Electrical Engineering at the University of Sheffield, United Kingdom. She received her B.Eng. degree from Xi'an Jiao Tong University in 2001 and her Ph.D. degree from the Hong Kong University of Science and Technology in 2005. From 2005 to 2012, she was with the Centre for Telecommunications Research at King's College London. She has published over 100 peer-reviewed journal and conference papers. She is the lead editor/author of the book *Heterogeneous Cellular Networks — Theory, Simulation and Deployment*, Cambridge University Press, May 2013. She is an Editor for *IEEE Wireless Communications Letters* and *IEEE Communications Letters*. She was Co-Chair of the Wireless Communications Symposium at the IEEE ICC 2015, and Workshop Co-Chair for the IEEE International Conference on Green Computing and Communications 2013.

Keping Long [SM] (longkeping@ustb.edu.cn) received his M.S. and Ph.D. degrees at UESTC in 1995 and 1998, respectively. He worked as an associate professor at BUPT. From July 2001 to November 2002, he was a research fellow in the ARC Special Research Centre for Ultra Broadband Information Networks (CUBIN) at the University of Melbourne, Australia. He is now a professor and dean at the School of Computer and Communication Engineering (CCE), Inverstiy of Science and Technology Beging. He is a member of the Editorial Committee of Sciences in China Series Fand China Communications . He has also been a TPC and ISC member for COIN, IEEE IWCN, ICON, and APOC, and Organizing Co-Chair of of IWCMC '06, TPC Chair of COIN '05/'08, and TPC Co-Chair of COIN '08/'10, He was award-ed the National Science Fund Award for Distinguished Young Scholars of China in 2007 and selected as the Chang Jiang Scholars Program Professor of China in 2008. His research interests are optical Internet technology, new generation network technology, wireless information networks, value-added service, and secure network technology. He has published over 200 papers, 20 keynotes, and invited talks.

Hamid Aghvami [F] (hamid.aghvami@kcl.ac.uk) joined the academic staff at King's College London in 1984. In 1989 he was promoted to reader, and in 1993 was promoted to professor in telecommunications engineering. He is/was the founder/director of the Centre for Telecommunications Research at King's. He has published over 580 technical journal and conference papers, and filed over 30 patents. He was an executive advisor/chairman/managing director of many wireless communications companies. He was a member of the Board of Governors of the IEEE Communications Society in 2001–2003, was a Distinguished Lecturer of the IEEE Communications Society in 2004–2007, and has been a member, Chairman, and Vice-Chairman of the Technical Program and Organizing Committees of a large number of international conferences. He is also founder of the International Symposium on Personal Indoor and Mobile Radio Communications, a major yearly conference attracting some 1000 attendees. He was awarded the IEEE Technical Committee on Personal Communications Recognition Award in 2005. He is a Fellow of the Royal Academy of Engineering and the IET, and in 2009 was awarded a Fellowship of the Wireless World Research Forum.

Victor C. M. Leung [S'75, M'89, SM'97, F'03] (vleung@ece.ubc.ca) is a professor of electrical and computer engineering and holder of the TELUS Mobility Research Chair at UBC. His research is in the areas of wireless networks and mobile systems. He has co-authored more than 900 technical papers in archival journals and refereed conference proceedings, several of which have won best paper awards. He is a Fellow of the Royal Society of Canada, a Fellow of the Canadian Academy of Engineering, and a Fellow of the Engineering Institute of Canada. He is serving on the Editorial Boards of *IEEE JSAC-SGCN*, *IEEE Wireless Communications Letters*, *IEEE Access*, and several other journals. He has provided leadership to the Technical Program Committees and Organizing Committees of numerous international conferences. He was the recipient of the 1977 APEBC Gold Medal, NSERC Postgraduate Scholarships from 1977–1981, a 2012 UBC Killam Research Prize, and an IEEE Vancouver Section Centennial Award.

There is still no proper approach to integrate network slicing with C-RAN, SDN and NFV to provide point-to-point connection between physical radio equipment and radio equipment controller. Cooperation between network slicing and other 5G technologies is necessary to enable more network slices in future 5G networks.

Network Slices toward 5G Communications: Slicing the LTE Network

Kostas Katsalis, Navid Nikaein, Eryk Schiller, Adlen Ksentini, and Torsten Braun

The authors describe the network slicing concept by unveiling a novel network slicing architecture for integrated 5G communications. They demonstrate its realization, for the case of evolved LTE, using state-of-the-art technologies. They elaborate on the LTE-specific requirements toward 5G, and point out existing challenges and open issues.

ABSTRACT

The upcoming 5G ecosystem is envisioned to build business-driven network slices to accommodate the different needs of divergent service types, applications, and services in support of vertical industries. In this article, we describe the network slicing concept by unveiling a novel network slicing architecture for integrated 5G communications. Further, we demonstrate its realization for the case of evolved LTE using state-of-the-art technologies. Finally, we elaborate on the LTE-specific requirements toward 5G, and point out existing challenges and open issues.

INTRODUCTION

Due to the recent mobile traffic explosion, mobile network operators (MNOs) have been severely challenged to provide the needed capacity increase. However, there is growing consensus that traditional network capacity increase methods, like vertical and horizontal scaling, cannot cope with this demand, since they create excessive operating and capital expenditures. Furthermore, the upcoming 5G ecosystem will involve a number of vertical markets, such as automotive, smart grid, and the Internet of Things (IoT), and will support a number of use cases, with extreme diversity in the required service offerings. The concept of network slicing through efficient resource and services sharing is increasingly gaining momentum as a promising solution that is able to meet both challenges. It relies on cloud-based approaches for flexible sharing of resources including antenna, bandwidth, spectrum, processing power, storage, and networking, while enabling novel business opportunities for over the top (OTT) service providers and vertical industries. Note that the concept of network slices is not new and recently has been refined by the Next Generation Mobile Networks Alliance (NGMN) [1], adopted and adapted by the main telecom manufacturers. In principle, a network slice can be defined as a composition of adequately configured network functions, network applications, and underlying cloud infrastructures, which are bundled together to meet the requirement of a specific use case or business model on a per tenant basis [1, 2].

In this article, we devise a novel network slicing architecture for 5G systems. Our contributions are three-fold. First, a three-layer technology-agnostic architecture is described, where we introduce a novel network slice service layer (SL) that is responsible for the whole life cycle management of the network slice. Second, the idea of a Network and Application Store (NAS) is introduced to facilitate the complex procedure of defining the network slice. Third, a realization of the concept of network slicing using the LTE network is described to show the feasibility of the proposed architecture by exploiting the current technological landscape. Indeed, LTE is expected to serve as the cornerstone of wireless access technologies for a rich set of use cases toward 5G communications. Particularly, we describe how to actually slice the LTE network and the relevant supporting technologies, methods, and techniques. The proposed architecture is generic and can be used to support both LTE and evolved LTE, as well as the heterogeneous 5G radio access network (RAN). In our approach we exploit cloud technologies, software-defined networking (SDN) [3], and network functions virtualization (NFV) [4] as a means to provide the necessary tools to break down the vertical system organization, while tailoring network slices to particular use cases.

This article is organized as follows. We present the concept as well as the related work. Then we describe a novel network slicing architecture. This is used as a reference for the realization of the approach and the creation of network slices in LTE networks.

CONCEPT, DEFINITIONS, AND RELATED WORK

According to NGMN, a 5G network slice supports the communication service of a particular connection type with a specific way of handling the control and data (user) plane for this service. It is composed of a collection of network functions and specific radio access technology (RAT) settings, which are combined together for the specific use case or business model [1]. Work on network slicing concepts is delivered in the context of the Fifth Generation Public Private Partnership (5G-PPP) Architecture Working Group activities, while also delivered in various EU projects. In the METIS II project, the network slicing requirements are described [5], resulting in the definition of the main categories of slices. These are related to three generic services: extreme mobile broadband (xMBB), ultra-reliable low latency communication (uRLLC), and massive machine type communication (mMTC), while the RAN is one of the main enablers. In the 5G-NORMA project, SDN and NFV tech-

Digital Object Identifier:
10.1109/MCOM.2017.1600936

Kostas Katsalis, Navid Nikaein, and Adlen Ksentini are with EURECOM; Eryk Schiller and Torsten Braun are with Universitat Bern

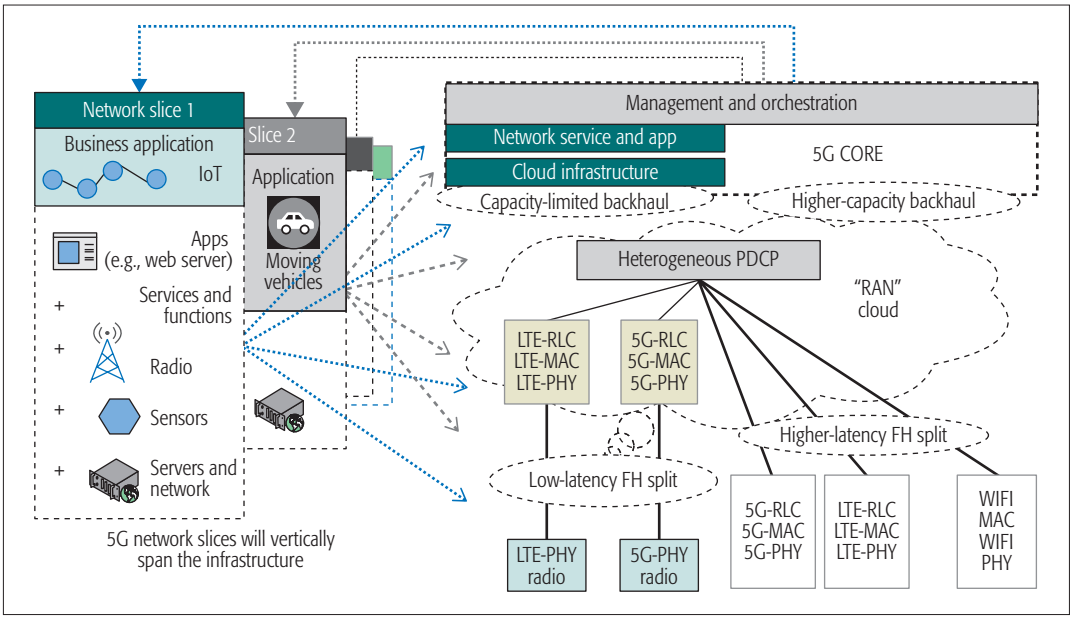


Figure 1. Network slicing at the 5G RAN. A 5G network slice is a bundle of network services, functions, network applications, resources, and accoutrements.

As the concept of Network Slicing is in an initial state, the proposed architecture can serve as a reference point and alleviate a number of important design issues related to the Network slicing lifecycle and management. The innovation of the approach lies on the design and operation of the SL and the interaction with the NAS and IL.

nologies are exploited to enable dynamic sharing of network resources among operators [6]. From the industry perspective, a similar description is provided by Ericsson (5G Systems, white paper, 2015). The International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) is also in the field; the ITU FG Group IMT-2020 analyzes how emerging 5G technologies will interact in future networks and also focus on the topics of network slicing orchestration and management. Clearly, from all the existing definitions and approaches, the foundation of 5G network slices is built around virtualization technologies, multi-tenancy and multi-service support, integrated network programmability, and the adoption of the SDN/NFV design paradigms [6].

Network Slices in the Heterogeneous RAN

The wireless domain of the envisioned 5G systems will be heterogeneous and composed by a number of technologies, mainly the evolved LTE, the New Radio access technology (e.g., millimeter-wave), and new generation Wi-Fi (e.g., 802.11ax). For the LTE domain, the Third Generation Partnership Project (3GPP) has agreed on a detailed work plan for Release 15, the first release of 5G specifications. These are described in the 3GPP Technical Specifications Group (TSG) 72 activities. In the envisioned 5G environment, network slices are expected to vertically span the infrastructure environment and actually utilize any available type of physical or virtual resource of the 5G heterogeneous RAN, as shown in Fig. 1. In order to provide vertical network slices the necessary control and management procedures must run in a technology agnostic way of the actual access network implementation. To enable network slicing in the future mobile network generation, 3GPP SA and 3GPP RAN groups are building technical specifications to integrate network slicing in the upcoming specifications. More specifically, the 3GPP SA group is discussing a solution to enforce network slicing using the eDECOR concept (3GPP, TR 23.711, Release 14). This is a solution recently specified to implement the principle of a dedicated core network (DCN). The RAN sharing concept is studied by the 3GPP RAN groups and is already utilized by mobile virtual network operators (MVNOs). The aim of these activities is to combine the concept of RAN sharing and the eDECOR to create an end-to-end network slice.

Network-Slicing-Enabled 5G Architecture

In this section, we present the main design elements of a proposed network slicing architecture, which is illustrated in Fig. 2. Our proposal stands for a three-layer design that includes: a Business Layer (BL), the Network Slice Layer (SL), and an Infrastructure Layer (IL), together with the operation of the NAS. Note that an initial design of the architecture was proposed in [7]. However, in this article we extend the analysis of the SL operations, while we elaborate in detail on the complex procedures to define and deploy a network slice description. We highlight that despite the multitude of proposed architectures toward 5G communications ([8, 5, 9]), there is no single design available for a unified framework that supports the network slicing concept and at the same time is able to:

- Efficiently capture the need for integrated network programmability and SDN control
- Support service orchestration and NFV techniques in multi-domain RAN
- Provision for concepts like the cloud-RAN and mobile edge computing (MEC).

As the concept of network slicing is in an initial state, the proposed architecture can serve as a reference point and alleviate a number of important design issues related to the network slicing life cycle and management. The innovation of the approach lies on the design and operation of the

The complex procedure of the NSD/NSM creation is made in a slice manifest factory. Note that due to a high degree of multi-tenancy, a negotiation component is also required. While a logical definition of services and networks is initially provided by the verticals from the BL to the SL, a negotiation procedure will actually provide the final delimited NSD.

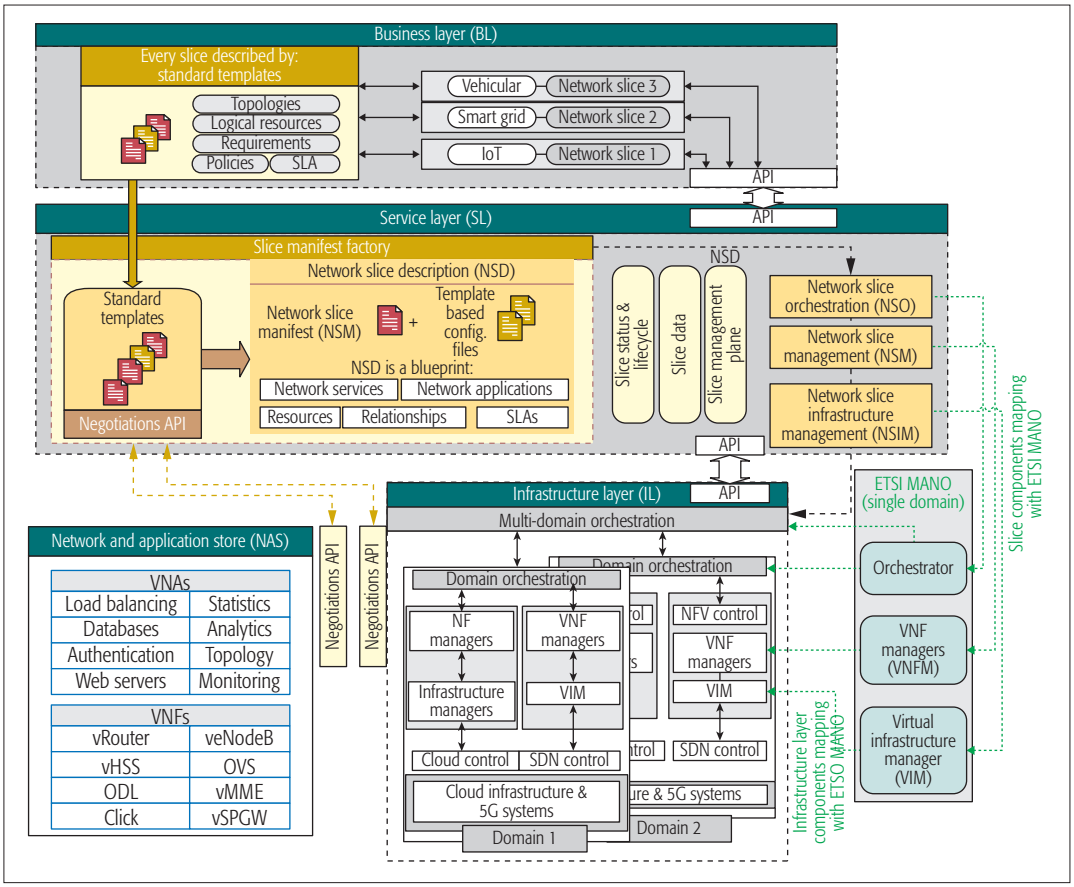


Figure 2. Network Slicing Architecture towards 5G communications.

SL and the interaction with the NAS and IL. In the following we analyze the different components of the proposed architecture.

Business Layer

5G networks must cope with a wide range of use cases and must be able to satisfy strict performance requirements. These use cases span from public safety, high mobility, and business-critical applications, to IoT and high-speed broadband vehicular access, covering three categories as defined in the METIS II project (i.e., xMBB, uRLLC, and mMTC). The slice owner on top of the business layer creates the desired use case (e.g., IoT) and is the one that actually triggers the building of the network slice. Such a use case can be based on standard reference network slice templates that describe the existing business application.

Network Slice Service Layer

This layer supports all the functions used for the life cycle management of each network slice, related to the deployment, instantiation, management, control, scaling and termination of the network slices. It is also the layer where the transformation of network slice templates to an operational bundle of resources and services is made, tailored to a particular use case. The bundle is described by an end-to-end Network Slice Description (NSD) that also provides details on the data models and interfaces across the network functions and applications.

Network Slice Description: An NSD is used to describe the slice by means of resources, services, relationships, and service functions chains. Due to the high complexity of the required components, the NSD is a network slice manifest file (NSM) with metadata for a group of accompanying files that describe a coherent network slice. The accompanying files are based on templates that define all the details required by the SL. That is, a service template is particular for a specific service and needs to define the input parameters, configuration primitives, the relationships/dependencies, resources and constraints, units (number of instances), as well as machines (physical or virtual) and domains of operation. The NSD also includes the necessary configuration primitives for slice instantiation and operation. The complex procedure of the NSD/NSM creation is made in a slice manifest factory (Fig 2, SL center). Note that due to a high degree of multi-tenancy, a negotiation component is also required. While a logical definition of services and networks is initially provided by the verticals from the BL to the SL, a negotiation procedure will actually provide the final delimited NSD:

- Negotiation between the SL and IL: The SL needs to exploit the best/maximum infrastructure offering.
- Negotiation between the SL and NAS: Exploit the best templates that can be reused for network functions and network applications.

After the negotiations, the final NSD and NSM are created and then passed to a network slice service orchestrator (NSO) entity in order to provision and deploy service bundles and actually drive the orchestration procedures.

SL Internals: Our design is based on the European Telecommunications Standards Institute (ETSI) NFV management and orchestration (MANO) concepts delivered by the ETSI NFV Industry Specification Group (ISG) [10], while we consider that in this layer the relevant software components operate on a slice basis rather than a domain basis. In this layer, all the slice-related functionalities are performed including the slice life cycle management and upgrade procedures. More specifically, in the SL the network services operate under the control of a Network Slice Service Manager (NSM) and a dedicated NSO. The NSO orchestrator entity is responsible for the composition and on-demand allocation and creation of all the physical network functions (PNF) and virtual network functions (VNFs) requested for the virtual slice, combined with their interconnectivity and support services. The orchestrator entity operates on top of a distributed NSM, which is responsible for the life cycle management of the entire network slice. The NSO, in turn, interacts with a Network Slice Infrastructure Manager (NSIM), which handles the allocation of virtual resources (computing, storage, network), through interaction with the infrastructure layer. The interaction with the IL is made through communication between the NSIM operating in the SL and a hierarchical multi-domain orchestrator in the IL. Note that currently there is no single definition of multi-domain orchestration, and indeed multi-domain orchestration is an open issue according to the work delivered in ETSI. Depending on the context, it can be administration-based, technology-based, area-based, or operator-based. Our design is generic enough to include all these cases. The SL design also considers additional services, like slice data management and additional supported services required for the slice operation and maintenance.

Network and Application Store

Supporting complex use cases on per network slice basis requires the coupling of a rich set of VNFs and virtual network applications (VNAs). A marketplace of VNFs and VNAs can be thought of as the network counterpart of mobile application stores, like the Google Play Store for Android applications. Essentially, with the NAS, one can deliver customized network function and service templates tailored to particular use cases. For example, an LTE network slice can result from several templates, which dynamically install and configure all the LTE network-specific elements for both the packet core and the access network. We consider that an NAS must be able to support multiple stores that will, however, be exposed to the SL using a common application programming interface (API). The main idea is that in order to create a vertical network slice, we can easily discover and consume: a set of VNFs like virtual routers, switches, or firewall services; and VNAs like Hadoop clusters, web servers, or databases. A distinction between VNAs and VNFs must be made, as their execution environment and SDK are potentially different, while the SL needs to be aware of them during the negotiation. Note that according to the definitions provided by ETSI mobile edge computing (MEC), mobile edge (ME) applications are running as virtual machines (VMs) on top of virtualized infrastructures and can interact with the ME platform to consume and provide ME services. According to the terminology used in the ETSI MEC Working Group, an ME application can be either a VNF or a VNA.

Infrastructure Layer

This layer shall support a real-time reconfigurable cloud ecosystem and virtualization for fast and ultra-fast services. In addition, it supports connectivity as a service and delivers the resulted bundle of network services. In more detail, the IL includes the bare metal physical infrastructure and the virtualization layer, which is responsible for physical resource abstraction. The relevant design elements include programmable computing, network and storage hardware, programmable RF hardware and software, and any type of programmable network. It also includes the cloud and network (SDN-based) control systems. The SDN network control is about establishing communication between PNFs, VNFs, and VNAs on demand. Furthermore, efficient SDN control methodologies are used to promote network agility and facilitate the service level agreement (SLA)-based network configuration. Finally, we consider operation over multi-cloud providers, where both physical and virtual infrastructures are available like Amazon, mobility as a service (MaaS), and local environments. A multi-domain orchestrator is running on top of all the PNF/VNF managers and cloud/SDN controllers, managing the end-to-end operations in the IL.

From Virtual Slices to Real Deployment: Slicing in LTE Evolution

In this section, we describe a realization of the proposed architecture in the case of LTE networks. Note that the proposed architecture is technology-agnostic and can be realized with other wireless technologies as well, such as 5G New Radio or new generation Wi-Fi. We elaborate on the way to create LTE network slices using the open source OpenAirInterface (OAI) software platform, supported by the OpenAirInterface software Alliance. OAI offers a software implementation of the whole LTE protocol stack and can operate over commodity hardware for the deployment of the eNodeB and the core network (CN).

Although the network slicing concept seems to be a natural evolution of virtualization, even for some simple use cases its realization can be extremely complex. In addition, in LTE the control procedures are inherently complicated for both the control and data planes and are related to IL. For ease of understanding we describe a simple example with the interactions between the layers.

Example of a LTE Network Slice with Enhanced Mobile Broadband Support and QoS

We consider a simple modeling approach with the following three phases: planning, provisioning, and operation:

Planning Phase: A request for an LTE network slice with eMBB support and quality of service (QoS) guarantees is made from the BL to the SL using a logical, technology-agnostic NSD. The

Although the Network Slicing concept seems to be a natural evolution of virtualization, even for some simple use cases, its realization can be extremely complex. In addition the LTE the control procedures are inherently complicated for both the control and data plane and these are related to IL.

Layer	Technology drivers
SL	**SL** (NSO, NSM, NSIM): nothing available. **NSD/NSM:** TOSCAN [12], IBM's Blueprint, rSLA
NAS	FP7-TNOVA (www.t-nova.eu): developers can sell their PNFs and VNF software through auctioning EU FP7-UNIFY (www.fp7-unify.eu): information base, where the resource characteristics of PNFs can be stored FP7-MCN (https://www.mobile-cloud-networking.eu/): a service catalog lists network services composed of multiple network functions EU H2020 SONATA (www.sonata-nfv.eu): emulation platform to support network service developers to locally prototype and test complete network service chains **Open Source JUJU Charm Catalog (https://jujucharms.com)**
IL	• **Orchestration:** Openstack Tacker, Rift IO, Hurtle, Open-O, Open-Baton, Cisco's Network Services Orchestrator (NSO), Huawei CloudOpera • **VNFM:** Canonical JUJU, Cloudify, Nokia CloudBand Application Manager, Cisco Elastic Services Controller (ESC) VNFM, Ericsson Network Manager (ENM), Huawei CloudOpera • **VIM:** OpenStack, CloudStack by Citrix, Cloudify, Ericsson Cloud Manager (ECM), Microsoft Azure, Google and Amazon clouds, Hypervisor Technologies (KVM, DOCKER, LCX/LXD, XEN, ESCi, etc.)

Table 1. Technology drivers.

request describes the network topology of the EPC and eNodeB elements, together with interconnect requirements and the requested QoS.

- Negotiation A (between SL and NAS): A policy-based and SLA-compliant set of PNF and VNFs must be exposed to the SL for the specific request. The logical NSD is translated by the NAS into distinct VNFs. The idea is that while, for example, the SL triggers a request for a mobility management entity (MME), the NAS returns the best-matching VNF by means of policing and QoS satisfaction. In order to be completely hardware-agnostic, the NAS only interacts with the SL and not the IL.
- Negotiation B (between SL and IL): The multi-domain orchestrator is the IL component that interacts with the SL. Note that any type of resource or required communication should take into account SLAs of the composed VNAs and VNF bundles.

In our example, because the real-time base station system (the eNodeB) requires for given delay guarantees and EMBB, a specific scheduling approach and channel mapping procedure needs to be considered. After this negotiation, the final NSD/NSM is derived.

Provisioning Phase: All the hardware/software components are provisioned by messaging in the IL layer (triggered by the IL multi-domain orchestrator), a specific scheduler is used at the eNodeB to satisfy the SLA agreements, and SDN control has been applied to configure the switch fabric. All the software components (e.g., NSIM and NSM) have been initialized in the SL for this specific network slice.

Operation Phase: When the network is operational, end-to-end data bearers are established, and traffic performance indicators and network services are monitored, while actions are taken in case of degradation. The life cycle management and control of the slice and enforcement of the actions to overcome degradation are done through the NSSO orchestration functions and interactions with the NSSM and the NSIM.

LTE Network Slices: Technology Landscape

In this section, we describe the current landscape of technologies and tools that can drive the actual implementation of the network slices for LTE networks. A summary is depicted in Table 1.

Network Slice Service Layer (SL): Research activities like [11] describe issues related to SL; however, they are more relevant to IL operations. For the actual implementation of the SL, there is no framework that could even partially cover the functionalities required. Regarding the NSD/NSM files, recent activities are around the TOSCAN [12] model, while IBM's Blueprint and custom solutions are proposed. However, there is still no mature solution available.

Network and Application Store: Service catalogs with PNFs and VNFs are implemented in the context of the FP7-TNOVA, FP7-Unify, FP7MCN, and H2020 SONATA projects. Service developers publish their PNFs and VNF software, which can be used by other developers. A complete VNF marketplace and management system is also supported by Canonical's JUJU Framework.

Infrastructure Layer for LTE Network Slices

In the evolved LTE, network slicing is closely related to the concept of RAN sharing for multi-service offering. 3GPP has defined and ratified different kinds of architectures with varying degrees of sharing (see the 3GPP TS 23.251 specification). By means of mobile network resource sharing, actually three dimensions of the problem exist:

- Sharing the processing/network/storage infrastructure: The switch fabric and the core network/system (CPU, storage, memory) are virtualized and shared between tenants for the deployment of physical or virtual network elements such as SP gateway (SP-GW), MME, and home subscriber service (HSS) [13].
- Sharing the base station resources: Different sharing schemes and scenarios exist where the focus stays on the way the physical resource blocks (PRBs) in the frequency/time/space domain, are shared in the medium access control (MAC) layer to provide isolation while maintaining the multiplexing gain [14].
- Sharing the spectrum resources: The spectrum sharing problem is not related to MAC layer operations. It is related to the band of operation or activation of a component carrier. If multiple operators can share bands, the band of operation can be dynamically adjusted. Cognitive radio techniques fall under this category.

Cloud and NFV Control, Management, and Orchestration when Slicing the RAN: For the deployment of both the EPC and the eNodeB, commodity hardware (the one used for typical processing) and Openstack cloud control with hypervisor (e.g., KVM) or container-based (e.g., LXC/LXD, Docker) VM technologies can be used. In addition, a pervasive perception, especially from the telecom operator side, considers for the coupling of cloud technologies with NFV in order to alleviate the problem of LTE services' dependence on hardware. In Table I we summarize technologies and frameworks that can be used to support the functionalities required by the IL.

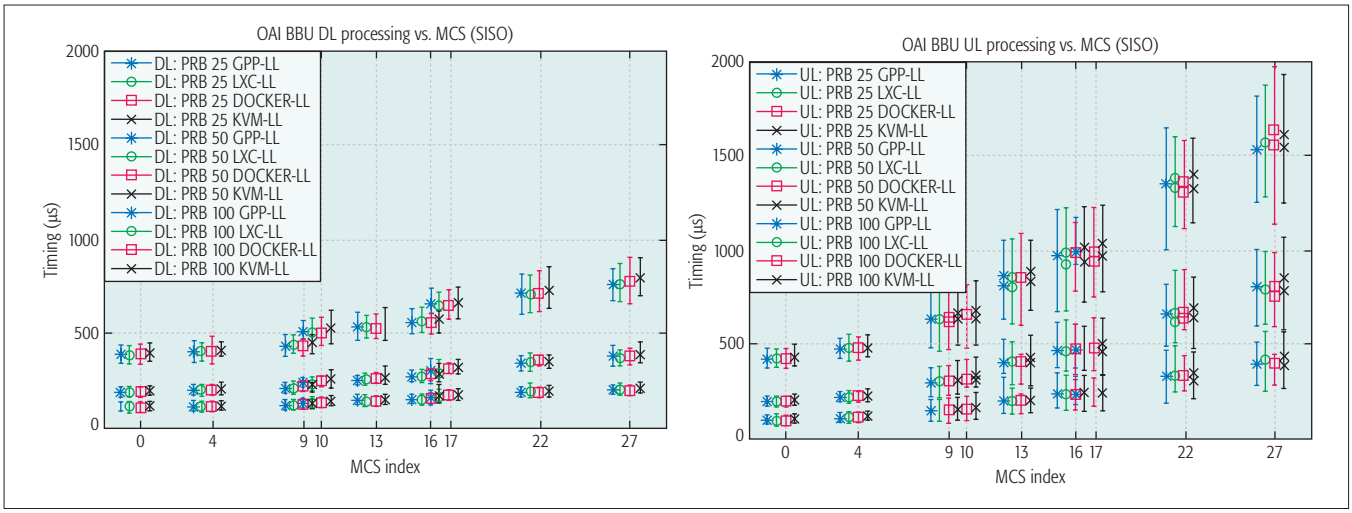


Figure 3. Performance comparison on running virtualized LTE.

However, natural questions arise in this case: Is the explosion of LTE elements as VNFs feasible? What is the cost of deploying LTE services as VNFs on top of virtualized environments? Or will there be performance degradation? What about the VIM and orchestration efficiency in the case of LTE networks? While in the following we answer the first three questions through two implementation experience examples, there is no clear answer for the third.

Implementation Experience A: Running LTE Components in VMs: In [2], the LTE as a service (LTEaaS) slice framework was presented, where both the EPC services and the eNodeB were deployed in a virtualized environment, using Openstack and Linux LXC containers. The OpenStacks Heat Orchestration Templates (HoT) were used to describe the specification of the LTE network elements. In this approach, all the advantages of using cloud control and services can be exploited to meet a number of challenges, like scalability issues or hardware dependencies. However, no control on the slice itself is provided after the deployment.

Regarding the performance when running LTE services in a virtualized environment, Fig. 3 compares the BBU processing budget of a general-purpose processor (GPP) platform with different environments: LXC, Docker, and KVM for the downlink (left) and the uplink (right). While, on average, the processing times are very close for all the considered virtualization environments, it can be observed that GPP and LXC have slightly lower processing time variability than that of DOCKER and KVM, especially when the data rate increases, that is, more PRBs and modulation and coding schemes (MCSs). Processing load is mainly dominated by uplink and increases with growing PRBs and MCSs. Furthermore, the ratio and variation of downlink processing load rate to that of uplink also grows with the increase of PRBs and MCSs. Indeed, the performance degradation can be negligible when running the LTE services over a virtualized environment. However, these results depict the performance assuming no multi-tenancy and no multi-user transmission. In a shared environment, concurrent operation of virtualized services coupled with high processing variability by multiple tenants can greatly affect the performance of all the different slices, sharing the underlay infrastructure.

Implementation Experience B: LTE Components as VNFs with OAI and the JUJU Framework: Our recent collaboration with Canonical (the company behind Ubuntu) has led to the open source exposure of the whole OAI LTE protocol stack for the EPC — MME, SP-GW, and HSS and the eNodeB entities using the JUJU VNFM framework. The eNodeB supports legacy 3GPP, and baseband unit (BBU) and remote radio unit (RRU) in support of functional split and Ethernet-based fronthaul.

The NFV concept in JUJU is built around software components called Charms. JUJU Charms are actually the set of scripts that encapsulates the VNF. A charm contains all the needed logic to deploy, integrate, scale, and expose the service to the outside world.

As shown in Fig. 4, the OAI solution can be chained together using JUJU Charms relationships, while relationships can be established with IP Multimedia Subsystem (IMS) Charms (provided, e.g., by OpenIMS or ClearWater) to rapidly build applications over LTE, such as voice and video. A sample definition for a single VNF, where the OAI-eNodeB is exposed, is presented on the left of Fig.4. Note that in order to have a complete functional VNF system, the total provisioning time derives from a summation of sequential steps:

- VM installation from a local or remote image
- Resolving packages dependencies
- Service installation and actual deployment

To give some insights on the LTE eNodeB deployment as a VNF, using the JUJU system over a clean installation requires 600 s, configuration 4 s, and service upgrades 122–300 s. These values are greatly affected, of course, by the available hardware and network and configuration options.

SDN Control and Programmable RAN Elements: One important feature that a network slicing architecture should integrate is the ability to control, in real time, the configuration of resources dedicated to one slice. To this aim, integrated network programmability and open APIs using the SDN approach is the indented way to actually

The most important open issues are related to the SL, since there is no solution available. Furthermore, effort must be given for the interfaces and APIs definition among all the architecture layers. Questions related to the NFV management and ETSI NFV MANO equivalence and the role of network slicing and the way it actually can be realized in the wireless domain, remain open.

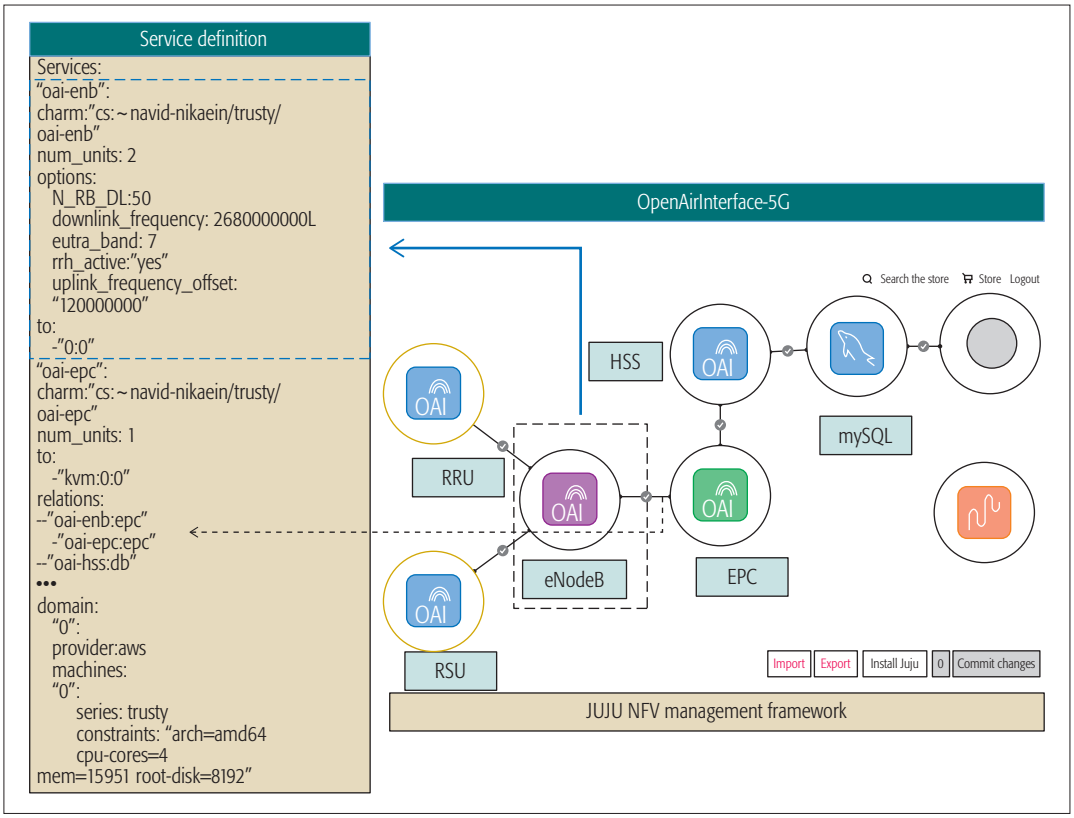


Figure 4. JUJU and OAI: The first open source LTE VNF solution.

control the network segment in support of network slicing.

- *SDN control on the switch fabric:* SDN control can be used to facilitate network agility through efficient control, coordination, and management of the physical or virtualized EPC core network. For example, SDN control can be used to control the virtual switches used for the virtual network interconnect. In addition, new control plane enhancements are now emerging. For example, SDN control is proposed to facilitate efficient S1-Flex operations. In this case, multiple (MME, serving gateway [S-GW]) elements can serve a common area while connected by a mesh network to the set of eNodeBs.
- *Programmable eNodeB:* For the realization of network slices at the eNodeB, efficient resource allocation and scheduling policy are required on a per tenant basis. Dynamic radio network functions chaining is also required to adapt the operation of the eNodeB for each tenant and support a multi-service architecture. These issues are also investigated in the 5G-NORMA project.

While controlling the switch fabric and EPC core network easily could be managed by SDN and its southbound API, programming the RAN and managing its resources at runtime is very challenging. Indeed, a programmable RAN underlay is absolutely essential in order to enable active sharing though functionalities that can be exposed to an integrated control plane. Most importantly, real-time constraints in the eNodeB impose extreme challenges, since toward 5G communications, responsiveness in control and coordination must be at the sub-millisecond level. Thus, available southbound APIs and protocols like NetConf, Openflow, and REST will not work in that case.

In our approach, we exploit a novel southbound control protocol called FlexRAN, which was first proposed and analyzed in [15], using OAI-based LTE systems. In Fig. 5 a high-level representation of the solution is depicted. The standard separation of the control and data planes is used, with an agent that resides in the eNodeB communicating and interacting with a real-time controller entity. In contrast to traditional wired SDN approaches, time-critical zones are considered for the re-programmability of the data plane on the fly by a centralized controller or delegated to the local agent. The agent exposes a set of RAN APIs, which can be used to control one or many local network functions potentially exposed as VNFs in the eNodeB. The considered network functions controlled by the agent include:

- Time-critical VNFs like user-specific PHY processing and MAC/RLC scheduling functions
- Non-time-critical VNFs like statistics gathering and Packet Data Convergence Protocol (PDCP)/Go Text Protocol (GTP) functions

Note that the orchestrator logic is the one that will trigger per-slice resource and service provisioning; the controller-agent will be responsible for all the management procedures at the eNodeB at multiple timescales.

Challenges and Open Questions

The most important open issues are related to the SL, since there is no solution available. Furthermore, effort must be made on the interfaces and APIs' definition among all the architecture layers. Questions related to the NFV management

and ETSI NFV MANO equivalence and the role of network slicing and the way it actually can be realized in the wireless domain remain open. Furthermore, the SDN/NFV coupling in native LTE control plane designs can potentially support slice-based SLA-driven RAN designs, which, however, are missing.

Regarding workflows and service chains' control of slice clients, the way we identify the users and guarantee isolation is an open research topic, while for the slice life management, the network operator needs to provide APIs for slice/system monitoring.

One additional dimension is related to orchestration procedures and the way the ETSI NFV MANO proposal needs to be extended and actually implemented. What is multi-domain orchestration and how we can achieve it? What are the domain boundaries? Extending the notion of domain to multi-domain, the idea is that many domains which offer specific functionality are jointly considered and exploited to deliver their functionality as a whole.

Conclusions and Future Work

In this article, we describe a novel network slicing architecture for integrated 5G communications, featuring the heterogeneous wireless domain. We demonstrate its realization for the case of evolved LTE using state-of-the-art technologies. We also elaborate on the LTE-specific requirements toward 5G and point out existing challenges for network slicing in the context of multi-domain, multi-tenant environments.

Acknowledgments

This work has been supported by the 5G-PPP project Coordinated Control and Spectrum Management for 5G Heterogeneous Radio Access Networks (COHERENT), H2020/JP 5G!Pagoda project and FP7 FLEX.

References

[1] NGMN Alliance, "Description of Network Slicing Concept," 5G P1, vol. 1, 2015.
[2] N. Nikaein *et al.*, "Network Store: Exploring Slicing in Future 5G Networks," *Proc. 10th ACM Int'l. Wksp. Mobility in the Evolving Internet Architecture*, 2015, pp. 8–13.
[3] V.-G. Nguyen, T.-X. Do, and Y. Kim, "SDN and Virtualization-Based LTE Mobile Network Architectures: A Comprehensive Survey," *Wireless Personal Commun.*, vol. 86, no. 3, 2016, pp. 1401–38.
[4] S. Abdelwahab *et al.*, "Network Functions Virtualization in 5G," *IEEE Commun. Mag.*, vol. 54, no. 4, Apr. 2016, pp. 84–91.
[5] I. Da Silva *et al.*, "5G RAN Architecture and Functional Design," METIS II white paper, 2016.
[6] P. Rost *et al.*, "Cloud Technologies for Flexible 5G Radio Access Networks," *IEEE Commun. Mag.*, vol. 52, no. 5, May 2014, pp. 68–76.
[7] K. Katsalis *et al.*, "5G Architectural Design Patterns," *2016 IEEE ICC Wksps.*, 2016, pp. 32–37.
[8] P. Rost *et al.*, "Mobile Network Architecture Evolution toward 5G," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 84–91.
[9] C. J. Bernardos *et al.*, "An Architecture for Software Defined Wireless Networking," *IEEE Wireless Commun.*, vol. 21, no. 3, June 2014, pp. 52–61.
[10] R. Mijumbi *et al.*, "Management and Orchestration Challenges in Network Functions Virtualization," *IEEE Commun. Mag.*, vol. 54, no. 1, Jan. 2016, pp. 98–105.
[11] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From Network Sharing to Multi-Tenancy: The 5G Network Slice Broker," *IEEE Commun. Mag.*, vol. 54, no. 7, July 2016, pp. 32–39.
[12] T. Binz *et al.*, "Portable Cloud Services Using TOSCA," *IEEE Internet Computing*, vol. 16, no. 3, 2012, pp. 80–85.

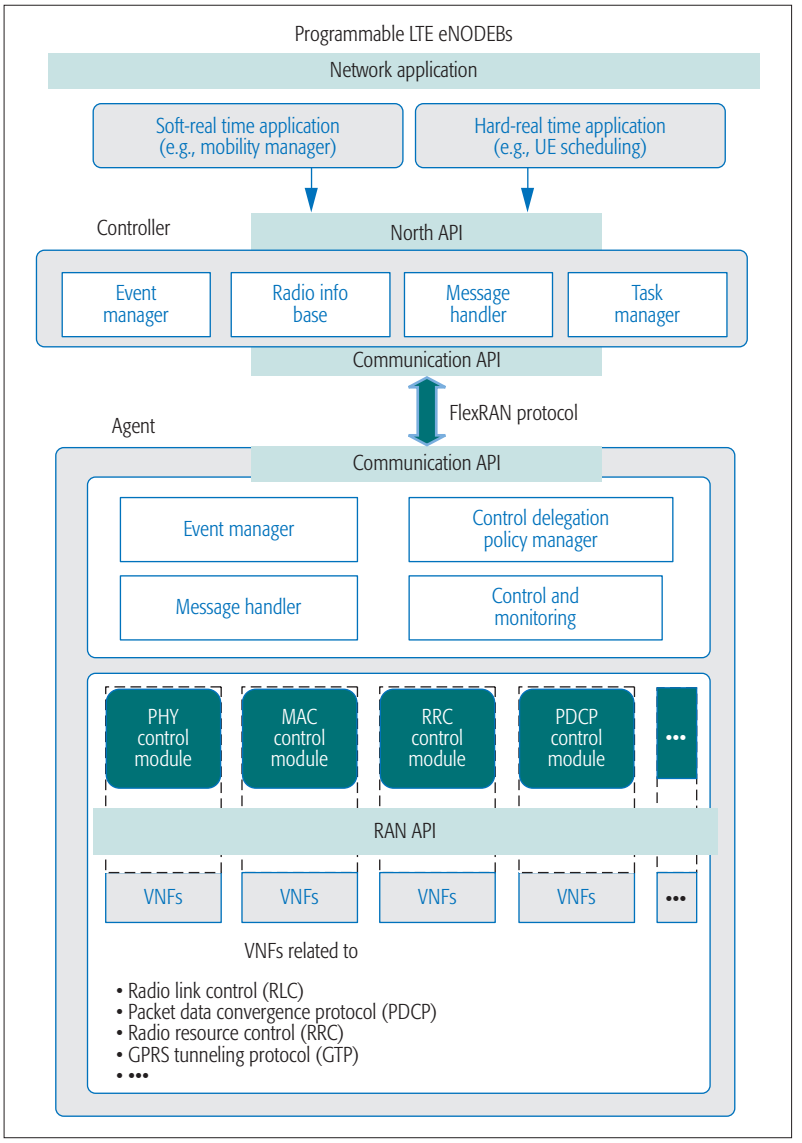


Figure 5. The FlexRAN protocol, agent, and controller.

[13] A. Antonopoulos *et al.*, "Energy-Efficient Infrastructure Sharing in Multi-Operator Mobile Networks," *IEEE Commun. Mag.*, vol. 53, no. 5, May 2015, pp. 242–49.
[14] R. Kokku *et al.*, "Nvs: A Substrate for Virtualizing Wireless Resources in Cellular Networks," *IEEE/ACM Trans. Net.* , vol. 20, no. 5, 2012, pp. 1333–46.
[15] X. Foukas *et al.*, "Flexran: A Flexible and Programmable Platform for Software-Defined Radio Access Networks," *Proc. 12th ACM Int'l. Conf. Emerging Networking Experiments and Technologies*, 2016, pp.427–41.

Biographies

Kostas Katsalis (kostas.katsalis@eurecom.fr) is a research fellow at EURECOM, Sophia Antipolis, France. He holds a Ph.D. (2010–2015) and an M.Sc. (2007) in electrical engineering, both from the University of Thessaly, Greece, under the supervision of Prof. Leandros Tassiulas. He received his diploma in electrical and computer engineering from the University of Patras, Greece, in 2005. He was a research associate and a researcher at CERTH-ITI, Greece, for six years, while he also has two years of experience in the mobile services industry. He has participated in the technical management activities for the FP7 CONTENT project and 5G-PPP XHAUL, and he is now involved in the 5G-PPP COHERENT and Fire+ Q4Health projects. His research interests focus on SDN, network functions virtualization, network slicing and RAN sharing, stochastic control theory, and network optimization.

Navid Nikaein (navid.nikaein@eurecom.fr) has been an assistant professor in the Communication Systems Department at EURECOM since 2009. He received his Ph.D. degree in com-

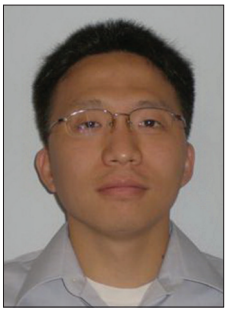
munication systems from the Swiss Federal Institute of Technology (EPFL) in 2003. Currently, he is leading a research group focusing on experimental system research related to wireless systems and networking. Broadly, his research interests include wireless access and networking protocols (4G/5G), cloud-native and programmable mobile networking (SDN, NFV, MEC), and real-time RF prototyping and emulation/simulation.

ERYK SCHILLER (schiller@inf.unibe.ch) received two M.Sc. diplomas: in electronics and telecommunications from the University of Science and Technology, and in theoretical physics from the Jagiellonian University, Cracow, Poland, in 2006 and 2007, respectively. He got a Ph.D. in computer science from the University of Grenoble, France, in 2010. He was a postdoctoral scholar at the University of Neuchatel, Switzerland. Since 2014, he has been with the University of Bern, Switzerland, as a senior researcher.

TORSTEN BRAUN (braun@inf.unibe.ch) got his Ph.D. degree from the University of Karlsruhe, Germany, in 1993. From 1994 to 1995 he was a guest scientist at INRIA Sophia-Antipolis (France). From 1995 to 1997 he worked at the IBM European Networking Centre Heidelberg, Germany. He has been a full professor of computer science at the University of Bern, Switzerland, since 1998 and a member of the SWITCH (Swiss education and research network) Board of Ttrustees since 2001.

ADLEN KSENTINI (adlen.ksentini@eurecom.fr) received his M.Sc. degree in telecommunication and multimedia networking from the University of Versailles Saint-Quentin-en-Yvelines, and his Ph.D. degree in computer science from the University of Cergy-Pontoise in 2005, with a dissertation on QoS provisioning in IEEE 802.11-based networks. From 2006 to 2016, he worked at the University of Rennes 1 as an assistant professor. During this period, he was a member of the Dionysos Team with INRIA, Rennes. Since March 2016, he has been working as an assistant professor in the Communication Systems Department of EURECOM. He has been involved in several national and European projects on QoS and QoE support in future wireless, network virtualization, cloud networking, and mobile networks. He has been a Guest Editor of *IEEE Wireless Communications*, *IEEE Communications Magazine*, and two issues of ComSoc *MMTC Letters*. He has been on the TPCs of major IEEE ComSoc, ICC/GLOBECOM, ICME, WCNC, and PIMRC conferences. He is currently the Vice-Chair of the IEEE ComSoc Technical Committee on Software (TCS).

ADVANCES IN OPTICAL COMMUNICATIONS TECHNOLOGIES

Xiang Liu Zuqing Zhu

In 2017, as fiber optic communications technologies continue to demonstrate their advantages in telecom and data center networks, we are also witnessing attractive and promising progress on optical wireless communications, which can potentially work with RF communications to meet the ever-increasing demands for higher date transmission rates and smart home networking. Meanwhile, the innovations in optical communications and networking systems can never be realized without fundamental support from the physical infrastructure layer. The recent advances on few-mode fibers open up appealing opportunities for equipment vendors and network operators to solve the capacity crunch problem using mode-division multiplexing. To integrate the momentum gained from these technical advances, an efficient and intelligent network control and management (NC&M) mechanism is essential, especially for building heterogeneous networks to support a wide range of services with various traffic patterns. Therefore, the implementation of software-defined networking (SDN) in optical communications networks appears inevitable, and we expect to see more advances in this area in 2017.

In this second Optical Communications Series (OCS) issue of 2017, we have selected four contributions that address the optical camera communication, few-mode optical fibers, YANG models for vendor-neutral optical networks, and protected converged optical access networks.

In the first contribution, "Optical Camera Communication: Motion over Camera," S. Teli, W. Cahyadi, and Y. Chung present a flexible and novel motion detection scheme over a smart device camera for optical camera communication (OCC). The motion detection or motion over camera (MoC) is designed to detect motion in terms of the user's finger movement via the camera while the OCC link is active. A simple but efficient quadrant-division-based motion detection algorithm is proposed for reliable and accurate detection of motion. Regarding key applications, it is envisioned to be applied in a smart home environment. The proposed MoC can also be considered in the context of a hybrid optical wireless communication system operable with existing RF-based systems such as Wi-Fi.

In the second contribution, "Few-Mode Optical Fibers: Original Motivation and Recent Progress," K. Kitayama and N. Diamantopoulos present their review of R&D activities on few-mode fiber, a special class of multimode optical fibers, beginning with its original motivation in the late 1970s to ease difficulty in splicing single-mode fibers, the operation principles, and the reason behind the research discontinuation in the mid-1980s. In addition to the earlier work, the article also reviews the progress of few-mode fibers after the resurgence of research in the 2010s. Recent revisiting of few-mode fibers is mainly motivated to solve the capacity crunch problem of optical fiber transmissions using mode-division multiplexing. The authors discuss difficult challenges that current research on mode-division multiplexing is facing. Such a revisit of few-mode fibers after their invention more than 30 years ago deserves showcasing for those engaged in research and development today.

In the third contribution, "YANG Models for Vendor-Neutral Optical Networks, Reconfigurable through State Machine," M. Dallaglio, N. Sambo, F. Cugini, and P. Castoldi present YANG models for optical networks, especially for those adopting flexible grids. The article first presents the YANG language and its syntax. Then it reviews some YANG models for elastic optical networks, detailing nodes, links, media channels, and sliceable transponders. Finally, the article describes and demonstrates in a control plane testbed an innovative YANG model enabling advanced transponder reconfiguration (based on a finite state machine). This work impacts the control (configuration) and management (operation, administration, and maintenance) of next generation core and metro networks by showing solutions that provide high device programmability and flexibility. It also impacts the adoption of white boxes (i.e., switching and compute nodes aggregated with modules from different vendors). The deployment of white boxes requires standard vendor-neutral solutions for control and management, and the presented YANG models go in this direction.

In the fourth contribution, "Dimensioning and Assessment of Protected Converged Optical Access Networks," A. Shahid and C. Machuca present a converged access network planning and dimensioning tool for planning and dimensioning of networks for fixed mobile convergence based on geographical information systems (GISs). This tool proposes a new clustering algorithm to decrease fiber and duct length. Furthermore, five protection schemes are proposed, modeled, and compared in dense urban, urban, and rural areas to improve connection availability to more availability-demanding endpoints.

BIOGRAPHIES

ZUQING ZHU [SM'12] (zqzhu@ieee.org) received his Ph.D. degree from the University of California, Davis, in 2007. He is currently a full professor at the University of Science and Technology of China. Prior to that, he worked in the Service Provider Technology Group of Cisco Systems, San Jose, California. His research focuses on optical networks, and he received the Best Paper Awards from IEEE ICC 2013, IEEE GLOBECOM 2013, IEEE ICNC 2014, and IEEE ICC 2015.

XIANG LIU [F'17] (xiang.liu@huawei.com) received his Ph.D. degree in applied physics from Cornell University in 2000. He is currently the senior director of Optical Access Networks Research at the U.S. R&D Center of Huawei Technologies, focusing on next-generation optical access technologies. He spent the early part of his career at Bell Laboratories in New Jersey, working on high-speed optical fiber transport technologies. He is a Fellow of the OSA and a Deputy Editor of Optics Express.

Optical Camera Communication: Motion over Camera

Shivani Teli, Willy Anugrah Cahyadi, and Yeon Ho Chung

OCC is a pragmatic version of VLC based on a smart device camera that allows easier implementation of various services in smart devices. This article presents a flexible and novel motion detection scheme over a smart device camera in OCC. The motion detection is conducted in conjunction with a static downlink optical camera communication, where a mobile phone front camera is employed as the receiver and an 8 × 8 dot matrix LED as the transmitter.

ABSTRACT

OCC is a pragmatic version of VLC based on a smart device camera that allows easier implementation of various services in smart devices. This article presents a flexible and novel motion detection scheme over a smart device camera in OCC. The motion detection is conducted in conjunction with a static downlink optical camera communication, where a mobile phone front camera is employed as the receiver and an 8 × 8 dot matrix LED as the transmitter. In addition to the 8 × 8 dot matrix LED for data transmission, 10 white LEDs are also employed for providing illumination, acquiring camera focus, and light metering. The motion detection or MoC is designed to detect the user's finger movement through the OCC link via the camera. A simple but efficient quadrant division based motion detection algorithm is proposed for reliable and accurate detection of motion. The experiment and simulation results demonstrate that the proposed scheme is able to detect motion with a success probability of up to 96 percent in the mobile phone camera based OCC. It is envisioned that the proposed motion detection can facilitate cost-effective and convenient smart home environments in the OCC, where the provision of illumination and short-range wireless communications has already been addressed.

INTRODUCTION

Visible light communication (VLC) has emerged as an attractive communication technology over the last decade because it uses existing lighting infrastructure composed of light emitting diodes (LEDs) as the transmitters. VLC takes advantage of free unregulated frequency allocation, high security, and harmlessness to human health, and provides higher-speed, lower-cost wireless communications compared to radio frequency based wireless communications. Due to these advantages, several LED-based VLC transmission technologies for indoor wireless communication systems have been documented [1, 2].

Over the past few decades, mobile phones have been equipped with a built-in complementary metal oxide semiconductor (CMOS) camera. Current mobile phones are capable of capturing high-resolution videos with a resolution of at least 1280 × 720 pixels and a capture rate of 30 fps [3]. Considering the various advantages and availability of mobile phone cameras, a new optical communication technique using cameras has been studied in IEEE 802.15 SG7a within the framework of optical wireless communications and considered as a candidate for IEEE 802.15.7rl, which is called optical camera communication (OCC) [4, 5]. The OCC technique is an extension of VLC with the advantage of no extended hardware cost of the receiver in most smart devices [5]. Unlike conventional VLCs, which employ photodetectors (PDs), the OCC utilizes a mobile phone CMOS camera as the receiver [3, 6]. That is, OCC captures two-dimensional data in the form of image sequences, thus being able to transmit more information compared to photodetector-based VLCs.

Recently, a concept of motion detection has been introduced as an additional functionality in VLCs, where illumination and communication are two primary functionalities [7]. A motion detection scheme is deemed attractive and viable for controlling smart devices in future VLC-based smart homes [7, 8]. VLC-based motion detection and its optical shadowing compensation have been investigated for smart home applications [7, 9]. However, the VLC based motion detection technique in [7] has an unrealistic placement of PDs in smart home applications. In the context of motion detection itself, a gesture control scheme using a vision-based control method was introduced [10]. It detects gestures by scanning the peak of a user's fingers using a webcam and controls the mouse cursor in a PC. A similar study was reported in which the motion detection and open finger counting through a webcam were proposed in an indoor environment [11]. A gesture control technique using infrared beam was investigated by the authors of [12].

In this article, a simple and convenient motion detection scheme over a mobile phone camera in the OCC is proposed. It is aimed at providing an additional means of motion-based device control through a smartphone camera in an existing indoor LED-camera communication link. In other words, the proposed scheme can offer three independent functionalities: illumination, communication, and motion detection. The mobile phone camera in the OCC is used as the receiver for both communication and motion detection. The principle of the motion detection is to monitor the movement of the user's fingers captured in the mobile phone camera. To accurately detect and identify the user's finger movement on the mobile phone camera, we designed a quadrant division based algorithm. To verify the proposed

Digital Object Identifier:
10.1109/MCOM.2017.1600923

The authors are with Pukyong National University.

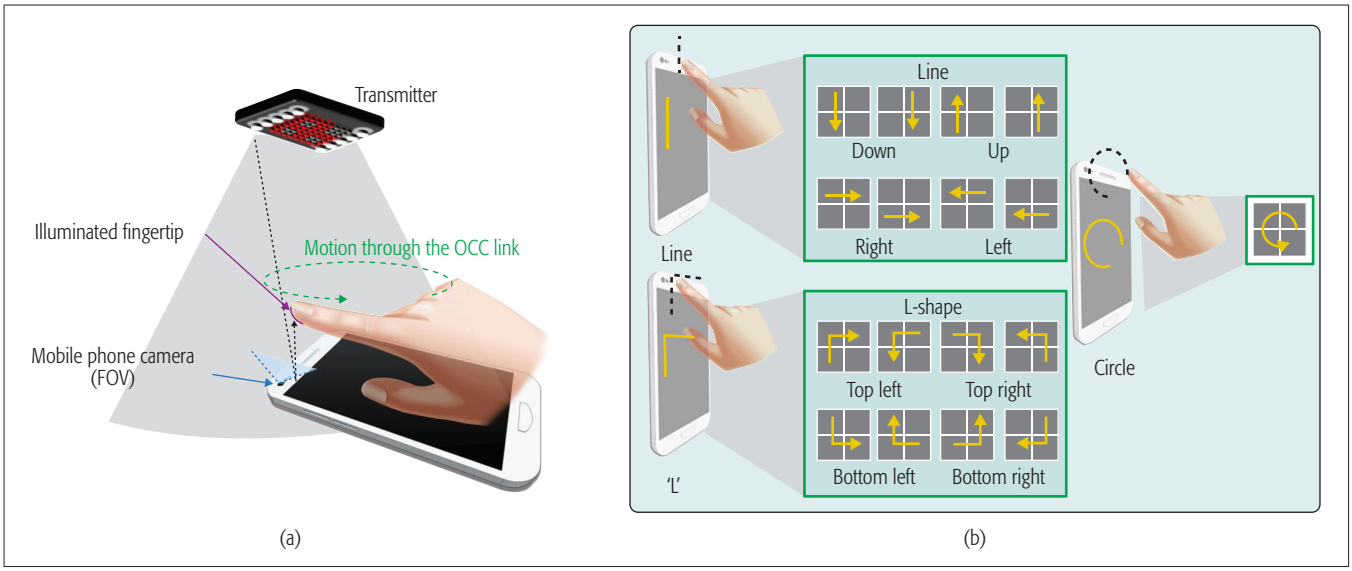


Figure 1. Proposed MoC in the OCC: a) system overview; b) three motions: line, L-shape, and circle.

scheme, we conducted experiments with three motions, that is, line, L-shape, and circle. It is obvious that during motion detection, the OCC link can be affected; hence, a compensation method also needs to be considered. To address this compensation, researchers have recently considered keyframe (header) based transmission and demonstrated that acceptable communication quality is achievable up to 30 cm distance between the mobile phone camera and the dot matrix LEDs [6]. The proposed scheme utilizes this periodic keyframe transmission for acceptable communication quality while performing the motion detection.

The following sections provide details of the proposed motion over camera in the OCC, its experiment setup, results, and conclusions.

Proposed Motion Detection over Camera in the OCC

System Overview

The proposed motion over camera (MoC) in the OCC is carried out by monitoring the movement of the user's finger captured in the front camera of a mobile phone, followed by a detection and identification process. Figure 1 illustrates the proposed motion over camera in the OCC. Motion is performed through the OCC link, where an 8 × 8 dot matrix LED is used as the transmitter, and 10 white illumination LEDs are placed for both illumination and reference light for camera light metering and focus [6]. These illumination LEDs also play an important role in illuminating the user's finger as the illumination light strikes the mobile phone screen and is then reflected back toward the fingertip as shown in Fig. 1a. Since there is clear distinction between the finger and its surrounding, the illuminated finger is traceable by the camera.

The user is required to make a motion over the camera of a mobile phone placed under the dot matrix LED in a static condition. This motion is captured by the mobile phone camera in the form of a video, which is then split into various frames for processing. We have designed a quadrant division based motion detection algorithm for the processing of the frames. For demonstration purposes, we chose three simple but natural motions: line, L-shape, and circle motions. Figure 1b shows these three exemplary motions. The figure also shows possible directions for the line and L-shape motions. The directions of motions are also considered in the motion detection algorithm.

The block diagram of the OCC system incorporating the MoC is shown in Fig. 2a. The transmitter comprises the data generation block that generates random binary data for transmission along with its keyframe. The keyframe is a special header frame introduced in the generated data for evaluating the transmitted data in the receiver [6]. For the data modulation, we employed on-off keying (OOK) modulation, which is most commonly used for OCC to transmit data, through each LED of the 8 × 8 dot matrix LED array [3]. The mapping block maps the data according to the LED array addresses. The mapped data is then passed on to the LED driver for OCC transmission through the dot matrix LED.

In the receiver, the mobile phone camera is used for both motion detection and OCC data reception. Over the OCC link, a motion is created by the user's finger movement. The key principle of the detection algorithm is to compare any changes between the frames received from the mobile phone camera. The changes are expressed in the form of centroids that represent the center of a moving object in a coordinate. The detected centroids are then fed to the motion detection algorithm, where a distribution of centroids is analyzed and the motion is subsequently identified. On the simultaneous OCC link, meanwhile, a demapping process is performed in the form of time and spatial synchronization to detect headers and extract the data from the received frames. For a precise LED detection in the array on the OCC link, an efficient detection scheme called differential detection threshold (DDT) was employed [6].

As described previously, a keyframe is added periodically in the transmitter as a head-

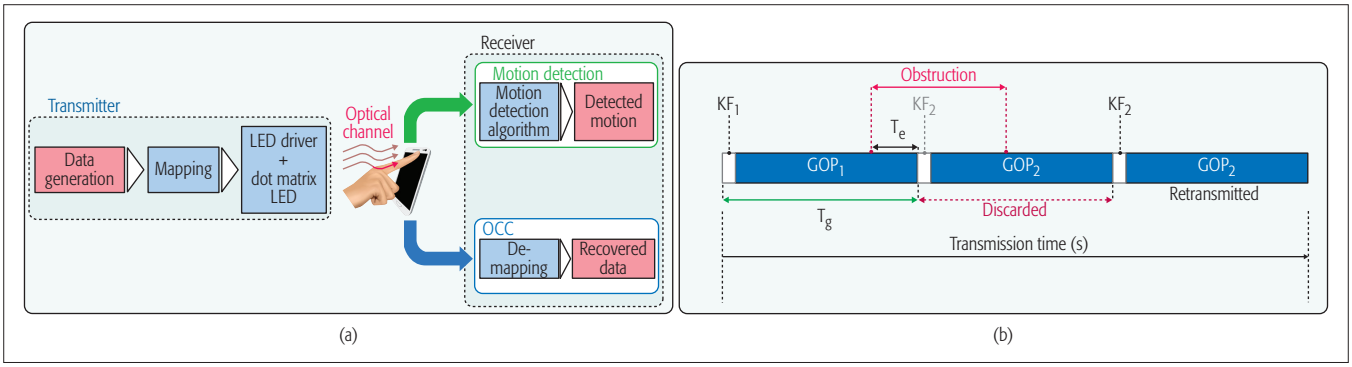


Figure 2. a) Block diagram of the MoC in the OCC; b) keyframe configuration.

er between every group of pictures (GOP). A GOP refers to a group of data frames. This keyframe plays an important role in performing data synchronization, through which it compensates for data loss by repeat request when the link is obstructed due to motion. Obviously, the keyframe reduces the data rate slightly, because it takes one time-slot in every GOP and thus the duration of the keyframe and GOP, denoted as T_g, can affect the data rate. To elaborate it further, when the obstruction due to motion occurs as in Fig. 2b, some part of GOP_1 (T_e), KF_2 and part of GOP_2 will be damaged, causing bit errors in the received data. Since the keyframe KF2 is not detected in the receiver, the most recent GOP (i.e., GOP_2) will be discarded and retransmitted via the receiver's repeat request. Hence, the data of GOP_2 will eventually be recovered. Unfortunately, the data over T_e period is lost and is not compensated in the present scheme. This data loss can be reduced by reducing T_g. A shorter T_g would, however, decrease the data rate. Therefore, there is a trade-off between the error rate (or T_g) and the data rate in the scheme. This issue is further elaborated together with the experiment results in the Results section.

Quadrant Division Based Motion Detection Algorithm

In the proposed MoC, we designed a quadrant division based motion detection algorithm. A flowchart of the quadrant division based motion detection algorithm is illustrated in Fig. 3a. Without loss of generality, it is assumed that the user creates one of the three exemplary motions. The algorithm detects the motions over the OCC link. For example, if the user makes a line motion using a finger over a mobile phone camera, the centroids generated by tracking the motion are recorded as a line. It is important to note that this motion tracking is made possible by the illuminated finger, which makes a clear distinction between the finger and the surroundings.The algorithm divides

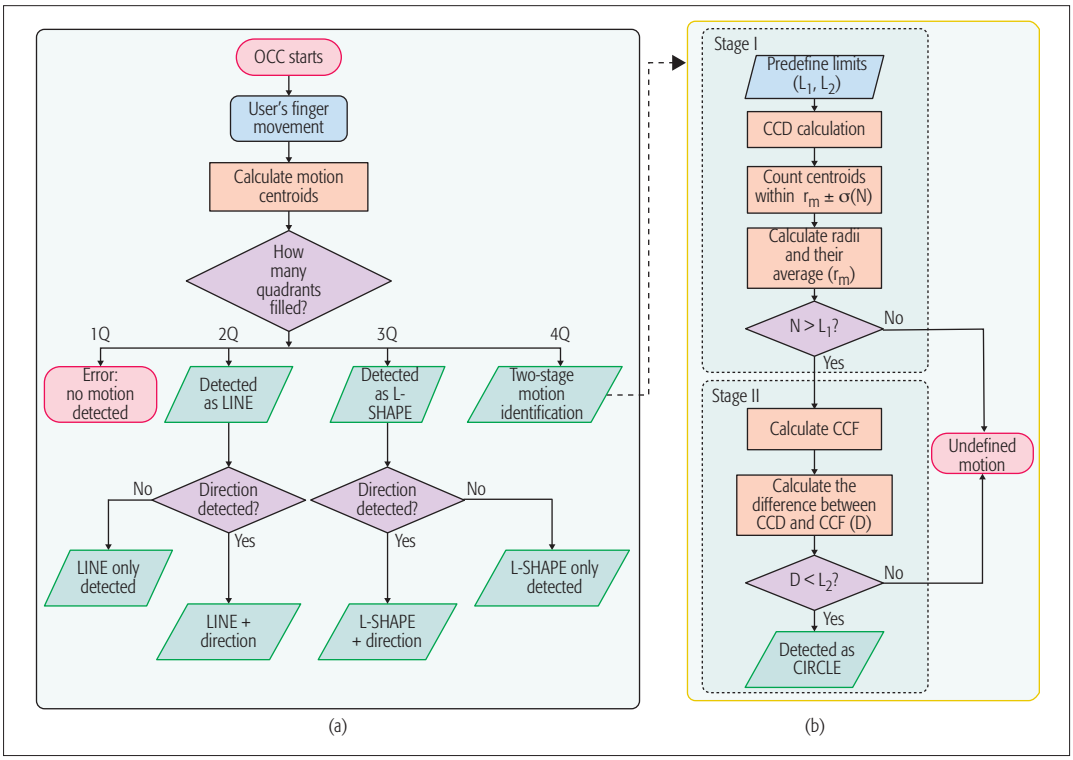


Figure 3. Quadrant division based motion detection algorithm: a) flow chart of the motion detection algorithm; b) two-stage motion identification for the circle motion.

the screen into four quadrants based on the Cartesian coordinate system and counts how many quadrants are filled by the centroids. For the line motion, only two quadrants need to be filled by the centroids. If the centroids fill more than two quadrants, two other possible shapes will be identified. As shown in Fig. 3a, if three quadrants are filled with centroids, the motion is identified as an L-shape, while four quadrants occupied by centroids go through a two-stage motion identification. If these two stages are satisfied, the motion is identified as a circle. For the present study, if the number of occupied quadrants is less than two, the motion is disregarded.

In addition to identifying the motions, the algorithm identifies the directions for the line and L-shape motions. The principle of direction detection is based on the detection of the order of quadrant filling. Again, in the case of the line motion, the algorithm first identifies the shape of the motion and finds the order of the quadrant filling. The directions for the line motion are detected according to the following order of the quadrant filling:

Left line : Q1 → Q2 or Q4 → Q3.
Right line : Q2 → Q1 or Q3 → Q4.
Up line : Q4 → Q1 or Q3 → Q2.
Down line : Q1 → Q4 or Q2 → Q3.

Similarly, for the L-shape motion, three quadrants are expected to be filled with motion centroids. As in the line motion, the direction of the L-shape motion can also be identified based on the direction in which the motion is performed:

Top left L-shape: Q1 → Q2 → Q3 or Q3 → Q2 → Q1.
Bottom left L-shape: Q4 → Q3 → Q2 or Q2 → Q3 → Q4.
Top right L-shape: Q2 → Q1 → Q4 or Q4 → Q1 → Q2.
Bottom right L-shape: Q3 → Q4 → Q1 or Q1 → Q4 → Q3.

As part of further verification of the proposed algorithm for motion detection, Fig. 3b shows a detailed description of the circle motion identification that would be considered relatively complex to detect. We consider a two-stage motion identification process based on centroid distribution (CD) and the center of centroid distribution (CCD). Note that the CCD is the center of all the centroids distributed over four quadrants. The two stages are also based on the circle Hough transform (CHT) technique for defining radius levels for circle detection [13]. CHT is a basic technique used in digital image processing for detecting circular objects in a digital image. The two-stage motion identification procedure is described below.

Stage I: The CCD is first found. The distance of each centroid to this CCD (i.e., radius) is then obtained. The average of the radii is then computed as r_m. Considering the CD, some centroids significantly deviating from r_m can be discarded as they do not contribute to detecting the shape. To this end, we set a value of standard deviation (σ) so that the centroids within $r_m \pm \sigma$ are found. The number of centroids in this range, N, is then obtained. It should be noted that σ needs to be determined under the consideration of a perfect circle shape and an image frame size as adopted in the CHT [13]. The algorithm then detects the circle motion by comparing N with a predefined limit (L_1). If N is larger than L_1, it is determined as a detectable motion. The decision for the circle motion will be finally made in stage II.

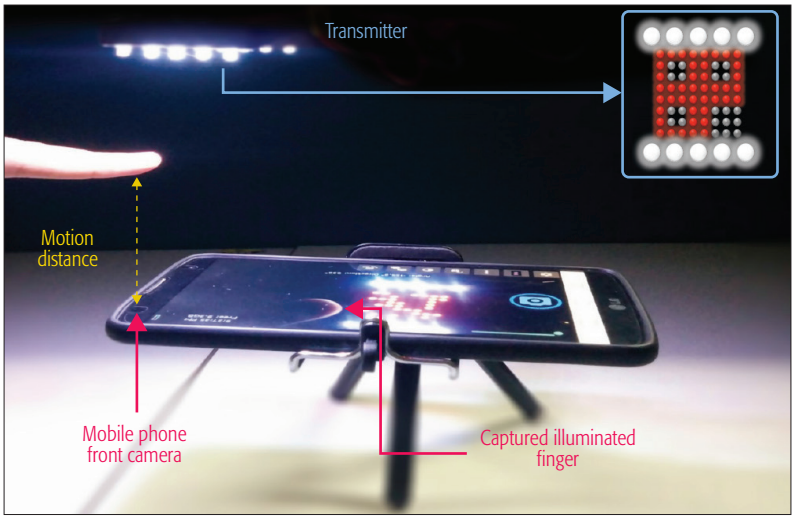


Figure 4. Experiment setup.

Stage II: In this stage, the center of capture frame (CCF) is found. Obviously, the CCF is fixed as it is the center of the capture frame over which the motion is performed. The distance between the CCD and the CCF is calculated and denoted as D. It is true that D is expected to be very small for the circle motion. That is, if D is smaller than a limit (L_2), the motion is detected as a circle.

It is important to note that although the two-stage motion identification algorithm for the circle motion has been proposed with a view to allowing various circle motions that the user would make over the OCC, it can be reduced to a single-stage algorithm for simple and rapid detection. That is, the algorithm with stage I only can also be applied for most circle motions, except for very irregular circles. In addition, it is certain that the proposed algorithm can be further extended to detect various other circle-like motions, such as arc, ellipse, and semicircle.

One important aspect of motion detection based on mobile phones is the duration of motion. If the motion is performed very fast, the CD would be sparse, resulting in irregular distribution and subsequently undefined motion. In the current experiments, a suitable value of empirically obtained Δt is 4 s with a tolerance of ± 2 s. For obvious reasons, the motion duration (Δt) is subject to both the user and shapes. In addition, it can be limited by the capture rate of the camera.

Experiment Setup

To verify the MoC in the OCC, an experiment was conducted with a mobile phone camera and an LED dot matrix and illumination LEDs. Figure 4 shows the experimental setup with the captured illuminated finger. For the purpose of demonstration of the proposed motion detection, experiments were performed at four different distances, that is, 12 cm, 15 cm, 18 cm, and 21 cm

One important aspect of the motion detection based on mobile phones is the duration of motion. If the motion is performed very fast, the CD would be sparse, resulting in an irregular distribution and subsequently undefined motion.

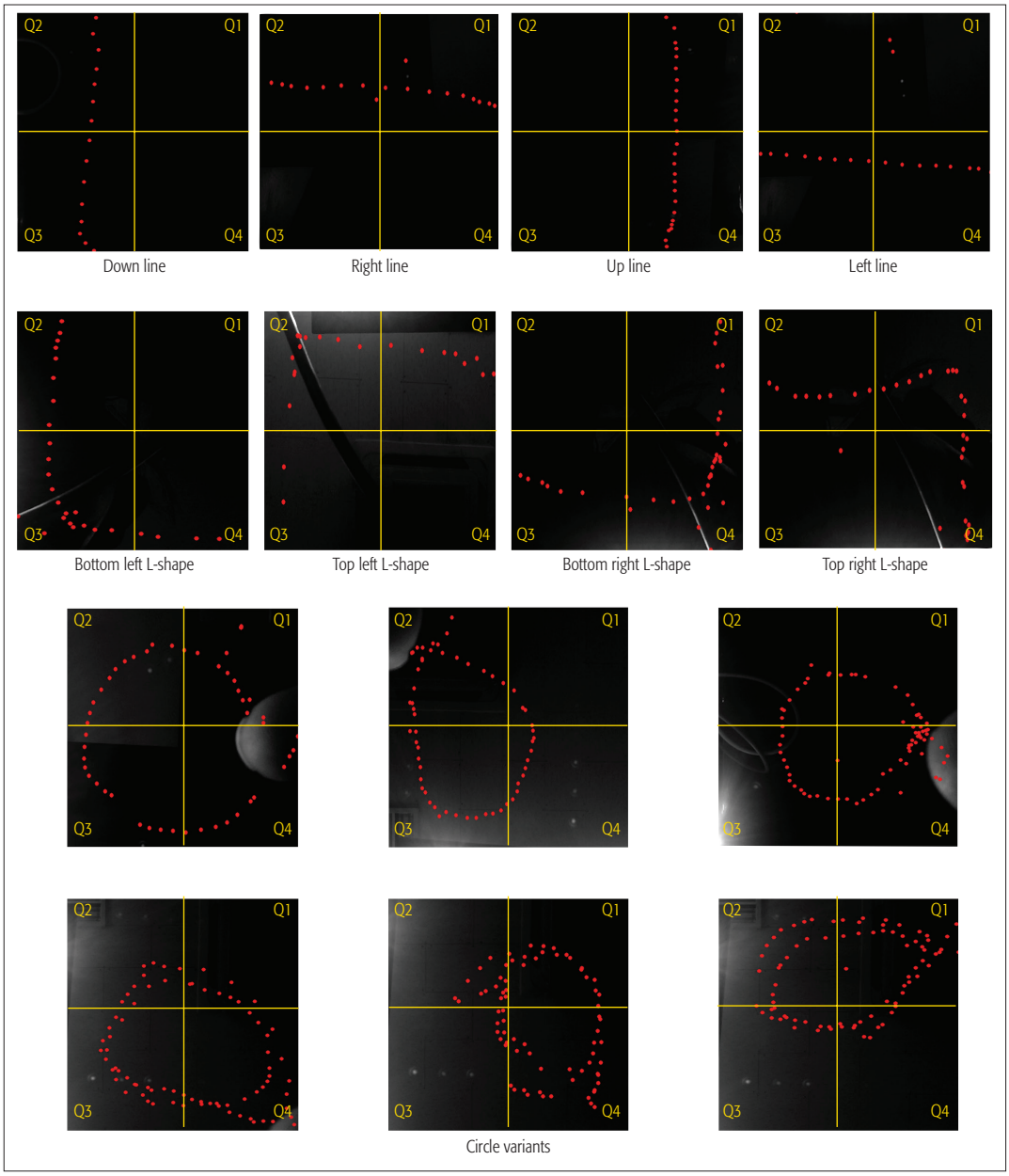


Figure 5. Experiment results: detected centroids of line, L-shape, and circle.

under a static condition. Similar to the transmitter employed in [6], we used an 8 × 8 dot matrix LED array with 4.31 V supply voltage and 10 illumination LEDs with 3.143 V supply voltage and 60 mW optical output power. In addition, five different *Tg* values were used for the transmission, that is, 100 ms, 200 ms, 250 ms, 500 ms, and 1000 ms.

Motions and data were received on an Android mobile phone camera that has a resolution of 1920 × 1080 pixels with a capture speed of 30 fps. An optimum motion distance between the user finger and the mobile phone was found to be in the range of 7–8 cm for all considered transmission distances. When the user forms a motion, it is captured by the mobile phone camera in the form of a video.

For a mobile phone camera with a lower resolution, it would result in a smaller OCC distance, but the motion detection performance presented remains unchanged, due to the fact that the motion distance in the present experiments is still close enough to the camera. A higher LED illuminance level can certainly increase the transmission and motion distances. Likewise, a higher capture speed benefits dense motion centroids; thus, the success probability of motion detection can be increased. The high capture speed will also reduce the motion duration. Therefore, the present scheme can be designed to be more practically viable in accordance with camera features and light intensity.

Results

Experiment results are shown in Fig. 5, where the centroids are marked in red dots. These red dots represent a tracked motion of the user's finger. These centroids represent three detected shapes, that is, line, L-shape, and circle.

Based on the proposed algorithm, the frame for the motion detection is divided into four quadrants, and the detected motion is represented by

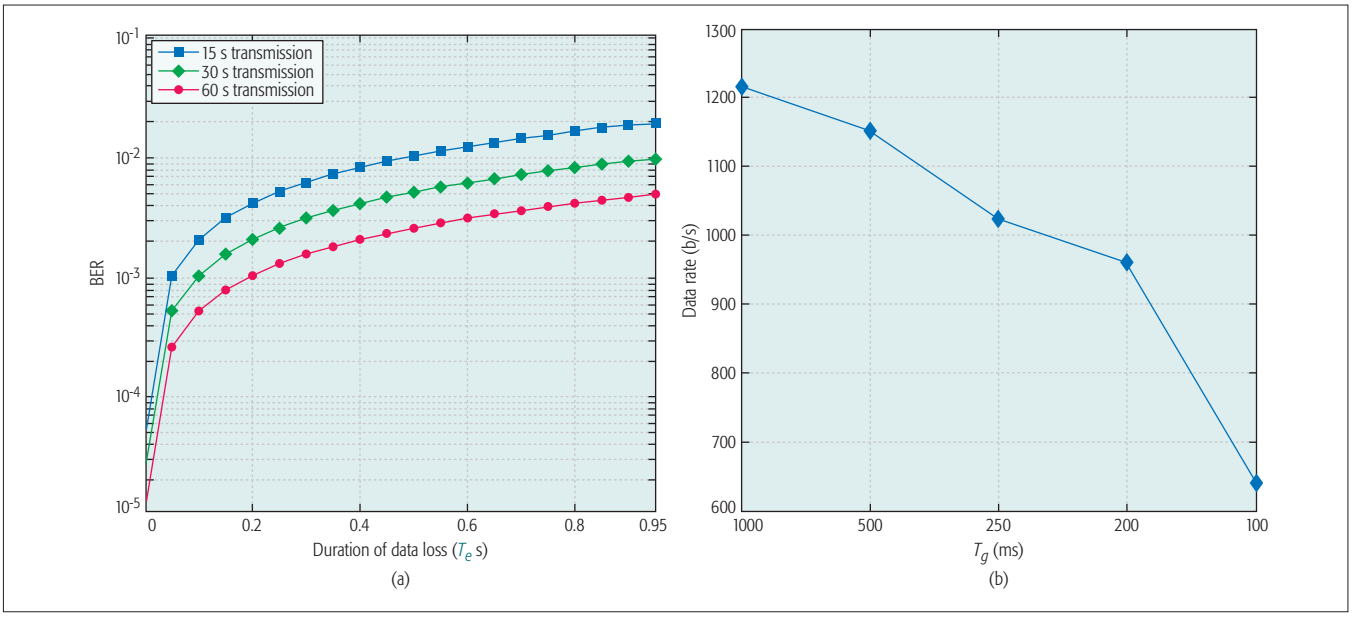


Figure 6. Performance analysis: a) BER; b) data rate.

centroid points (i.e., red dots). As the algorithm checks for the number of occupied quadrants, the motions are classified into line, L-shape, and circle. For the line and L-shape motions, the directions are also detected by finding the order of the quadrants filled. Figure 5 shows four different directions — up, down, right, and left line, and also top and bottom left and right L-shape motions. It should also be noted that the experiments were conducted for various types of circles to verify the robustness of the detection algorithm.

Since the OCC link supports communication as well as illumination, it is important to ensure that sufficient illuminance is provided in the first place. To this end, we measured average illuminance at the transmission distances of 12 cm, 15 cm, 18 cm, and 21 cm, and the values were found to be 2226 lx, 1533 lx, 1041 lx, and 721 lx, respectively. Thus, it was observed that the illuminance levels satisfy the illumination standard set forth by the International Organization for Standardization (ISO) [1].

Table 1 shows the experiment results in terms of the percentage of success for the motion detection performed over a total of 90 experiments. That is, for each distance, 30 experiments were performed,10 experiments per shape. In the experiments, the directions for the line and L-shape motions were also included. It is observed that the maximum percentage of success, 96 percent, was achieved at 12 cm distance. It is also found that the percentage of success decreases as the distance increases. Up to a distance of 18 cm, it was possible to detect the motion relatively accurately. For the 21 cm distance, however, the percentage of success was reduced to 76 percent. This is due to the fact that the illumination level of the finger becomes lower as it moves away from the illumination LEDs.

As noted previously, the proposed scheme is based on the periodic keyframe. It is interesting to analyze performance variation over the obstructed time during the user's motion. As we used an effective capture speed of 20 fps, the frame period is 50 ms. Figure 6a shows the bit error rate (BER) analysis in terms of T_e. It is observed that a longer data transmission produces improved BERs. This is due to the fact that the scheme can repeat the obstructed frames, thus improving the BER. For the 60 s transmission, an acceptable BER value of 10^{-3} was obtained at a T_e value of 0.2 s.

Shapes	12 cm	15 cm	18 cm
Circle	10	9	8
L-shape	9	9	8
Line	10	10	9
Percentage of success	96%	93%	83%

Table 1. Percentage of success relevant to distance.

The retransmission of obstructed frames would yield a lower data rate in the OCC. It is then worth analyzing the data rate relevant to T_g. Figure 6b shows the result. Note that the maximum achievable data rate in the current setting (no keyframes, 8 × 8 dot matrix LEDs, 20 fps) is 1280 b/s. In the current OCC-based MoC, the maximum data rate of 1216 b/s was achieved at a T_g value of 1000 ms. The reduction in the data rate is caused by the addition of the keyframe. It is evident that the smaller a T_g value is, the lower the data rate will be.

Future Scope

A mobile phone based MoC is attractive to various indoor applications in the presence of indoor optical wireless communications. While the data transmission through an LED-camera link is performed, various smart devices can be controlled via the user's motion on the mobile phone. Specifically, although the MoC in the OCC link has been experimented on a laboratory scale, practical applications through smart devices (e.g.,

The experiment results demonstrate that a success probability of 96 percent and a data rate of up to 1216 bps were achieved, while the OCC link was in operation. It is anticipated that the MoC in the OCC can trigger a new dimension of the OCC applications in a smart home or industry environment.

smartphones or camera fitted watch straps) can be envisioned not only for smart users but also for those who need special aids. The proposed MoC can also be considered in the context of a hybrid optical wireless communication system operable with existing RF-based systems such as WiFi in order to harmoniously transmit control signals based on applications and devices [14].

The MoC can be made mobile in such a way that while the user is on the move, the motion can be performed. To ensure reliability in this mobility supported MoC, the proposed scheme should take into account changed positions of the CD and CCD. The algorithm could be enhanced with some modifications. Further, the communication link quality and data speed in the OCC-based MoC scheme can be improved with advanced cameras (e.g., a recent 330 fps camera), a modulation scheme, and a modified keyframe configuration for a more practical MoC in an indoor OCC environment.

The MoC in the OCC could also be enhanced by accommodating a concept of deep learning [15], thereby performing accurate detection in a computationally efficient way. That is, based on the observation of the motion, we can train the detection system with the most probable motion of the user. By considering all possible samples from observation, a database is created, leading to training the system for the motion detection in either a static or mobile manner. In this way, deep learning technology can contribute to increasing reliability significantly in the MoC.

Conclusions

A simple but efficient motion over camera scheme in optical camera communications has been presented. It provides motion detection plus two usual functionalities: illumination and communication. In concrete terms, the quadrant division based motion detection algorithm has been proposed, which delivers a decision on the motion a user performs on a mobile phone. Under the assumption that the user performs a motion in a normal fashion, that is, within the motion duration (Δt) in the present work, nine different motions inclusive of all directions except for the circle motion are found to be accurately distinguishable. Considering additional analysis and evaluation on the OCC communication quality, the scheme ensures acceptable communication quality as well as ensuring sufficient illumination in an indoor environment. The experiment results demonstrate that a success probability of 96 percent and a data rate of up to 1216 b/s were achieved while the OCC link was in operation. It is anticipated that the MoC in the OCC can trigger a new dimension of OCC applications in a smart home or industry environment.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the article. This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2015R1D1A3A01017713).

References

[1] T. Komine and M. Nakagawa, "Fundamental Analysis for Visible-Light Communication System Using LED Lights," *IEEE Trans. Consumer Electronics*, vol. 50, no. 1, 2004, pp. 100–07.
[2] C. Medina, M. Zambrano, and K. Navarro, "LED Based Visible Light Communication: Technology, Applications and Challenges — A Survey," *Int'l. J. Advances Engineering Technology*, vol. 8, no. 4, 2015, pp. 482–95.
[3] N. Saha *et al.*, "Survey on Optical Camera Communications: Challenges and Opportunities," *IET Optoelectronics*, vol. 9, no. 5, 2015, pp. 172–83.
[4] Y. M. Jang, "IEEE 802.15 WPAN 15.7 Amendment — Optical Camera Communications Study Group (SG 7a)," 13 8 2016; http://www.ieee802.org/15/pub/SG7a.html, accessed 13 Aug. 2016.
[5] N. Le. and Y. M. Jang., "Performance Evaluation of MIMO Optical Camera Communications Based Rolling Shutter Image Sensor," *Proc. Eighth Int'l. Conf. Ubiquitous and Future Networks*, Vienna, Austria, 2016.
[6] W. A. Cahyadi, Y. H. Kim and Y. H. Chung, "Mobile Phone Camera-Based Indoor Visible Light Communications with Rotation Compensation," *IEEE Photonics J.*, vol. 8, no. 2, 2016, pp. 1–8.
[7] A. Sewaiwar, S. Tiwari and Y. H. Chung, "Visible Light Communication Based Motion Detection," *Optics Express*, vol. 23, no. 20, 2015, pp. 18,769–76.
[8] S. Tiwari, A. Sewaiwar, and Y. H. Chung, "Color Coded Multiple Access Scheme for Bidirectional Multiuser Visible Light Communications in Smart Home Technologies," *Optics Commun.*, vol. 353, 2015, pp. 1–5.
[9] S. Tiwari, A. Sewaiwar, and Y. H. Chung, "Optical Bidirectional Beacon Based Visible Light Communications," *Optics Express*, vol. 23, no. 20, 2015, pp. 26551–64.
[10] N. Lalithamani, "Gesture Control Using Single Camera for PC," *Proc. Int'l. Conf. Info. Security and Privacy*, Nagpur, India, 2015.
[11] D. H. Lee and Y. T. Park, "Vision-Based Remote Control System by Motion Detection and Open Finger Counting," *IEEE Trans. Consumer Electronics*, vol. 55, no. 4, 2009, pp. 2308–13.
[12] D. Ionescu *et al.*, "A New Infrared 3D Camera for Gesture Control," *IEEE Int'l. Instrumentation and Measurement Technology Conf.*, Minneapolis, MN, 2013.
[13] L. Hong and Q. Yueliang, "Detecting Persons Using Hough Circle Transform in Surveillance Video," *Proc. Int'l. Conf. Computer Vision Theory and Applications*, France, 2010.
[14] S. Shao *et al.*, "Design and Analysis of a Visible-Light-Communication Enhanced WiFi System.," *IEEE/OSA J. Optical Commun. Networking*, vol. 7, no. 10, 2015, pp. 960–73.
[15] S. C. Hoo *et al.*, "Deep Convolutional Neural Networks for Computer-Aided Detection: CNN Architectures, Dataset Characteristics and Transfer Learning," *IEEE Trans. Medical Imaging*, vol. 35, no. 5, pp. 1285-1298, 2016.

Biographies

Shivani Teli (telishivani27@gmail.com) is a graduate student in the Department of Information and Communications Engineering, Pukyong National University, Busan, Korea. She received her Bachelor's degree from Savitribai Phule Pune University, Maharashtra, India, in 2015. Her research interests are wireless communication systems, visible light communications, and optical camera communications.

Willy Anugrah Cahyadi (wac.zze@gmail.com) is a Ph.D. candidate in the Department of Information and Communications Engineering, Pukyong National University. He received his B.Sc. in electrical engineering and M.Sc. in microelectronics from Institut Teknologi Bandung, Indonesia, in 2008 and 2012, respectively. His research interests are visible light communications, optical camera communications, Internet of Things, and multimedia optical communications.

Yeon Ho Chung (yhchung@pknu.ac.kr) is a professor in the Department of Information and Communications Engineering, Pukyong National University. He obtained an MSc. from Imperial College London, United Kingdom, in 1992 and a Ph.D. from the University of Liverpool, United Kingdom, in 1996. He is a member of the Editorial Board of the *International Journal of Wireless Personal Communications*. He was a visiting professor at Pennsylvania State University, University Park, and also at Chiba University, Japan. He received the Top 2014 Paper Award from *Transactions on Emerging Telecommunications Technologies*. His research interests are visible light communications, wireless communication systems, massive MIMO, and advanced mobile transmission schemes.

Few-Mode Optical Fibers: Original Motivation and Recent Progress

Ken-ichi Kitayama and Nikolaos-Panteleimon Diamantopoulos

ABSTRACT

This article reviews the R&D activities in few-mode fibers, a special class of multimode optical fibers, beginning with its original motivation in the late 1970s, the operation principles, and the reason why research was discontinued in the mid-1980s. Preliminary characterizations of the test few-mode fiber fabricated for the first time are also introduced. Besides the earlier works, we review the progress of few-mode fibers after the resurgence of research in the 2010s on optical transmission and networking through mode-division multiplexing and other emerging applications. Recent revisiting of few-mode fibers is totally different from the original motivation, and it is mainly to solve the capacity crunch problem of optical fiber transmissions using legacy single-mode fibers. We address difficult challenges current research on mode-division multiplexing is facing, including differential mode group delay, channel crosstalk due to mode coupling, and their compensation technique through multiple-input multiple-output electronic signal processing. We also address the general perspective of niche applications in the near future. Such a revisit of few-mode fibers after its invention more than 30 years ago deserves showcasing for those engaged in research and development today to show how all research can eventually prove to be important no matter if it finds practical usage for different purposes in the beginning or not, as well as how people can work out a certain problem in many different ways.

INTRODUCTION

The ultimate spectral efficiency of single-mode fibers (SMFs) is limited by fiber nonlinearity, the so-called nonlinear Shannon's limit [1]. In order to mitigate the forthcoming capacity crunch of current optical fiber links, there have been several approaches, including a highly phase-noise-managed optical frequency comb as the light source and an exotic hollow core fiber with ultra-low nonlinearity. Besides space-division multiplexing (SDM) using multicore fibers, mode-division multiplexing (MDM) could be another solution to the capacity crunch. In the context of MDM, few-mode optical fiber (FMF) or two-mode fiber,[1] a special class of multimode optical fibers (MMFs), has come back to light as the transmission medium for SDM. The difference between the MMF and the FMF is not only in the number of modes but also in the number of available data channels. FMF carries few guided modes up to a few tens, and each mode is treated as an individual data channel in the MDM. In contrast, the number of modes of a typical MMF is a few hundred, and all the modes combined serve as a single data channel in MMF transmission systems.

The first ever FMF was invented back in 1978 by two NTT laboratories independently [2]. The principal author of this article was one of the inventors. That time was the transition period from MMFs to SMFs to realize 400 Mb/s long-haul systems. It might be hard to imagine nowadays, but a common consensus was that low-loss splicing of SMFs was a big challenge.[2] The initial motivation for the FMF research was thus to enlarge the core radius by shifting from single-mode operation to the two-mode region, while nearly equivalent transmission capacity to SMF is maintained by carefully setting the operating V-value[3] where the differential mode group delay (DGD) between the two modes becomes zero. Note that the velocity of the pulse envelope, which determines the pulse distortion in a dispersive medium, is governed mainly by the mode dispersion in FMF and its derivative with respect to the frequency, the so-called mode group delay. As the DGD increases, the pulse envelope becomes broader.

However, the fusion-splicing loss of SMF rapidly went down to 0.1 dB in a year or so, and 400 Mb/s long-haul systems using SMF cables for the first time were commercialized in 1984 in Japan. Therefore, FMF lost its initial purpose and did not see the light of day, and it took about 35 years to see the current resurgence of FMF research. It is noteworthy that dating back from the 1980s/1990s to the present, MMF found versatile application not in long-haul transmission systems but in-house/building and short-reach communications such as inter- and intra-data centers. For example, the IEEE 802.3 Ethernet Working Group has standardized the specifications of MMFs for bit rates up to 400 Gb/s and reaches ranging 100–300 m. More details can be found on the home page of IEEE 802.3.

Optical transmission using FMF through MDM has been gaining attention in recent years. The total transmission capacity increase of FMF through MDM compared to SMF can ideally be as many times as the mode count. To date, heroic transmission experiments of up to 15 modes and over 1200 km have been demonstrated [3, 4]. However, difficult challenges remain, including

The authors review the R&D activities in few-mode fibers, a special class of multimode optical fibers, beginning with its original motivation in the late 1970s, the operation principles, and the reason why research was discontinued in the mid-1980s. They review the progress of few-mode fibers after the resurgence of research in 2010s on optical transmission and networking through the mode division multiplexing and other emerging applications.

[1] In our definition the two-mode fiber allows the propagation of the fundamental and first-order guided modes, while, the second and higher-order modes can propagate in the FMF. Hereafter, we restrict ourselves to use only "FMF" for the readers' convenience.

[2] The fusion splicing of SMFs requires fine three-dimensional positioning between two cores, and this was performed manually by optical power monitoring at the other fiber end. In contrast, current fusion splicing can be performed automatically without manual positioning.

[3] V-value is proportional to the product of core radius and the square root of relative refractive index difference between core and cladding, divided by the operation wavelength.

Ken-ichi Kitayama is with the Graduate School for the Creation of New Photonics Industries and the National Institute of Information and Communications Technology; Nikolaos-Panteleimon Diamantopoulos was with Osaka University and is currently with NTT Device Technology Laboratories.

Digital Object Identifier: 10.1109/MCOM.2017.1600876

Up to date, hero transmission experiments of up to 15 modes and over 1200 km have been demonstrated. However, difficult challenges remain, including the channel crosstalk due to the mode coupling, the pulse distortion due to large DGD, and their compensation technique through MIMO electronic signal processing.

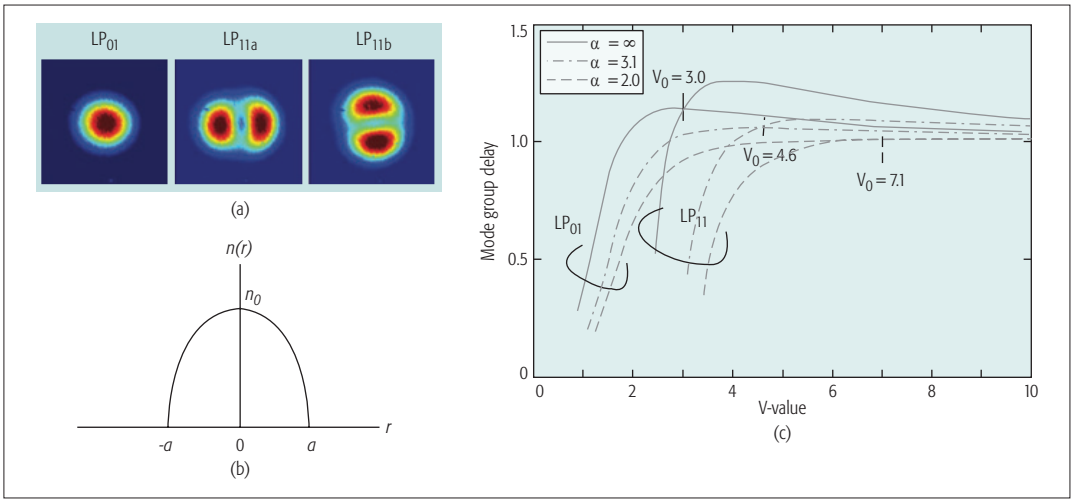


Figure 1. a) Mode field patterns of LP01, LP_{11a}, and LP_{11b} modes; b) graded-index profile; c) theoretical mode group delays of LP_{01} and LP_{11} modes for the step-index ($a = \infty$), and the parabolic graded-index profiles ($a = 2.0$ and $a = 3.1$).

channel crosstalk due to mode coupling, pulse distortion due to large DGD, and their compensation technique through multiple-input multiple-output (MIMO) electronic signal processing.

This article consists of two parts: the history of FMF and its present status. In the history part, we review the operation principle of original FMF and the major achievements of our theoretical and experimental studies, which may provide some clue for currently ongoing research relevant to FMF. In addition, preliminary characterizations of the test FMF fabricated in the early 1980s are presented, including the DGD property, the mode coupling in the fiber and at a splice point, and the DGD compensation technique of FMF links with positive and negative signs of DGDs. In the latter part, we introduce the current status of MDM transmission using FMFs, followed by the MDM network. Finally, we touch on emerging applications of FMF and give a general overview.

Fundamentals of Few-Mode Fiber

The Design Principle of Few-Mode Fiber

An initial motivation for FMF research was to enlarge the core radius by moving beyond the single-mode operation region into a few-mode region, maintaining a huge bandwidth equivalent to SMF. To this end, the design principles of the original FMF were the following:

- The first-order higher LP_{11} mode in the linearly polarized (LP) mode representation are allowed to propagate simultaneously with the fundamental LP_{01} mode. Hereafter, we use the LP representation for simplicity.
- DGD between the LP_{01} and LP_{11} modes are equalized at the V-value, V_0.
- V_0 is set just below the cutoff V-value, V_{c2}, of the second-order LP_{21} mode.

This FMF supports three LP modes, including the fundamental LP_{01} mode and two first-order LP_{11a} and LP_{11b} modes by taking into account the circular dependence (Fig. 1a). When the dual polarization is taken into account, the actual mode count is six.

Although it may not be practical to operate at $V = V_0$ where the mode group delays of the LP_{01} and LP_{11} modes are precisely equalized, it is imperative to maintain the DGD as small as possible even if there is a V-value offset from $V = V_0$. In a step-index profile, however, the DGD rapidly increases with the V-value offset from V_0 as shown by the dashed-dotted curve in Fig. 2. The key to yielding ample tolerance to the V-value offset was to adopt a graded-index profile. Assume that the refractive index profile has an -power law profile (Fig. 1b), given by

$$n(r) = \begin{cases} n_0\left[1-\Delta\left(\frac{r}{a}\right)^{\alpha}\right] (0 \le r \le a) \\ n_0(1-\Delta)(r > a) \end{cases} \quad (1)$$

where n_0, Δ, and a denote the index value at the core center, the relative index difference between the core and cladding, and the core radius, respectively. Note that the step-index profile is given by $\alpha = \infty$, while on the other hand, a parabolic profile is the case with $\alpha = 2$. Then a question arises as to what the optimum α value is. A rule of thumb is that as α value is decreasing, V_0 becomes larger. As a consequence, the largest V_0 in the two-mode region is obtained with the optimum value, $\alpha = 3.1$, where $V_0 = V_{c2} = 4.6$ as shown in Fig. 1c. For $\alpha < 3.1$ the third-order LP_{21} mode can propagate at $V = V_0$. By comparing $V_0 = 3.0$ for the case with the FMF having a step-index profile, the core diameter is enlarged by 53 percent. It should also be remembered that the core diameter can be enlarged to nearly twice as large as that of the step-index SMF with $V_{c2} = 2.4$.

Test Few-Mode Fibers and Their Characteristics

A fiber manufacturing company, Fujikura Ltd., prepared several test graded-index FMFs with a sophisticated index-profiling technique by a modified chemical vapor deposition (MCVD) process in the early 1980s, and the preliminary characterizations were completed [5]. Currently, there are several other fiber cable manufacturing companies, such as Corning, OFS, and Prysmian, that also provide high-quality FMFs. We briefly review the characteristics of the test FMF, particularly focusing on the DGD and the mode coupling, which are two of the main concerns of MDM transmission described hereafter.

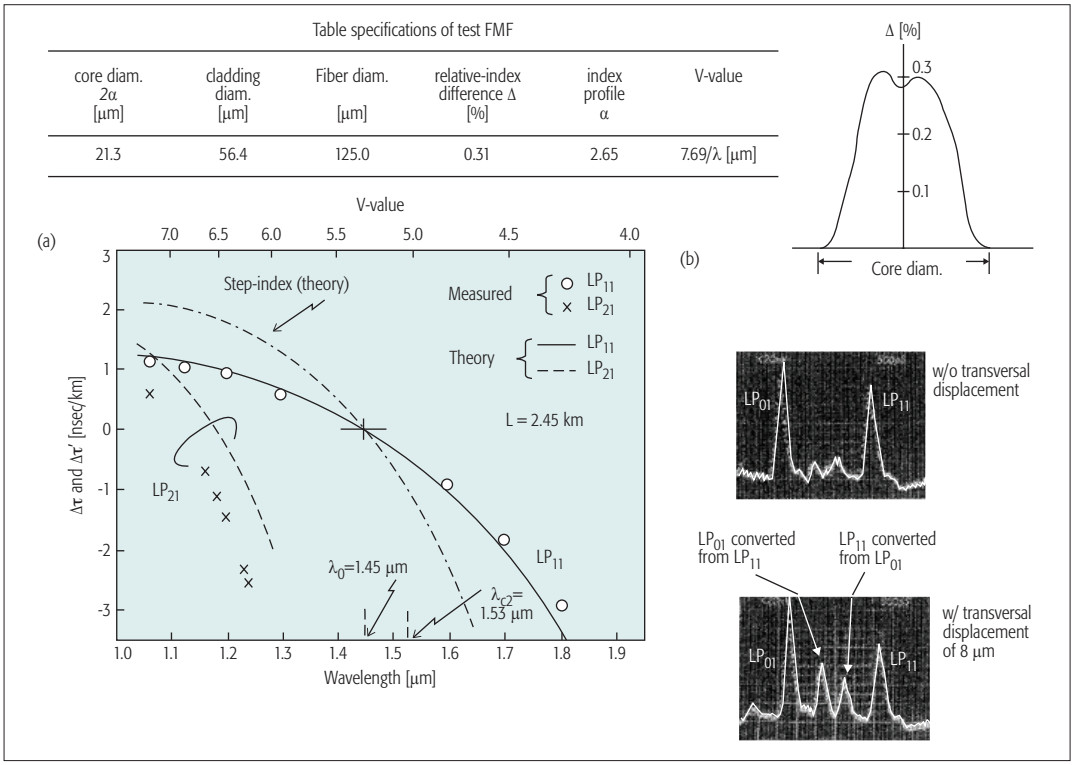


Figure 2. a) Measured and theoretical DGDs of the test FMF $\Delta\tau$ between LP_{01} and LP_{11} modes and $\Delta\tau'$ between LP_{11} and LP_{21} modes; b) pulse propagation in the FMF after a splice point without and with the transversal displacement of 8 μm (partly after [5, Fig. 4]).

As seen from the table of the test FMF specifications in Fig. 2, we have successfully attained the original purpose of the core diameter being 21 λm, almost double that of the SMF. The graded-index profile has a small central dip due to the nature of the MCVD process and the α value is 2.85, slightly deviated from the targeted 3.1. The fiber length was 2.45 km. The measured and theoretical DGD between the LP_{01} and LP_{11} modes as well as that between the LP_{01} and LP_{21} modes are plotted in Fig. 2. The measurements were conducted by using the short pulse propagation. The mode group delays of the LP_{01} mode and LP_{11} mode were equalized not at the targeted 1.55 μm but unintentionally at the wavelength λ_0 = 1.45 μm. The cutoff wavelength λ_{c2} of LP_{21} mode is 1.53 μm, slightly longer than λ_0 = 1.45 μm. The DGD caused by the wavelength offset (solid curves) in the vicinity of λ_0 is much smaller compared to that of an FMF having a step-index profile (dashed-dotted curve). For benchmarking, a typical DGD value between the LP_{01} and LP_{11} modes of the state-of-the-art FMF is 60 ps/km.

Mode coupling occurs both inside a fiber and at the splice point. Mode coupling has an impact on the DGD, and the DGD of the FMF link is proportional to the number of independent sections or the square root of the overall length in the strong-coupling regime [6]. The mode coupling in a fiber is a dynamic process that can be caused by intrinsic fiber imperfections (e.g., micro-bending, geometrical non-uniformity) as well as external factors including temperature/stress variations, macro-bending, vibrations, and so on, and eventually incurs radiation loss. Micobending particularly refers to a bend with a wide range of curvature, presumably induced by the stress in the nylon coating process and stranding in the cabling. We observed that the excess loss measured before and after the nylon coating of the test fiber was as small as 0.1 dB/km. There was no change before and after the nylon coating in the measured DGDs between the LP_{01} and LP_{11} modes and the one between the LP_{01} and LP_{21} modes. These observations are supporting evidence that there was small mode coupling inside the FMF. The state-of-the-art fiber manufacturing process of FMFs could further reduce the geometrical imperfections and excess loss due to microbending during the coating and cabling, resulting in weaker mode coupling. An imperfect fiber splice also induces mode coupling. In order to reduce mode coupling at a splice point, geometrical mismatches such as transverse displacement and tilt were carefully avoided in the experiment. As a result, the double-peak pulses of the LP_{01} and LP_{11} modes with equal amplitudes were obtained at the output of the fiber link without the transversal displacement Fig. 2, bottom). When the transverse displacement of 8 m at the splicing occurs, two additional peaks, arising from the energy exchange between LP01 and LP11 modes, are clearly seen between the double-peak pulses with higher amplitude.

To yield a low-DGD FMF link in a wide spectral range for wavelength-division multiplexing (WDM) transmission, the dispersion compensation by connecting FMFs having DGDs with opposite signs can be adopted [7]. As mode coupling gets stronger and/or the fiber link length becomes longer, the degree of DGD compensation diminishes. Note that in an MMF the mode coupling mitigates pulse broadening, leading to the aforementioned square root dependence on the distance. Recently, the DGD-compensated FMF link in the entire C+L-

Unlike in the 1980s and 1990s, when MMF was installed in offices/buildings for IEEE 802.3 Ethernet, this time around the scientific community proposed exploiting the orthogonality of each spatial mode for multiplexing, in addition to exploring the increasingly available MIMO electronic processing (e.g., in wireless communication systems).

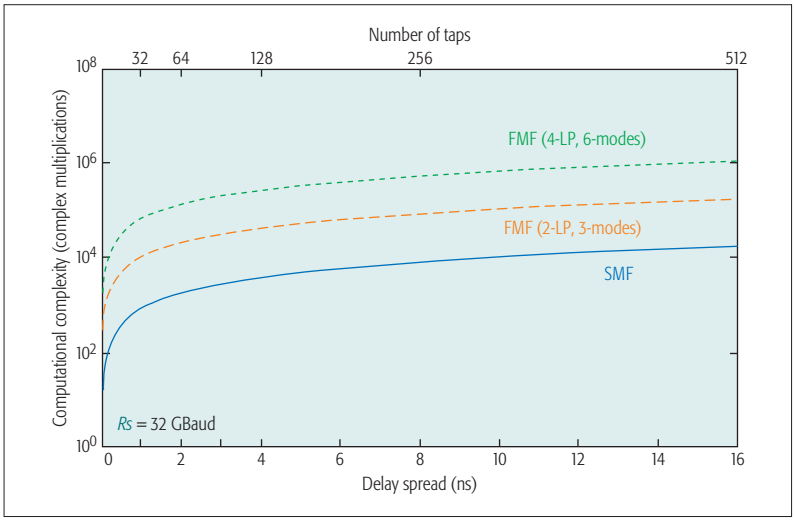


Figure 3. Computational complexity of MIMO electronic signal processing expressed in total complex multiplications for the dual-polarization SMF and 3- and 6-mode FMF cases. For the calculations, frequency domain equalization was considered as follows: $MN\log_2 M$ complex multiplications for FFT, M^2N complex multiplications for calculating channel matrices, M^3N complex multiplications for matrix inversions, and M^2N complex multiplications for matrix multiplications. M: number of spatial channels; N: number of taps. Sampling was considered to be 1 sample/symbol.

band has been experimentally demonstrated [8]. The DGD of a 102.6 km long link is below 1 ps/km in the C-band and below 4 ps/km in the C+L-band. This supports the observation that the mode coupling in a fiber and at a low-loss splice can be negligible within a practical fiber length.

Deploying Few-Mode Fibers for Mode-Division Multiplexing

Mode-Division Multiplexed Transmission

In recent years, research in the field of FMF has re-emerged, this time for the purpose of serving as a potential medium for spatial MIMO optical transmission [9]. By utilizing the spatial dimension in the optical fiber, different signals can be assigned to different propagating modes in an MDM scheme, capable of enhancing the capacity per fiber and eventually pushing the nonlinear Shannon limit upward [1] without depending on nonlinear compensation. So, unlike in the 1980s and 1990s, when MMF was installed in offices/buildings for IEEE 802.3 Ethernet, this time around the scientific community has proposed exploiting the orthogonality of each spatial mode for multiplexing, in addition to exploring the increasingly available MIMO electronic processing (e.g., in wireless communication systems).

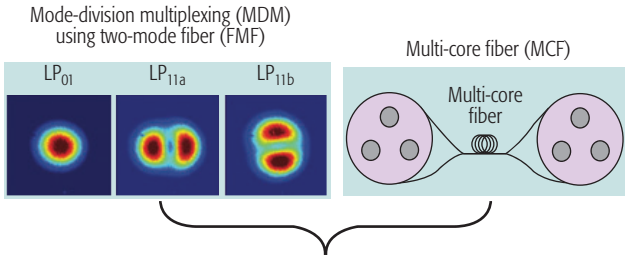
Developments of the enabling technology for MDM include mode-multiplexing/demultiplexing (mux/demux) devices, which allow the assignment of different signals from SMFs to FMF modes and vice versa. One of the most prominent technologies of this kind, due to its low-loss performance and small footprint, is the photonic lantern, a device that was originally inspired by applications in infrared astronomy [10]. A photonic lantern is composed of several SMFs placed inside a ferule, which is then tapered down to FMF size through a drawing process. For two-way operation, the number of SMF cables matches the number of modes of the FMF port.

One of the strong arguments on space multiplexing technologies such as MDM, compared to the deployment of parallel SMF systems, is the potential to decrease the energy consumption and cost of the overall system. The idea is that several energy-consuming elements that perform the same operation could be replaced by only a single energy-efficient element through spatial integration. An example is optical amplification using few-mode Erbium doped fiber amplifiers (FM-EDFAs). By using only a single FM-EDFA, all M modes inside the FMF are simultaneously amplified, saving the overall energy consumption for optical amplification by a factor of $1/M$. The first experimental demonstration of an MDM system employing FM-EDFA was done in [11], where 88 WDM channels in each of the three spatial modes of a two-LP-mode fiber were all amplified together by a single inline FM-EDFA.

MDM, as a form of optical MIMO transmission, inevitably induces crosstalk (XT) among different modes, arising from mode coupling. Such coupling is attributed to mode-multiplexing components, as well as fiber imperfections, as described in the previous section, and it is categorized as weak coupling or strong coupling according to its strength [6]. To compensate for the modal XT in an MDM system, MIMO electronic digital signal processing is required, usually employed at the receiver side. One important consideration is the feasibility of MIMO electronic processing for real-time implementation. It is known that the complexity of MIMO electronic processing depends on the number of modes and the number of filter taps required for electronic processing, and other factors [6]. Note that the latter is proportional to the total DGD of the system (Fig. 3). For feasible deployment of MDM, it is thus crucial to consider possible DGD compensation techniques, and to identify the relationship between mode coupling and DGD.

As briefly discussed in the previous section, there are three prominent approaches for DGD compensation. The first approach is based on refractive index profile engineering (e.g., graded index) for compensating DGD at a certain wavelength. The main disadvantage of this approach is that low DGD cannot be achieved for a wide spectrum operation and therefore is not suitable for WDM. The second approach is the management of DGD by using positive and negative DGD fiber spans in tandem [8]. This approach can support both low-DGD and wideband operation, but the effectiveness of the DGD compensation is affected by strong coupling events during propagation such as fiber splices. Today, the longest distance (1200 km) MDM/FMF transmission experiment ever recorded was based on this second approach [4]. Moreover, studies have shown that in the weak coupling regime, DGD is proportional to the fiber length , while in the strong coupling regime it is proportional to $\sqrt{L}$ [6]. Therefore, a third proposal is to support fiber transmission in the strong coupling regime for effectively reducing DGD.

Another merit of FMFs is their high intra-modal nonlinear tolerance, particularly for the higher-order modes due to their larger mode effective areas [12]. It should be noted, though, that this argument is generally valid when a single spatial



	Size	Splicing	Aeff	Fabrication	Opt. amp	MIMO el. proc.
MDM with FMF	= SMF	☺	> SMF	☺	☺	Needed
MCF	≠ SMF	☹	= SMF	☹	☹	Not needed

Table: Overview of MDM achievements and record transmission experiments in chronological order

Achievement	Year/ref.
Early FMF proposals, design, and fabrication	Late '70s, early '80s [6, 7]
Enabling devices for MDM (photonic lantern)	2005 [10]
First 6 × 6 MIMO transmission utilizing all 3-modes in a FMF	2011 [9]
First transmission demonstration using FM-EDFA	2011 [11]
Record 1200 km transmission over FMF	2012 [4]
Switching architectures for MDM	2015 [13, 14]
Transoceanic 6600 km quasi-single-mode transmission over an FMF	2015 [12]
30 × 30 MIMO over 15 modes, 9-LP FMF	2015 [3]

Figure 4. Capacity increase: Few-mode fiber vs. multi-core fiber and a summary of MDM achievements.

Even though there is an attempt to use FMFs for long-haul transmission, FMFs are unlikely to be used for MIMO transmission over long distances due to the complexity of the required MIMO electronic processing. However, FMFs are indeed promising for long-haul quasi-SM transmission.

mode is excited for transmission, also referred as quasi-single-mode (quasi-SM) transmission, but it is a much more complicated problem in the case of MDM where all modes are excited. That is because the aggregate effect of all the inter-modal nonlinear contributions can pose significant signal distortions, and the entire process is DGD dependent. However, considering that current SMF-based WDM transmission systems are limited by nonlinear interactions [1], using quasi-SM transmission over FMF is a promising solution for long-distance and high-capacity transmission. In such a case, mode multiplexing acts only as the means to excite and extract the signal to/from one of the modes and not as the means to assign different signals to different modes. In the first quasi-SM demonstration [12], the LP_{01} mode in an FMF was used to transmit a WDM signal over a total distance of 6600 km. Some of the record achievements and heroic transmission experiments of MDM since then are summarized in chronological order on the table on the right of Fig. 4.

It should be noted, however, that MDM is not the only approach to space multiplexing: there is also the multi-core fiber (MCF) approach,[4] as shown in Fig. 4. In the table on the left side of Fig. 4, the deployments of FMF and MCF are compared from various practical viewpoints. We treat here uncoupled core MCF. We leave out another type of MCF, so-called coupled-core MCF, although it has exhibited impressive performance, particularly in an ultra-long distance transmission systems. It would be interesting to compare the coupled-core MCF with the FMF, and this will be our forthcoming study. The dimension of the FMF cable is the same as the existing SMFs, but that of MCF will be larger depending on the number of cores. Meanwhile, the effective areas (Aeff) of the modes in an FMF are larger than those of SMFs and MCFs, providing higher nonlinear tolerance for quasi-SM transmission. Also, the splicing technique of MCF is still premature, while its fabrication cost is higher. In addition, the FM-EDFA is a straightforward extension of the SM-EDFA, but for the MCF case a complicated pumping scheme might be needed. In the FMF, however, the problem of the modal-XT remains, which requires the addition of MIMO electronic processing, the computational complexity of which might be a concern. The merits of FMF compared to MCF, however, are worth mentioning and, as discussed later on, there are several interesting applications that fit FMFs uniquely.

Mode Division Multiplexed Network

When considering an optical network that employs FMFs and MDM, it is important to address how the switching and the reconfigurable optical add/drop multiplexing (ROADM) operation should be [13, 14]. In the legacy SMF-based WDM optical networks, the WDM-ROADM architecture is employed using wavelength mux/demux, that is, wavelength-selective switches (WSSs), to add and drop individual wavelength channels. Since the optical networks that are expected to take advantage of MDM technology will also be based on legacy WDM technologies, the MDM-ROADM operation should be a straightforward extension of the WDM-ROADM, essentially forming a combined WDM/MDM-ROADM. A question therefore arises as to whether mode-mux/demux should be used along with the WSSs in order to add/drop individual spatial channels or not.

The current consensus is that, since modal-XT is unavoidable, signals in all modes should be propagated, switched, and eventually received together so that MIMO electronic processing is feasible at the receiver. "Spatial superchannels" can therefore be formed using what is usually referred as joint switching [13], in which the ROADM allows the add/drop of all the modes "jointly" (bundled together) in a certain wavelength. In such an approach, the flexibility in the spectral domain can still be maintained, but the spatial domain is restricted to a fixed networking operation.

On the other hand, the mode itself can provide an extra dimension as an identifier of the path, flow, and packet, along with the time slot, wavelength, and optical code identifiers. Therefore, for finer granularity than the spatially fixed

[4] A third approach obviously exists in which MDM is utilized by few-mode cores in MCFs, but this is simply a combination of the first two approaches and can be left out of the present discussion.

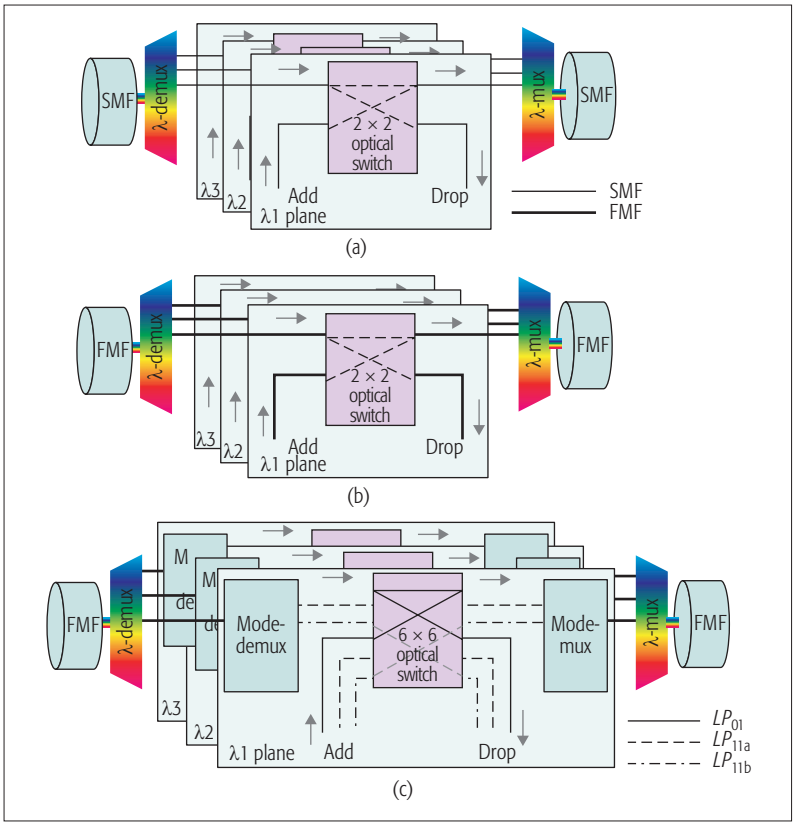


Figure 5. a) WDM-ROADM; b) joint-switched MDM-ROADM; c) mode-unbundled MDM-ROADM.

joint switching approach, the add/drop of individual spatial channels is preferred, that is, switching of individual modes, or rather, mode groups, that is, mode unbundling [14]. In such a case, the routing and mode path assignment (RMA) problem is treated in a similar manner to the well-known routing and wavelength path assignment (RWA) problem. Therefore, such a configuration would only increase the number of ports but not the complexity of the overall switching layer.

In Figs. 5b and 5c, the architectures of the MDM-ROADM of the joint switching and mode unbundling approaches are compared. For comparison, the SMF-based WDM-ROADM is depicted in Fig. 5a. For simplicity, the case with three modes and three wavelengths, λ_1, λ_2, and λ_3, are illustrated. Figure 5b illustrates add/dropping using 2 × 2 optical switches, while in Fig. 5c mode unbundling requires 6 × 6 optical switches. In the mode unbundling approach, however, the problem of modal XT still remains to be solved. Due to their always strongly coupled relationship [5], modes within the same mode group should be left out of this discussion and always be considered as remaining bundled. For modes at different mode groups, or rather switching of different mode groups, several approaches can be considered, for example, the use of low-XT FMFs, the use of bidirectional assignment of different mode groups [14], or approaches in the digital domain.[5]

Emerging Applications

Even though there is an attempt to use FMFs for long-haul transmission [4], FMFs are unlikely to be used for MIMO transmission over long distances due to the complexity of the required MIMO electronic processing [6]. However, as discussed above, FMFs are indeed promising for long-haul quasi-SM transmission [12].

On the other hand, a more realistic viewpoint is to consider FMFs for relatively short distance applications, in which the DGD and the complexity of the MIMO electronic processing, if required, is manageable. Particularly, FMFs can play a key role in advancing the capacity while minimizing the effort for cable management of metro area networks (MANs) [14] and data center networks, two types of networks that in recent years are experiencing tremendous traffic growth, only expected to rise further in the forthcoming years. Some initial effort has been put forth in these directions. In a preliminary demonstration, a 62 km ring utilizing FMFs was presented in [14].

As an example, in Fig. 6 the deployment of FMF is compared to the SMF case for MAN in terms of number of components for a 3× capacity increase scenario. The number of transmitters (Txs) and receivers (Rxs) in both cases are the same. A notable difference is in the optical amplifier. SMF requires three, but FMF requires only one. Also, the joint switching approach uses a single spatial switch in the ROADM, while the mode unbundling case uses as many switches as the mode count.

Finally, a very interesting emerging application of FMFs is in the area of optical sensing. The addition to the space dimension, and particularly in light of the fact that different modes have different propagation properties (propagation constants, nonlinear coefficients, etc.), allow FMFs to be a multi-sensor of several properties simultaneously, within a very small footprint. The field has gained increasing interest in R&D over the last few years. Notably, the authors in [15] have successfully demonstrated simultaneous stress and temperature sensing using different modes in an FMF. In addition, it is worth noting that there has been a demonstration of few-mode waveguides integrated with MDM mux/demux devices based on silicon photonics. Such a photonic integrated scheme is promising for scaling the transmission capacity of on-chip optical communications because it allows energy- and cost-efficient single-wavelength laser to be utilized without using a multi-wavelength laser array.

General Perspective

The re-emergence of FMF research, sparked by the need for higher capacity over a single fiber, and the enabling technology of MDM have ignited a promising new era for FMFs and optical communications in general. Initially abandoned research has come back to light with a new purpose, marking breakthroughs in the field of optical transmission ever since, as summarized in the table on the right side of Fig. 4. To further promote the research on MDM toward new emerging applications, it is worth mentioning our hopefully not over-optimistic perspective.

Based on various surveys and white papers, the compound annual growth rate (CAGR) of the transmission capacity in metro and DC traffic continue to be nearly 60 percent for a few years, while the CAGR of WDM transmission system capacity stays at roughly 20 percent. There is a common consensus that SDM, an additional parallel dimension in optical transmission, is one of the solutions

[5] Several approaches to this problem have been presented, mainly in the field of wireless-MIMO transmission, but they are left out of the discussion here.

to fill this gap in CAGRs. As far as the MDM is concerned, the need for MIMO electronic processing is crucial, and therefore, its success heavily relies on complementary metal oxide semiconductor (CMOS)-based electronic processing. Moore's law, an empirical trend of electronic device integration, is claimed to be reaching its end. Nevertheless, we still see a good prospect for post-Moore technologies such as "More Moore," "More than Moore," and "Beyond CMOS," which will eventually enable MIMO electronic processing of high computational complexity, freed from the constraints of the distance as well as the mode count in the MDM transmission of practical use cases.Hence, even though the perspective of FMF is still unclear in terms of whether it eventually finds practical applications, its long history and the fruitful physics it incorporates seem to highlight a brighter future.

Summary

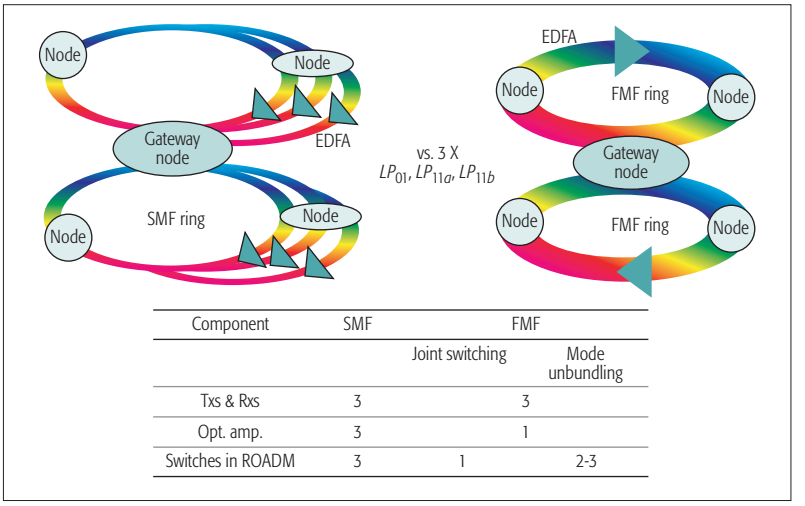
In the first part, the operation principle of FMF invented in the late 1970s has been reviewed. The FMF was originally developed to ease the difficulty in splicing SMFs by almost doubling the core diameter of the SMF. The characteristics of the DGD and the mode coupling of the test graded-index FMF having nearly optimum structural parameters have been presented. In the second part, the revisit of FMFs for MDM transmission has been reviewed, while the MDM network operation and the emerging applications have been discussed. This revisit of the FMF after its invention more than 30 years ago deserves showcasing for those engaged in research and development today, on how every research study can prove to be important eventually, no matter if it has found practical use cases for different purposes from the beginning or not.

Acknowledgments

The authors would like to thank R. Maruyama, N. Kuwaki, S. Matsuo, K. Aikawa, and K. Nishide of the Advanced Technology Laboratory, Fujikura Ltd., for their invaluable discussion and for providing us with test FMFs. The authors would also like to thank Y. Yoshida of NICT, and A. Maruta and T. Isoda of Osaka University for their invaluable comments and providing the numerical simulations. This work has been partly supported by the R&D project "Agile Deployment Capability of Highly Resilient Optical and Radio Seamless Communication Systems," funded by the National Institute of Information and Communications Technology (NICT), Japan.

References

[1] P. P. Mitra and J. B. Stark, "Nonlinear Limits to the Information Capacity of Optical Fibre Communications," *Nature*, vol. 411, June 2001, pp. 1027–30.
[2] J. Sakai *et al.*, "Design Considerations of Broadband Dual-Mode Optical Fibers," *IEEE Trans. Microwave Theory Technol.*, vol. 26, no. 9, Sept. 1978, pp. 658–65.
[3] N. K. Fontaine *et al.*, "30 × 30 MIMO Transmission over 15 Spatial Modes," *Proc. OFC 2015*, Th5C.1, Los Angeles, CA, Mar. 22–26, 2015.
[4] S. Randel *et al.*, "Mode-Multiplexed 620-GBd QPSK Transmission over 1200 km DGD-Compensated Few-Mode Fiber," *Proc. OFC/NFOEC 2012*, PDP5C.5, Los Angeles, CA, Mar. 4–8, 2012.
[5] A. O. Arik, K.-P. Ho, and J. M. Kahn, "Group Delay Management and Multiinput Multioutput Signal Processing in Mode-Division Multiplexing Systems," *J. Lightwave Technol.*, vol. 34, no. 11, June 2016, pp. 2867–80.



Component	SMF	FMF	
		Joint switching	Mode unbundling
Txs & Rxs	3	3	
Opt. amp.	3	1	
Switches in ROADM	3	1	2-3

Figure 6. Deployment for the capacity increase in MAN: single-mode fiber vs. few-mode fiber.

[6] K. Kitayama *et al.*, "Structural Optimization for Two-Mode Fiber: Theory and Experiment," *IEEE J. Quantum Electron.*, vol. 17, no. 6, June 1981, pp. 1057–63.
[7] Y. Kato *et al.*, "Modal Equalization for Two-Mode Fibre Link Using a Step-Index Fibre," *Electron. Lett.*, vol. 18, no. 9, Apr. 1982, pp. 356–58.
[8] R. Maruyama *et al.*, "Two Mode Optical Fibers with Low and Flattened Differential Modal Delay Suitable for WDM-MIMO Combined System," *Opt. Express*, vol 22, no. 12, June 2014, pp. 14,311–21.
[9] R. Ryf *et al.*, "Space-Division Multiplexing over 10 km of Three-Mode Fiber Using Coherent 6 6 MIMO Processing," *Proc. OFC/NFOEC 2011*, PDPB10, Los Angeles, CA, Mar. 6–10, 2011.
[10] S. G. Leon-Saval *et al.*, "Multimode Fiber Devices with Single-Mode Performance," *Opt. Lett.*, vol. 30, no. 19, Oct. 2005, pp. 2545–47.
[11] E. Ip *et al.*, "883112-Gb/s WDM Transmission over 50 km of Three-Mode Fiber with Inline Few-Mode Fiber Amplifier," *Proc. ECOC 2011*, Th.13.C.2, Geneva, Switzerland, Sept. 18–22, 2011.
[12] F. Yaman *et al.*, "First Quasi-Single-Mode Transmission over Transoceanic Distance using Few-Mode Fibers," *Proc. OFC 2015*, Th5C.7, Los Angeles, CA, Mar. 22–26, 2015.
[13] D. M. Marom *et al.*, "Wavelength-Selective Switch with Direct Few Mode Fiber Integration," *Opt. Express*, vol. 23, no. 5, Feb. 2015, pp. 5723–37.
[14] N. P. Diamantopoulos *et al.*, "Mode-Unbundled ROADM and Bidirectional Mode Assignment for MDM Metro Area Networks," *J. Lightwave Technol.*, vol. 33, no. 24, Dec. 2015, pp. 5055–61.
[15] A. Li *et al.*, "Few-Mode Fiber Based Optical Sensors," *Opt. Express*, vol. 23, no. 2, Jan. 2015, pp. 1139–50.

Biographies

Ken-ichi Kitayama [LF'16] (kitayama@gpi.ac.jp) received his M.S in 1974 and Ph.D in 1981 from Osaka University, Japan. He joined NTT Laboratory in 1976. In 1995, he joined CRL (presently, NICT), Japan.In 1999, he became a professor at Osaka University. Since April 2016 he is a Professor Emeritus of Osaka University, and a Project Professor at the Graduate School for the Creation of New Photonics Industries, Hamamatsu, Japan. He also serves as an R&D adviser of NICT, Tokyo. He has published more than 310 journal papers and a book, *Optical Code Division Multiple Access — Fundamentals and Practical Perspective*.

Nikolaos-Panteleimon Diamantopoulos (n.p.diamantop@gmail.com) received his B.Sc. degree from the University of Peloponnese, Greece, in 2009, his double M.Sc. degree from Aston University, United Kingdom, and Scuola Superiore Sant'Anna Pisa, Italy, in 2012, and his Ph.D. degree in information and communications technology from Osaka University in 2016. Also, throughout his career he has worked on several EU R&D projects at Athens Information Technology, Greece. Currently he is a research associate at NTT Device Technology Laboratories, Japan.

YANG Models for Vendor-Neutral Optical Networks, Reconfigurable through State Machine

Matteo Dallaglio, Nicola Sambo, Filippo Cugini, and Piero Castoldi

Multi-vendor interoperability can be achieved at node and network levels by relying on standard data modeling. YANG represents an attractive data modeling solution for network component definition. This article reports on the work done on YANG models for optical networks with particular reference to flexible-grid networks.

Multi-vendor interoperability can be achieved at node and network levels by relying on standard data modeling. YANG represents an attractive data modeling solution for network component definition. This article reports on the work done on YANG models for optical networks with particular reference to flexible-grid networks.

ABSTRACT

Multi-vendor interoperability can be achieved at node and network levels by relying on standard data modeling. YANG represents an attractive data modeling solution for network component definition. This article reports on the work done on YANG models for optical networks with particular reference to flexible-grid networks. In addition to a YANG model description for link, node, and media channels, YANG for a sliceable transponder is introduced given the importance of such a data plane device for the next generation backbone. Then a contribution is provided in proposing YANG models for events and state machine to further extend and increase the programmability of networks. This latter contribution is particularly relevant in the case of faults or physical layer degradation in a network. Finally, YANG models are validated in an experimental control plane testbed.

INTRODUCTION

Recently, network operators have shown interest in the deployment of data plane hardware providing multi-vendor interoperability [1]. This way, operators can use systems of different vendors optimizing transmission performance (e.g., achievable transmission distance), network device reuse, and capital expenditure without the need for being tied to single-vendor equipment. Multi-vendor operability can be applied in two different contexts: network and node. In the former, a network composed of nodes provided by different vendors is operated under the same control system (e.g., elastic black links [1]). In the latter, a node composed of components provided by different vendors is assembled under the same control system. This has brought about the concept of *white boxes*. With respect to *black boxes* provided by a single vendor, white boxes are assembled with different vendors' components (i.e., disaggregated hardware).

To support control and management of multi-vendor networks and white boxes, standard operator-defined data models are required so that common application programming interfaces (APIs) can be adopted for controlling/managing these multi-vendor optical systems [2].

A key candidate language to describe a standard-defined data model is the emerging Yet Another Next Generation (YANG) [3–5]. Regarding flexible/elastic optical networks [6, 7], which are the focus of this article, some recent works have provided YANG models to describe basic attributes of links (e.g., identification), nodes (e.g., connectivity matrix), media channels, and transponders (e.g., supported forward error correction, FEC) [4, 8–10].

However, effort is still required to achieve detailed models of optical devices and their functionalities to increase the level of programmability of networks. As an example, some actions have to be taken on data plane devices when events such as soft failures (i.e., performance degradation implying bit error rate [BER] increase) occur; for example, transmission should be consequently switched to a more robust modulation format [11]. Typically, actions upon failure or degradations imply either manual intervention or the involvement of a centralized controller. In the latter case, when the controller is first notified of the soft-failure event, it makes a decision and configures the involved network devices accordingly (such method requires certain time). Alternatively, the device is programmed at the moment of the installation to take an action or a reconfiguration after a specific event occurs. Currently, no YANG model has been defined to allow the controller to (re)configure events, actions, and state machine or functions on a generic network device.

In this article, we first introduce the YANG modeling language and the YANG-related works done in the field of optical networks (in particular, elastic optical networks). Then a model for the sliceable transponder is detailed. Furthermore, we propose and demonstrate the enhancement of YANG to model events and functions that can be executed in an ordered way through a finite state machine (FSM). The latter models enable a remote controller (on behalf of a network operator) to instruct a device controller about critical events and actions to be taken if these events occur. The actions to be taken and the critical events can be re-programmed on the device by simply sending a new message configuration on the device local controller with the new information.

YANG LANGUAGE

YANG [3] is a data modeling language standardized by the Internet Engineering Task Force (IETF). It has been developed in the context of NETCONF [12], a protocol standardized as

Digital Object Identifier:
10.1109/MCOM.2017.1600733

Matteo Dallaglio, Nicola Sambo, and Piero Castoldi are with Scuola Superiore Sant'Anna; Filippo Cugini is with CNIT.

an answer to specific requirements of the IETF [5]: developing standards for network configuration and management, and using XML for data encoding. Thus, NETCONF is a protocol for the configuration and management of network devices that operates on data encoded in XML. YANG has been developed and standardized as a language to model data into NETCONF messages. In particular, a YANG module can be translated into an XML representation called YIN. For this reason, commonly used XML tools can be adopted to process YANG data models, making YANG suitable for NETCONF. Thus, one of the main advantages of YANG is the XML representation, which makes YANG also adoptable by other protocols (e.g., RESTCONF) besides NETCONF. As stated in the introduction, in the last years the interest of operators in YANG has grown because of the possibility to standardize common models for configuration and management data in a vendor-neutral way. However, such models should be the synthesis of a trade-off between different vendors. This could represent a key limitation of YANG and NETCONF, since it may result in complex common models and in a time-consuming standardization process. In this context, YANG also supports "deviations" from the common model to enable a vendor to adopt small variations with respect to the original model. YANG can be hierarchically represented in a tree structure with a root and leaves.

Figure 1 shows an example of a generic YANG model and the resulting tree organization: root and leaves have names, data types, data values, and child leaves. For example, YANG defines data types as 16-bit unsigned integers (as "data-1," line 14 in Fig. 1a) or 64-bit signed decimal (as "data-2," line 18), and others [3]. New data types can be also defined. In Fig. 1a, "data-3" is of "NEW-TYPE" type. In the example, the new type can assume just three values (lines 5–12). YANG also includes the definition of lists. The "key" of a list is used to specify one or more leaves in a list that will uniquely identify an element (data instance) of the list. The example in Fig. 1a shows the model "example" composed of four leaves (each leaf is defined with the syntax "leaf," e.g., line 13): "data-1," "data-2," "data-3," and a list (line 27). Each piece of this data is associated with a type. A list is initiated with the command "list" (line 27), and the data of a list can have child leaves as "leaf-data-1" and "leaf-data-2." The resulting tree, obtained with the Pyang software [9], is visualized in Fig. 1b with "example" as the root; "data-1," "data-2," "data-3," and the list as leaves; and "leaf-data-1" and "leaf-data-2" as the leaves of each element in the list.

YANG data can be of two types: *configuration* or *state*. Configuration data is explicitly set by an external entity from the system (e.g., the centralized controller). State data cannot be set by the external entity, but they can be read. State data can be used for monitoring purposes. A further layer in the hierarchy indicating the list of configuration and state data can be defined, as detailed later. YANG also supports the definition of "Notification" to model the content of NETCONF Notification messages, which indicate that certain events have been recognized (e.g., a failed link). Moreover, although YANG is mostly considered as a data modeling language, it also provides the possibility to define executable functions through remote procedure calls (RPCs) that specify the name, the input, and the output parameters of a specific function, for example, switching on (off) a device inside a node. For further information the reader is referred to [3].

(a)

```
1.  module example {
2.      namespace "sssup:example";
3.  prefix example ;
4.
5.  typedef NEW-TYPE{
6.      type enumeration {
7.          enum type-one;
8.          enum type-two;
9.          enum type-three;
10.     }
11. }
12.
13. leaf data-1 {
14.     type uint16 ;
15. }
16.
17. leaf data-2 {
18.     type decimal64 {
19.             fraction-digits 18;
20.     }
21. }
22.
23. leaf data-3 {
24.     type NEW-TYPE ;
25. }
26.
27. list element-of-a-list {
28.     key "leaf-data-1";
29.     leaf leaf-data-1 {
30.         type uint16;
31.     }
32.     leaf leaf-data-2 {
33.         type uint16;
34.     }
35.  }
36. }
```

(b)

```
module: example
    +--rw data-1?                uint16
    +--rw data-2?                decima164
    +--rw data-3?                NEW-TYPE
    +--rw element-of-a-list      [leaf-data-1]
        +--rw leaf-data-1        uint16
        +--rw leaf-data-2?       uint16
```

Figure 1. a) Example of YANG code; b) resulting tree.

Then some considerations are here reported on the nature of YANG. First, it is a highly readable text language. This significantly simplifies management and troubleshooting operations compared to protocols relying on bit encoding, which require ad hoc software to parse encoded information. Nowadays, handling a text file instead of bit encoding does not represent a particular challenge. Moreover, in the case of bit encoding, the support of novel parameters at the data plane would imply redesigning the protocol messages' content, such as header and

YANG data can be of two types: configuration or state. Configuration data is explicitly set by an external entity from the system. State data cannot be set by the external entity but they can be read. State data can be used for monitoring purposes. A further layer in the hierarchy indicating the list of configuration and state data can be defined.

Thanks to the nature of YANG, when the model changes, the YANG model can be refined without redesigning the protocol, thus providing a much more effective solution with respect to bit encoding. Such an example has to be considered relevant given the continuous evolution of the technology at the data plane.

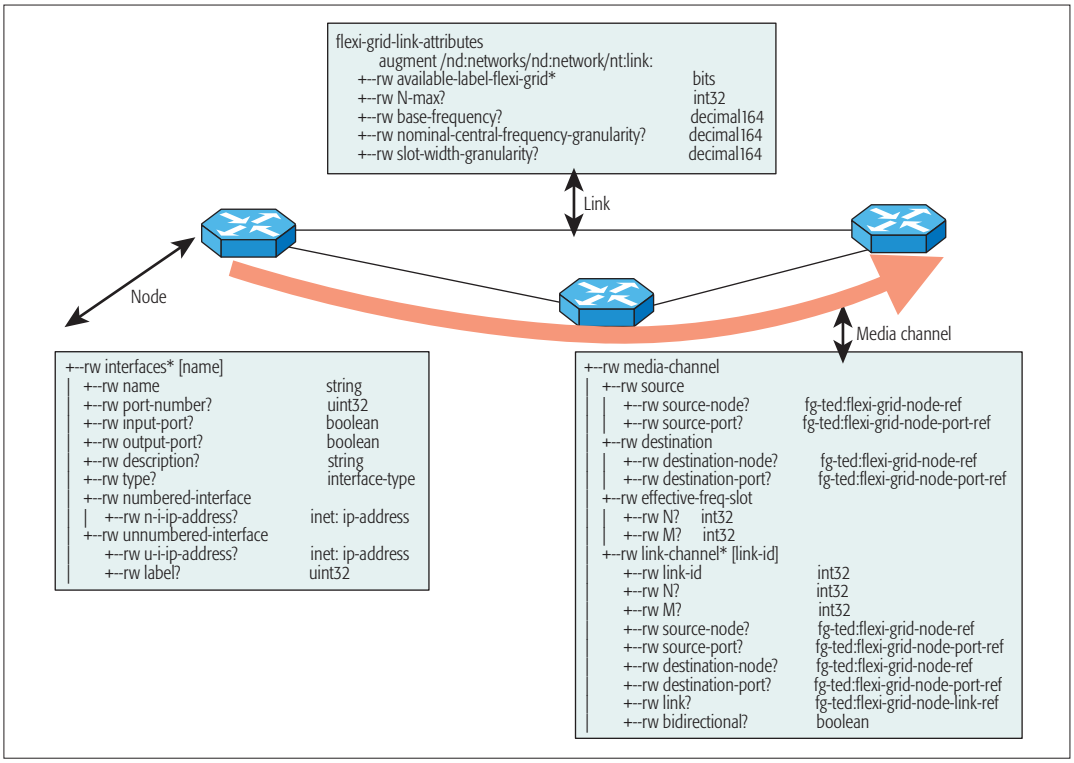


Figure 2. Portions of a YANG tree representation of flexible optical networks as proposed by [4]: node, link, and media channel.

objects. On the contrary, thanks to the nature of YANG, when the model changes, the YANG model can be refined without redesigning the protocol, thus providing a much more effective solution with respect to bit encoding. Such an example has to be considered relevant given the continuous evolution of the technology at the data plane.

In the context of optical networks, several standardization bodies and working groups (e.g., IETF, OpenConfig, OpenROADM) have released YANG models. As an example, the IETF draft in [13] defines a YANG model for representing, retrieving, and manipulating traffic engineering (TE) topologies supporting optical switching nodes. OpenROADM has recently defined YANG models focused on reconfigurable optical add/drop multiplexer (ROADM) disaggregation. These models describe how different pluggable devices for optical networks (e.g., amplifiers, transponders) can be interconnected. However, more details on the transponder parameters (e.g., chromatic dispersion, polarization mode dispersion, analog bandwidth) could be provided. OpenConfig aims to provide a set of vendor-neutral data models based on network operator requirements. In particular, OpenConfig released preliminary models on optical amplifiers, ROADMs, and transponders. The OpenConfig model does not consider disaggregation as OpenROADM does, while the transponder model is more accurate with respect to OpenROADM but still lacks some parameters (e.g., sampling rate, analog bandwidth) and does not define any Notification that can be very relevant for monitoring purposes [8].

In the next section, YANG models for flexible (or elastic) optical networks are introduced.

YANG Model for Elastic Optical Networks

Elastic optical networks (EONs) are circuit-switched optical networks equipped with flexible-grid spectrum selective switches (SSSs) [11]. SSSs enable switching of the configurable portion of the bandwidth, depending on the bandwidth required by the circuit or *media channel* (e.g., by fixing the modulation format, a high-rate connection requires more bandwidth than a lower-rate connection). The media channel is defined as a specific portion of the optical spectrum along an optical path between a source and a destination node [11]. For EONs, International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) G.694.1 states that a media channel occupies a portion of spectrum called *frequency slot*, defined by two parameters: the *central frequency* and the *width* of the occupied spectrum portion. According to this ITU-T specification, the central frequency can assume values in steps of 6.25 GHz, while the width has to be a multiple of 12.5 GHz. In [4], the authors have been focused on the representation of the flexi-grid optical layer dividing the model into two modules: one related to the TE database (TED) and the other one representing the *media channel*. The TED module defines the information required to represent nodes, links, transponders, and spectrum resources. Portions of the trees of these sub-modules are shown in Fig. 2.

The sub-module of the transponder, being more complex, is detailed in the next section. The "interfaces" leaf of the node sub-module is a list containing all the interfaces in the node. Each element of this leaf has several sub-leaves defining attributes of the considered interface (or port),

such as the name, the number, two Boolean variables indicating if it is an input or an output port, and the IP address if present. The model also includes the "connectivity matrix" (not shown in the figure): a list of connected input/output ports in the node. Additional information may be added. This model can be further augmented by including information on the add/drop part of the node, in particular, to define the reachability of an add port (or a drop port) to an output interface (or an input interface). More information on add/drop is included in the YANG model in [10].

The link sub-module consists of five leaves: the availability of flex-grid technology for that link, the maximum value *N* of slices supported by that link (i.e., slices of 12.5 GHz), the nominal central frequency for the link, the spacing among channels' central frequency (i.e., 6.25 GHz), and the slot width granularity (i.e., 12.5 GHz). The media channel sub-module consists of four main leaves: the source and destination nodes of the media channel, the frequency slot, and a list of traversed links. Both source and destination nodes include two leaves: one defining a reference to the module of the node (i.e., the tree of Fig. 2) and the other one related to the used interface (port) in such a node. This model can be further augmented including a reference to the transponder used by the media channel, the used add/drop port, and also information on the adopted transmission technique (e.g., Nyquist wavelength-division multiplexing, NWDM).

Sliceable Transponder

A sliceable transponder is a transponder generating multiple independent optical flows that can be directed toward different destinations [11]. A reference architecture agreed on among several vendors and operators has been proposed in [11]. In this article, we mainly refer to the transponder model in [9], which reports a comprehensive set of physical parameters with a particular reference to state data that can be used for monitoring purposes. In [9], the authors enhanced the YANG model for the sliceable transponder by leveraging on the one presented in [4]. In particular, more physical data has been included in the YANG model (e.g., baud rate, output power at the transmitter side, the local oscillator and the analog bandwidth at the receiver, monitoring parameters that are detailed in this section, and a reference to the media channels using the transponder). Moreover, a classification on the configurable and state data is provided. This YANG model reflects the transponder architecture of [11]. The transponder is composed of a set of subcarrier modules. Each subcarrier module is devoted to generating (at the transmitter side) or detecting (at the receiver side) an optical subcarrier. Similarly, the YANG model is organized per subcarrier module. The related tree is shown in Fig. 3. First, a Boolean data indicates if slice-ability is supported or not. Then a list of subcarriers' sub-modules is modeled. As configuration data, different data are present if the "direction" is in transmission or detection (e.g., local oscillator configuration if the module is in detection). Other data has to be specified in both transmission and detection: for example, baud rate, bit rate, modulation format, FEC. Note that we defined the type "frequency-ghz-type" to discern between the central frequency of a subcarrier and that of a media channel. Indeed, while the central frequency of a media channel has to follow ITU-T specifications in steps of 6.25 GHz, and thus can be expressed as just an integer number, the central frequency of a subcarrier of a media channel composed of several subcarriers does not necessary follow a grid [11]. Thus, the central frequency of a subcarrier can be any number. For this reason, we defined the type "frequency-ghz-type" to express the frequency value in "GHz." Regarding state data, first, configuration data is replicated into state data to enable an operator to verify ("read") the actual configuration of the transponder. Then other data is included in the model, mainly related to the monitoring capabilities of coherent detection. Indeed, thanks to the digital signal processing (DSP) at the receiver, it is possible to monitor end-to-end parameters associated with each subcarrier [11]. As an example, monitored parameters can be pre-FEC BER, Q-factor, chromatic dispersion (CD), and polarization mode dispersion (PMD), all expressed as decimal64. Other leaves of the subcarrier module comprise (not shown in the figure) the identification of the node and of the add/drop module, and a list of media channels that are using such a transponder. Finally, different from the representation in [4], the "transmission scheme" is included to identify the adopted transmission technique. For that, a new type is defined including NWDM, orthogonal frequency-division multiplexing (OFDM), and others. The full code of this model can be retrieved from [14].

Events and State Machine

A sliceable transponder can be reconfigured when some events occur [15]: for example, degradations of the physical layer due to aging may imply an increase of the pre-FEC BER. Such an event can be overcome by making the transmission more robust (e.g., by changing the modulation format or the FEC). This section is devoted to model events, actions, and FSMs. Such models are proposed to enable a remote controller (on behalf of a network operator) to instruct a device controller about critical events and actions to be taken if this event occurs. The actions to be taken and the critical events can be reprogrammed on the device by simply resending a new message configuration (e.g., through the NETCONF protocol, as detailed in the next section) on the device controller with the new information. Such a system has the prospect to speed up the reaction of the network to certain events/faults and to alleviate, in a standard way, the workload of the centralized controller. The speedup derives from the fact that the centralized controller is able to pre-configure, on the network devices, the actions to take when an event occurs. In this way, the device already knows what to do and can immediately react, avoiding informing the controller and waiting for the response indicating what to do. Consequently, part of the workload is also removed from the centralized controller, which can instruct the device once, transferring to it some intelligence to make decisions autonomously. When the reaction is successfully completed in the data plane, the centralized controller can be notified about the faults and the action taken.

In the context of optical networks, several standardization bodies and working groups (e.g., IETF, OpenConfig, OpenROADM) have released YANG models..

The use of YANG and, in particular, finding common models for events and transceiver actions/functions can be considered of relevance because of two main trends: network operators looking for common vendor-neutral solutions; and developing transponders supporting multiple transmission parameters and monitoring capabilities.

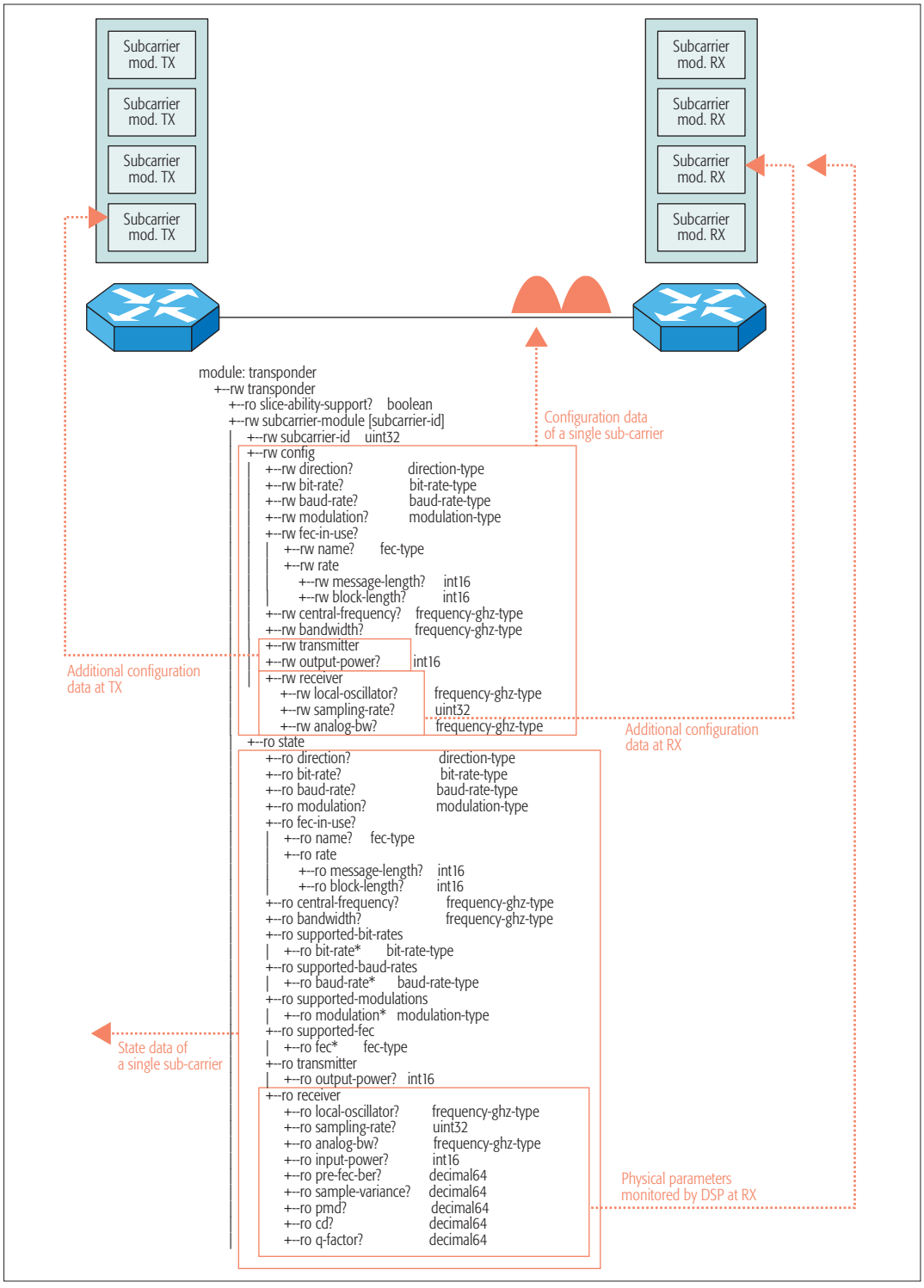


Figure 3. YANG tree representation of a sliceable transponder.

The use of YANG and, in particular, finding common models for events and transceiver actions/functions can be considered relevant because of two main trends: network operators looking for common vendor-neutral solutions; and developing transponders supporting multiple transmission parameters (e.g., bit rate, coding, modulation format, baud rate) and monitoring capabilities. Moreover, several activities of operators and vendors are evaluating the reduction of network margins [15] (i.e., worst-case margins for aging and transmission modeling inaccuracy), for example, to decrease the number of opto-electronic converters. This will cause networks to suffer more from changes in the physical layer (e.g., due to events such as soft failures), thus increasing the needs of devices supporting transmission adaptation (e.g., to increase robustness).

The proposed YANG model, schematized with the tree diagram of Fig. 4a, describes events (e.g., soft failures) and functions (e.g., baud rate and code change) to be executed in an ordered way following

an FSM. The model defines a list of events as the root of the hierarchy. An event is defined through two mandatory attributes ("name" and "type") and an optional attribute ("description"). Together, "name" and "type" attributes uniquely identify the event. The "type" attribute takes its value from a pool of possible event types predefined inside the YANG model. Currently, we have defined some known event types such as the "ON CHANGE" event to describe the change of an attribute value. Given that the change of an attribute does not necessarily mean a particular degradation or fault, we included in the model the sub-leaf "filter," which can be used to define a threshold to further characterize the event. For example, by referring to the "Q-factor" state data in Fig. 3, we may define an event named Q-factor change of type "ON CHANGE" and, as a filter, a threshold to indicate when the Q-factor falls below the threshold. Another leaf of the "event" is the "reaction." In particular, for each event, the controller can configure a reaction the device should have. The "reaction" is composed of a list of "operations" to perform when the event occurs. Each operation is identified through an "id" and can be either of types "simple" or "conditional." A "simple" operation contains the "execute" attribute that, recalling an RPC (as shown in the next section), is used to encapsulate the effective task to be executed and the "id" of the "next operation" (if any). A "conditional" operation, with respect to the "simple" one, contains in addition a "statement" attribute that can be "true" or "false" (related flow chart shown in Fig. 4b). The statement is checked at the beginning of the operation; then, depending on the outcome (true or false), only the correct operation is considered. "True" and "false" contain the "execute" and "next operation" as for the "simple" operation.

It is important to underline that this proposed model does not replace notification; indeed, the centralized controller should always be notified when an event occurs. However, in the meantime the device can already start reacting to the event. It is also important to note that reactions are not statically pre-configured; they can be revoked or reconfigured by the controller depending on the evolution of the network (e.g., depending on bandwidth availability).

We also propose a YANG model for an FSM. Each state of the machine is based on the Event YANG model. In particular, the FSM YANG model extends the YANG model for the events by adding the state information and state transition. More precisely, the model defines a list of states that, similar to the events, are configurable by the controller. Each state has a description attribute and it is identified through an ID. Each state also includes a list of events as defined in the event model, with the additional next-state attribute, which points to the next state.

Experimental Demonstration of YANG-Based Control Plane Modeling Events and State Machine

The proposed models have been experimentally demonstrated in a testbed composed of a centralized network controller (implementing phyton) and two transponder controllers (using ConfD) at the transmitter and receiver side, respectively.

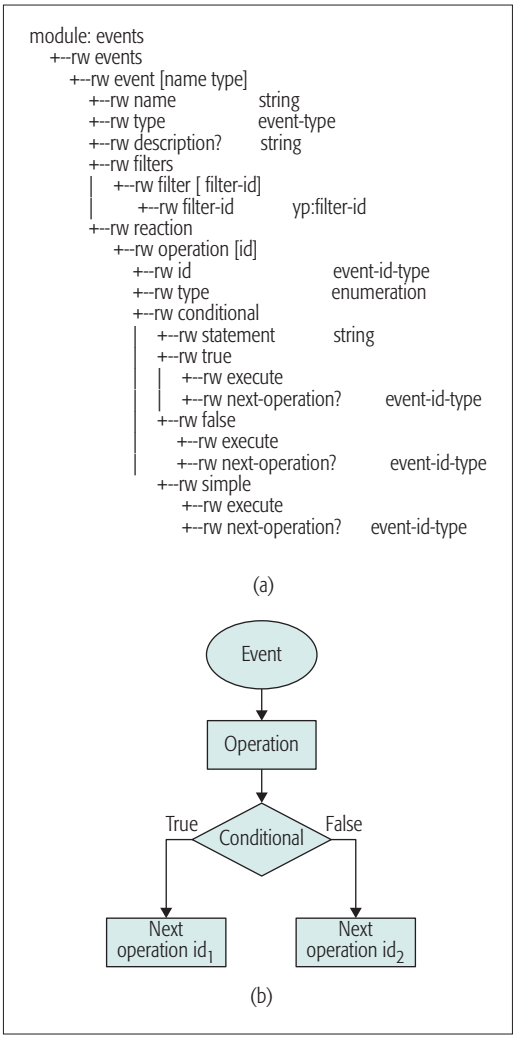


Figure 4. a) YANG tree representation of events and reactions; b) flow chart for conditional operations.

First, the transponder YANG model discussed earlier is considered, and a NETCONF message is generated to configure the following transmission parameters: 100 Gb/s net rate connection with a baud rate of 28 Gbaud, 7 percent of FEC, and polarization multiplexing quadrature phase shift keying (PM-QPSK) modulation format.

Then the configuration of events and state machine is performed as in Fig. 5a, which shows the NETCONF message exchange between the centralized controller and a transponder controller at the transmitter side. Similarly, message exchange has been performed with the controller at the receiver side. Initially, the centralized controller sends an <edit-config> message, as in [5], including the structure of the FSM and the associated events. This message enables the remote controller to instruct the device controller about FSM, critical events, and actions to be taken if these events occur. Once the device controller is instructed about FMS and the event, an acknowledgment message (<ok> message as in [5]) is sent to the remote centralized controller notifying that the operation has been concluded. The actions to be taken and the critical events can be reprogrammed on the device by simply sending a new message configuration to the device controller

It is important to underline that this proposed model does not replace notification; indeed, the centralized controller should always be notified when an event occurs. However, in the meanwhile the device can already start reacting to the event.

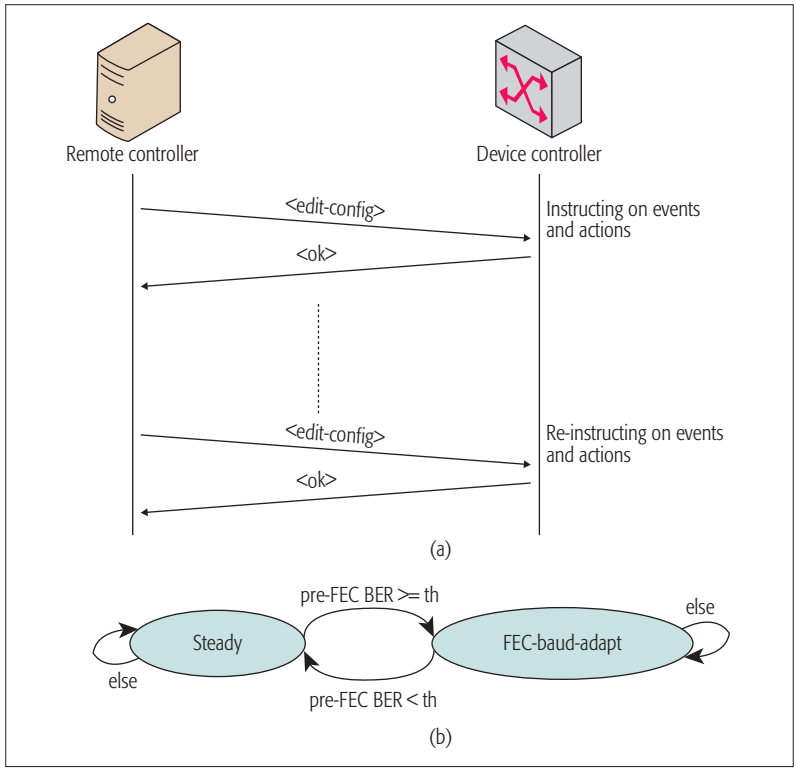


Figure 5. a) NETCONF message exchange in the testbed; b) implemented finite state machine.

with the new information. The experiment consists of configuring the FSM depicted in Fig. 5b, which is composed of two states: "Steady" and "Fec-Baud-Adapt." In the Steady state, the connection is in a healthy condition with a pre-FEC BER below the assigned threshold of 9×10^{-4}. If the pre-FEC BER exceeds the threshold, the state machine evolves to the Fec-Baud-Adapt state, where an adaptation to a more robust FEC (20 percent) and a baud rate change (to 31 Gbaud) are performed. Note that the centralized controller is aware of spectrum occupation. The receiver controller detecting the failure sends a notification of the event to the transmitter controller through the supervisory channel. This way, the transmitter controller reconfigures the transmission parameters (FEC) based on the event and the instructions in its FSM. From the FEC-Baud-Adapt state, if the pre-FEC BER returns below the threshold, the state machine moves back to the Steady state, readjusting the baud rate and the FEC to the initially configured values.

Figure 6a shows a portion of the message sent by the controller to the transponder to configure the FSM previously described. In particular, the Steady state with id 1 and Fec-Baud-Adapt with id 2 can be identified. The Steady state is the starting point as indicated by the current-state attribute. It responds to the "ON CHANGE" event, more precisely only when the pre-FEC BER changes to a value higher than 9×10^{-4}. The associated reaction to the event is composed of a single operation ("execute"). As stated in the previous section, the "execute" command recalls an RPC (Fig. 6a) consisting of changing the baud rate and the FEC. After the execution, the current state becomes the state with id 2 (Fec-Baud-Adapt) as indicated by the next-state attribute. The "Fec-Baud-Adapt" state also responds to the "ON CHANGE" EVENT, but in this case only when the pre-FEC BER goes below the threshold. Similar to the Steady state, a single operation is executed in reaction. In this case, the same RPC is recalled with different values: the FEC and the baud rate are restored to the initial values.

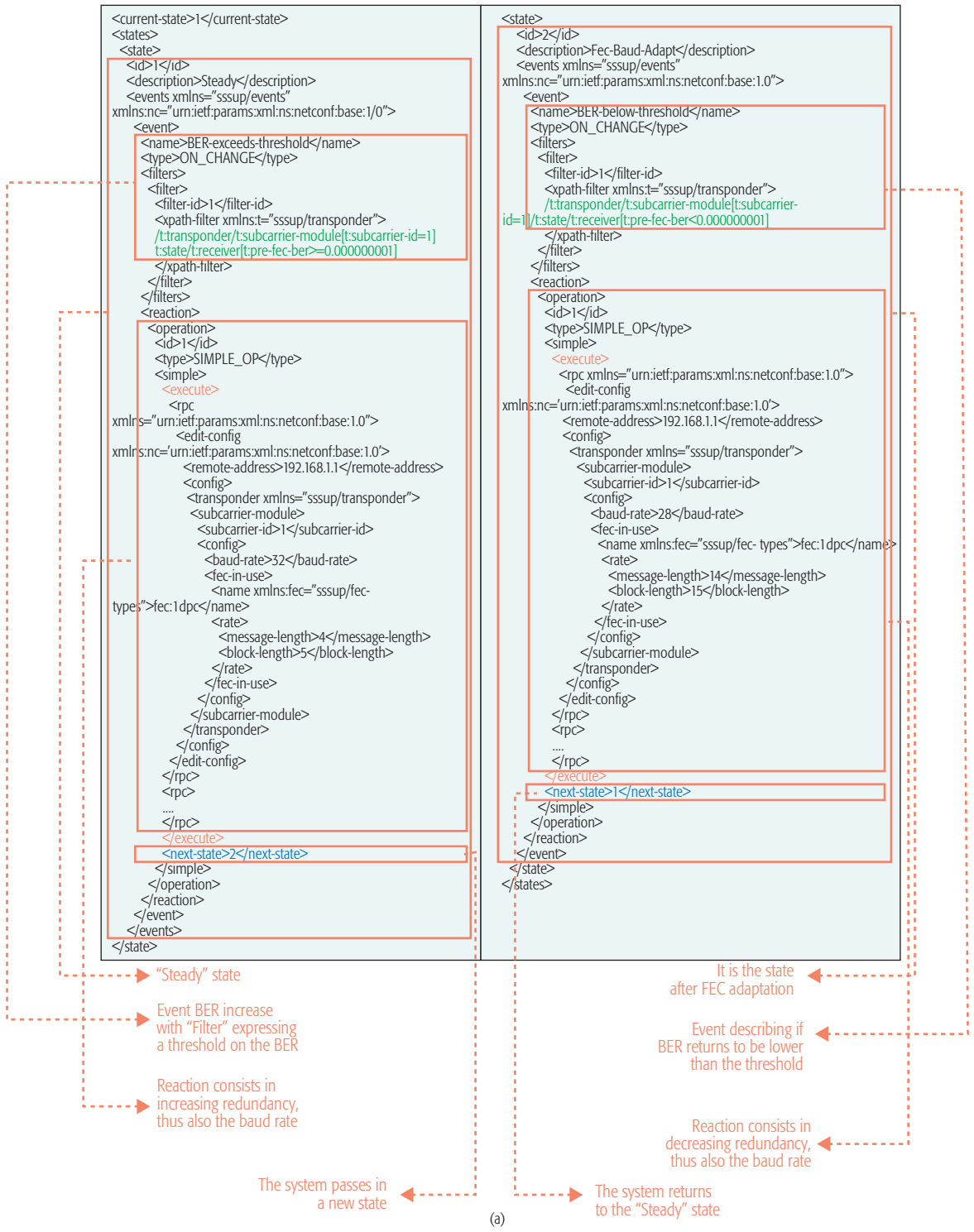
This way, the transponder device controller is successfully configured and instructed about the actions to perform when specific events occur. In the case of pre-FEC BER increase (or decrease), the transponder is able to automatically reconfigure itself without requesting the centralized controller and then waiting for its response on the actions to perform (only a notification message is generated).

Finally, we exploited simulations on a Spanish backbone (the same topology used in [15]) to identify the average number of 100 Gb/s PM-QPSK lightpaths affected by a soft failure. Results are shown in Fig. 6b. We generated an optical signal-to-noise ratio (OSNR) penalty spanning from 1 to 3 dB on random links. A lightpath is considered affected by the soft failure if the OSNR penalty causes a pre-FEC BER increase above the threshold of 10^{-3}; otherwise, the light path is assumed to be robust and can continue its normal transmission. The number of affected lightpaths increases with OSNR penalty since a higher penalty causes a higher pre-FEC BER increase. In the traditional case, the centralized controller has to receive notifications about the failure and the affected lightpaths, take a decision per lightpath (e.g., FEC adaptation), and send a message to reconfigure the involved devices. Thus, for high OSNR penalty, the centralized controller is also more loaded and reconfiguration at the data plane can suffer from delay. For example, in the case of 2 dB OSNR penalty, an average number of 16 lightpaths is affected. Conversely, a system exploiting the proposed YANG model for FSM is more scalable since the centralized controller is only notified upon failure.

Conclusions

In this article, the YANG modeling language has been described and enhanced to enable effective multi-vendor interoperability operations at both the network and node (i.e., white box) levels. Indeed, by standardizing a common language for network and node parameters, a controller can control and manage devices provided by different vendors, positively impacting the overall capital expenditure without being tied to single vendor's equipment. Specific enhancement has been introduced to also enable the YANG language to describe events and finite state machines, thus describing the set of actions to be performed at the node or device level without centralized controller intervention.

The defined YANG models for transponder, events, and finite state machines have been used in a control plane testbed to successfully configure, in a vendor-independent way, both transmission parameters and the actions to perform upon the occurrence of specific events. This way, upon pre-defined events at the physical layer (e.g., BER increase), the transponder is able to autonomously react without requiring time-consuming interaction with the centralized controller.



(a)

OSNR penalty [dB]	Average number of affected lightpaths	Operations at the controller upon failure (traditional approach)	Operations at the controller upon failure if FSM YANG is exploited
1	9.14	1) Receiving notifications about failure detection and involved lightpaths 2) Computation of recovery strategy per lightpath (e.g., FEC adaptation) 3) Sending messages for reconfigurations	1) Receiving notifications about failure detection, involved/ recovered lightpaths (e.g., FEC adaptation)
2	16.42		
3	22.52		

(b)

Figure 6. a) Capture of the control plane message instructing the device controller about the state machine; b) lightpaths involved in a failure and related operations at the centralized controller.

In the future, efforts in data modeling among vendors and operators will follow up to find common standard solutions. Moreover, functional models, such as finite state machine, can be enriched by adding new constructs besides "simple" and "conditional" operations.

In the future, efforts in data modeling among vendors and operators will follow up to find common standard solutions. Moreover, functional models, such as finite state machines, can be enriched by adding new constructs besides "simple" and "conditional" operations (e.g., error checking, and loops such as "for" and "while").

Acknowledgment

This work was supported by the EC through the Horizon 2020 ORCHESTRA project (grant agreement 645360).

References

[1] M. Gunkel *et al.*, "Vendor-Interoperable Elastic Optical Interfaces: Standards, Experiments, and Challenges," *IEEE/OSA J. Optical Commun. Networking*, vol. 7, no. 12, Dec. 2015, pp. B184–93.
[2] A. Shaikh *et al.*, "Vendor-Neutral Network Representations for Transport SDN" *Proc. 2016 OFC*, Anaheim, CA, Mar. 2016, pp. 1–3.
[3] M. Bjorklund, "YANG — A Data Modeling Language for the Network Configuration Protocol (NETCONF)," IETF RFC 6020, Oct. 2010.
[4] J. Vergara *et al.*, IETF draft-vergara-ccamp-flexigrid-yang-03, July 2016.
[5] J. Schonwalder, M. Bjorklund, and P. Shafer, "Network Configuration Management Using NETCONF and YANG," *IEEE Commun. Mag.*, vol. 48, no. 9, Sept 2010, pp. 166–73.
[6] M. Jinno *et al.*, "Distance-Adaptive Spectrum Resource Allocation in Spectrum-Sliced Elastic Optical Path Network," *IEEE Commun. Mag.*, Topics in Optical Communications, vol. 48, no. 8, Aug. 2010, pp. 138–45.
[7] L. Liu *et al.*, "OpenSlice: An OpenFlow-Based Control Plane for Spectrum Sliced Elastic Optical Path Networks," *Optics Express*, vol. 21, no. 4, Feb. 2013, pp. 4194–4204.
[8] https://github.com/openconfig/public/tree/master/release/models/optical-transport' accessed Dec. 2016
[9] M. Dallaglio *et al.*, "YANG Model and NETCONF Protocol for Control and Management of Elastic Optical Networks," *Proc. 2016 OFC*, Anaheim, CA, 2016, pp. 1–3.
[10] https://github.com/OpenROADM/OpenROADM_MSA_Public/tree/master/Version percent201.2, accessed Oct. 2016.
[11] N. Sambo *et al.*, "Next Generation Sliceable Bandwidth Variable Transponders," *IEEE Commun. Mag.*, vol. 53, no. 2, Feb. 2015, pp. 163–71.
[12] R. Enns *et al.*, "Network Configuration Protocol (NETCONF)," IETF RFC 6241, June 2011.
[13] X. Liu *et al.*, IETF draft-ietf-teas-YANG-te-topo-06, Oct. 2016.
[14] https://github.com/mattedallo/sssa/blob/master/yang-models/transponder.yang, accessed Mar. 2016
[15] N. Sambo *et al.*, "Monitoring Plane Architecture and OAM Handler," *J. Lightwave Technology*, vol. 34, no. 8, April 2016, pp. 1939–45.

Biographies

Matteo Dallaglio received his Master's degree cum laude in telecommunication engineering from the University of Trento together with a Diploma in communication network engineering from Scuola Superiore Sant'Anna, Pisa, in 2013. He is currently pursuing a Ph.D. in photonic technologies from Scuola Superiore Sant'Anna. His research interests include software defined networking, network functions virtualization, WDM network planning and modeling, PCE, and GMPLS protocols for traffic engineering.

Nicola Sambo is an assistant professor at Scuola Superiore Sant'Anna. He was a visiting student at France Télécom, Lannion. He is also collaborating with CNIT, Pisa, Italy. His research interests include optical network architecture, transmission performance modeling, and control plane. He is an author of about 100 publications including international journals, conference proceedings, and patents.

Filippo Cugini is with CNIT. His main research interests include theoretical and experimental studies in the field of optical communications and networking. He is a co-author of 12 patents and more than 200 international publications.

Piero Castoldi [SM] has been an associate professor at Scuola Superiore Sant'Anna since 2001, where he leads the area of Networks and Services. He had leading roles in the following EU projects: BONE, STRONGEST, IDEALIST, OFELIA, FED4FIRE, and 5GEx. His research interests cover network architectures, control, and data center architectures for grids and clouds. He is an author of more than 300 publications in international journals, conference proceedings, and patents.

Dimensioning and Assessment of Protected Converged Optical Access Networks

Arslan Shahid and Carmen Mas Machuca

ABSTRACT

Optical access networks are continuously evolving toward next generation solutions offering much higher bandwidth per endpoint and considerably longer optical reach. Their dimensioning and planning should be accurate and as close to realistic values as possible to become useful to network operators. This work presents a converged access network planning and dimensioning tool for planning and dimensioning of networks for fixed mobile convergence based on GIS. These networks connect to the CO, endpoints requiring different capacity and reliability constraints. This tool proposes a new clustering algorithm to decrease fiber and duct length. Furthermore, five protection schemes have been proposed, modeled, and compared in dense urban, urban, and rural areas to improve connection availability to the more availability demanding endpoints. The proposed assessment methodology compares the following parameters: component cost, power consumption, connection availability, indirect improvement in connection availability of residential users, FIF, and protection fiber length required per MBS. The article also includes a consolidated comparative analysis to find the best solution fulfilling the specific requirements of any network/service provider.

INTRODUCTION

Optical access networks can nowadays offer much longer reach and higher bandwidth communication than a few years ago. However, as the client count of access networks increases thanks to the increase of the delivered bandwidth, the impact of failure also increases. In this network-centric society, uninterrupted access to network services is becoming vital, and operators are now also considering protection of their access networks in addition to their aggregation and core networks. However, the cost factor is still very important due to the relatively low cost sharing of the access segment. One option to reduce cost is to use the same optical distribution network (ODN) to interconnect fixed endpoints (e.g., cabinets, buildings) as well as macro base stations (MBSs) at the so-called converged optical access networks. However, for this purpose, the network architecture should be able to offer different granularities in terms of bandwidth, connection reliability, and so on. Some new next generation optical access network (NGOA) architectures [1] offer the expected longer reach and bandwidth levels. However, they are initially unprotected; hence, in this article we propose different protection mechanisms to increase their connection availability.

Planning and dimensioning of access networks should be as accurate and realistic as possible. This is based on either geometric models or geographic models.

GEOMETRIC MODELS

Geometric models like the Triangle model [2], the Simplified Street Length Model [3], Gabriel graphs [4], and TITAN [5] are easy to use but may lead to inaccurate results/estimations, especially for uneven distributed data, which is the case in most practical cases. Geometric models only use the area-wide average parameters, and not local characteristics. In practice, the areas where optical access networks are deployed are not evenly populated, and the fiber trenching is constrained by various local conditions (e.g., parks, rivers, railways, or highways). This is a reason geometric models cannot contribute to accurate estimation of the deployment cost [6].

GEOGRAPHIC MODELS

Geographic models are the most preferred by operators because of their high accuracy, which ensures getting realistic results. These models can be used to select the right technology by evaluating all expenditures: capital expenditures (CAPEX), implementation expenditures (IMPEX), and operational expenditures (OPEX). The proposed methodology directly operates on available geospatial representation of the service area, which allows valid access network topologies to be provided. These topologies can be used as reliable and accurate bases for trenching, fiber length, and remote nodes (RNs) location planning. Geographical models also allow easier layout of network infrastructure and reduce IMPEX.

Some work has been presented on access planning using geographic models [7]. However, none of the existing dimensioning solutions address all the following aspects at once:

- Providing step by step dimensioning process description
- Completeness/breakdown of information about a shopping list (e.g., trenching diameter/depth, tube sizes)
- Ability to remove any inconsistent data from a geographic database (e.g., free standing features, dangles, cul-de-sacs)

This work presents a converged access network planning and dimensioning tool for planning and dimensioning of networks for fixed mobile convergence based on GIS. These networks connect to the CO, endpoints requiring different capacity and reliability constraints. This tool proposes a new clustering algorithm to decrease fiber and duct length.

Arslan Shahid is with National University of Sciences and Technology; Carmen Mas Machuca is with Technische Universität München.

Digital Object Identifier:
10.1109/MCOM.2017.1601204

The planning and assessment methodology proposed in this article has been applied to different protection schemes aiming at offering protection to some end points, in this case, to the MBS. The assessment of the different protection schemes has been done in three different areas: dense urban, urban and rural areas.

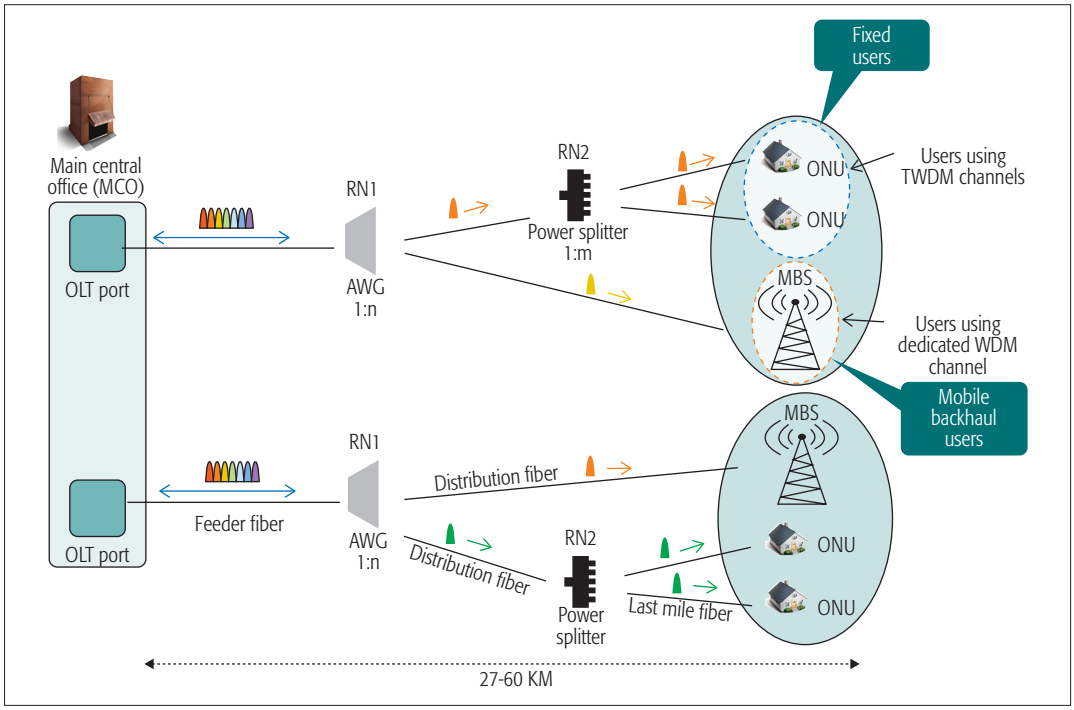


Figure 1. Two stage access HPON architecture: OLT (Optical Line Terminal); RN (Remote Node); AWG (Arrayed waveguide Grating); WDM (Wavelength Division Multiplexing); TDM (Time Division Multiplexing); ONU (Optical Network Unit).

- Coping with two or more stage splittings of NGOA networks
- Application to fixed-mobile convergence
- Improved clustering methodology considering street-aware distances instead of Euclidean distances reducing required fiber and duct
- Implementation of protection schemes

The planning and assessment methodology proposed in this article has been applied to different protection schemes aiming to offer protection to some endpoints, in this case, to the MBS (i.e., MBSs have higher availability requirements than residential users). The assessment of the different protection schemes has been done in three different areas: dense urban, urban, and rural areas.

It is important to mention that the proposed planning methodology is not limited to NGOAs, but can be applied to other access networks using other technologies by defining the number of remote nodes, their splitting ratio, required bandwidth, and so on.

The article is organized as follows. The following section introduces the generic NGOA architecture. Then we describe the complete dimensioning/planning methodology. Following that, we present the different protection schemes. Then we introduce the assessment methodology and the considered criteria. The next section presents the consolidated analysis of the proposed protection schemes. Finally we conclude the article.

NGOA for Converged Access Networks

Converged access networks aim to connect different types of endpoints (e.g., buildings and MBS) with the same ODN. Furthermore, node consolidation [8] is considered by operators in order to reduce the number of central offices and hence reduce OPEX when using NGOA, allowing longer reach and higher client count. Hence, the remaining central offices, referred as main central offices COs (MCOs), are now able to serve much larger service areas and more customers, but at the cost of decreasing the connection availability due to the longer distances, and increasing the failure impact [9].

Several passive optical networking (PON)architectures have been proposed in literature: next generation PON 2 (NGPON2 [1]), wavelength-division multiplexing PON (WDM-PON [1]), and hybrid PON (HPON) [1, 10]. Most of these architectures have more than one splitting stage. Although all the architectures can be used by the proposed planning tool, this explanation refers to HPON (depicted in Fig. 1) as it allows reusing existing ODN while fulfilling NGOA requirements. The optical line terminal (OLT) is placed at the MCO. The architecture has two stages of remote nodes. The first stage, denoted by RN1, uses WDM filters such as arrayed waveguide gratings (AWGs) for de-/multiplexing the downstream and upstream wavelengths. Compared to power splitters (PSs), an AWG has lower insertion loss and adds system integrity through wavelength separation. The second stage of remote nodes, denoted by RN2, involves PSs. As opposed to MBSs, which have dedicated wavelength, users connected to PSs share the wavelength capacity by using time-division multiple access (TDMA). This work considers MBS backhauled to the OLT; hence, one wavelength per MBS has been considered. However, the planning can easily be changed to more wavelengths per MBS for fronthaul solutions [11].

A system guarantees provisioning wavelength capacity B (e.g., 10 Gb/s) to each MBS or business user and B/N to each residential user with N being the splitting ratio of the PS.

The two-stage architecture considers three fiber sections as shown in Fig. 1:

- Feeder fiber (FF) is the fiber from the MCO to AWG.
- Distribution fiber (DF) is the fiber from AWG to PS or MBS.
- Last mile fiber (LMF) is the fiber from PS to the residential user's ONU.

This architecture has a tree topology where the OLT is at the root and is connected to AWGs, which are further connected to MBSs and PSs. This article focuses on the scenario of having one MCO; hence, distance to neighboring MCOs is very long due to node consolidation.

Dimensioning Methodology

This section introduces step by step the methodology to dimension a converged access network (with or without protection) in a real area. The steps of athe dopted methodology are:

•Select the area of study from Open Street Map (osm), which is a free GIS database from www.openstreetmap.org.

•Extract buildings data and road/street data, in our case, using ArcGIS (arcgis.com), which allows working with osm maps [12].

•For every building select a node (e.g., center or closest to the street) and associate it with its ONU location since in this case fiber to the building/home (FTTB/FTTH) has been considered (Fig. 2a).

•Unless the MBS locations are known (e.g., provided by the mobile operator), MBS can be placed based on the Voronoi model, or as a regular fishnet distribution given the inter-MBS distance (red stars in Fig. 2b). In this study, the MBS density is expected to influence more than the MBS distribution itself since the ratio of buildings vs. MBS is high. The MBSs are then associated with the nearest street node (green stars in Fig. 2b).

•1st stage clustering: As shown in Fig. 1, buildings are connected to PSs. Hence, given the PS splitting ratio and port usage, buildings are clustered (Fig. 2c). The proposed clustering algorithm has been designed to generate clusters of fixed size with the possibility to dynamically adjust individual cluster size and/or total number of clusters to maintain cluster quality and reduce the required infrastructure. The proposed clustering is presented in the next section. The centroid of each cluster is the best location for the PS. However, based on the experience of operators, they are relocated to the nearest intersection node (street crossing) because it increases accessibility and facilitates finding alternative paths required for protection (black triangles in Fig. 2d).

•2nd stage clustering: PS and MBS are clustered to AWGs based on the number of wavelengths and the port usage of the AWG (Fig. 2e). Although AWGs are initially placed at each cluster centroid, they are relocated to the nearest intersection node (yellow round shape).

•Compute the fiber layout of each fiber section (i.e., FF, DF, and LMF). The fiber layout can be computed using different approaches (e.g., simple shortest path, shortest path with maximum duct sharing [13, 14]). Based on the layout, the fiber required for each section as well as the duct can be computed. The duct is calculated by merging and dissolving all fiber paths. Furthermore, the cable size for each street segment can be computed, as shown in Fig. 2f.

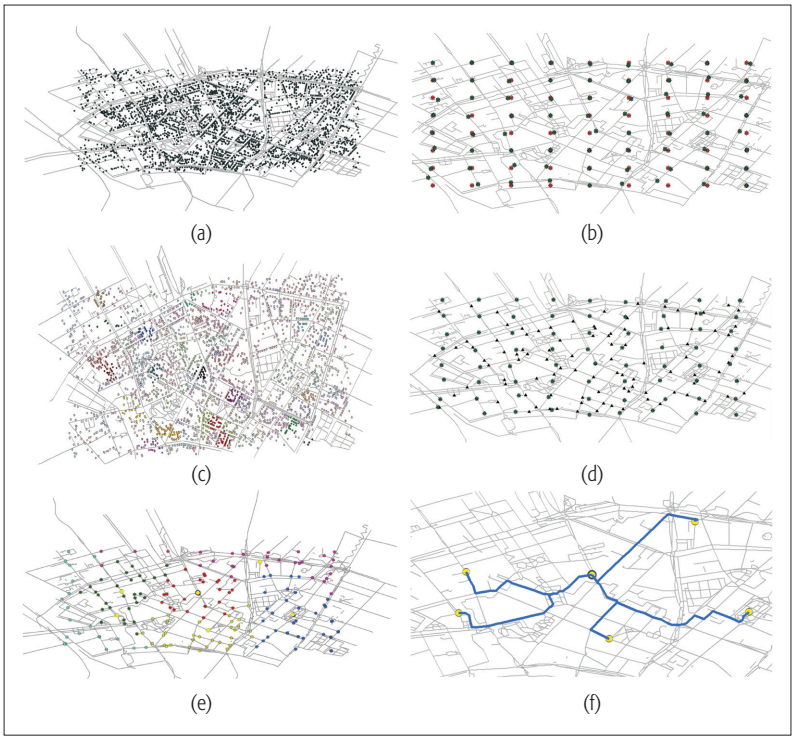


Figure 2. Planning methodology.

As a result of the network planning, the number and location of all components (MCO, AWGs, and PSs) as well as required fiber and cables in terms of different lengths and sizes are obtained. Although the fiber is aimed to be minimized, the maximum reach must not be exceeded. If it is exceeded, reach extenders should be placed at the right remote nodes.

Proposed Clustering Algorithm

Most of the clustering approaches considered in the literature are based on *K*-means clustering, that is, on Euclidean distances that may differ significantly from street-aware distances, especially in rural areas. Furthermore, *K*-means does not consider the impact that cluster sizes and distance have on infrastructure costs (e.g., adding a cluster, i.e., a splitter, may help to reduce costs, i.e., shorter distances).

In this section we propose a clustering algorithm that generates clusters given the splitting ratio with the possibility to dynamically adjust individual cluster size and/or total number of clusters to reduce the required infrastructure. It considers the following aspects.

Cost Matrix (CM): It is the matrix which stores the street-aware distances from one cluster element (CE) to the rest of the CEs. CEs are the elements that should be clustered (e.g., buildings at 1st stage clustering).

Initialization Method: Ascending order: One critical decision for any clustering algorithm is to identify from which node or seed master to start for building clusters. The proposed algorithm has been designed to compare different approaches:

- Considering distance from the seed master to the farthest seed member
- Considering the aggregate distance from the seed master to all its members

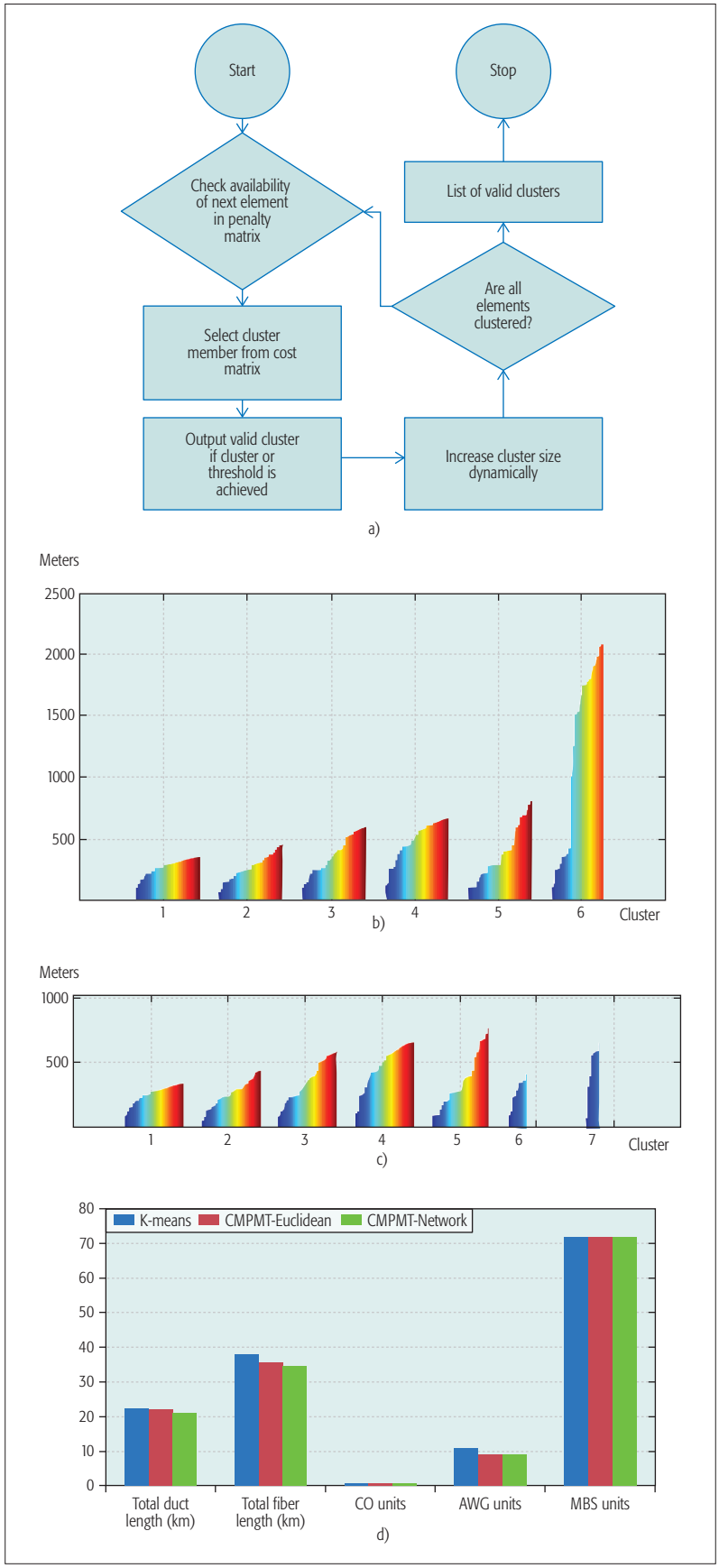


Figure 3. Clustering algorithm comparison. The proposed CMPMT algorithm may result in higher number of clusters. c) has one cluster more than b) but it reduces the required fiber: a) proposed CMPMT algorithm; b) modified K-means algorithm; c) clustering resutlting from proposed CMPMT; d) clustering comparison.

Both approaches consider either ascending or descending sorting order. We have identified that for the proposed DU, U, or R areas with reasonable road infrastructure, selecting aggregate distance with ascending order yields the best results [12].

Penalty Matrix: It is the matrix that stores the costs for the defined initialization method by considering the resulting clusters and largest cluster size.

Cost Threshold: This parameter defines the expected compactness of the cluster, and whenever it is exceeded, a new cluster is created instead of adding elements that are too dispersed. The impact of such a threshold is depicted in Fig. 3b, where savings of 28 percent on infrastructure cost can be achieved by adding 7 percent more clusters.

The proposed clustering algorithm is depicted in Fig. 3a. This algorithm has been compared to *K*-means and the impact on the number of clusters as depicted in Fig. 3b and 3c. In this case, PSs are clustered given the splitting ratio of AWGs. Figure 3b shows six different clusters and the length from each AWG to each PS of its cluster in meters. Each cluster may have a different number of PSs (the more colors, the more PSs are in the same cluster), and the PSs have been ordered based on their distance to their AWG. It can be observed that the last cluster contains fewer PSs and have significant longer distance. Figure 3c shows the advantage of the proposed scheme, which, by increasing by just one the number of clusters, significantly reduces the distance to the AWG. For that purpose, a comparison of the proposed algorithm using geographic distances (*CL Street Aware*) and using Euclidean distances (*CL Euclidean*) has been performed on the *K*-means for a DU area with 72 MBSs, as depicted in Fig. 3d. It can be observed that the infrastructure cost required per MBS is reduced by 6 percent with respect to *K*-means and by 4.7 percent with respect to Euclidean distances. It is pertinent to highlight that different *K* values were used, and the performance of each *K* value was evaluated. For fair comparison, the optimal/best solution found by *K*-means was selected and compared to our clustering algorithm, which yields better and more consistent results and, most importantly, does not require any sub-distance optimization.

Proposed End-to-End Protection Schemes

This article proposes different end-to-end (E2E) protection schemes that can be applied to different network points (e.g., RN1, RN2, MBS). However, in this article we apply different implementations of the schemes proposed by the authors in [15] to the E2E protection of MCO–MBS connections due to their high requirements in terms of capacity and reliability as well as their high impact factor (i.e., number of affected end users).

Disjoint Fiber Protection (DFP)

This scheme is based on the Type A protection scheme proposed in International Telecommunication Union — Telecommunication Standardization Sector (ITU-T) G.983.1, but applied to FF and DF of each MBS. As shown in Fig. 4a, the scheme needs disjoint FF as well as DF to each MBS. This

scheme requires the following additional equipment: one optical switch (OS) at each PON LT, one OS at each MBS, and two couplers and two AWGs at each RN1.

Ring Feeder Fiber Protection

The RFFP scheme proposes connecting all the AWG through a duct ring instead of dedicating a disjoint FF so that protection is achieved more easily (by an increase of working duct, protection is possible by using counter-wise fiber). The scheme is similar to the DFP depicted in Fig. 4a, but in this scheme RN1s are interconnected with a ring (i.e., working fiber will be clockwise and protection fiber anti-clockwise or vice versa depending on the location of the RN1). The working FF is the shortest fiber path, whereas the protection is the longer one. The ring is computed using the Traveling Salesman Problem (TSP) [6]. The TSP available at ArcGIS is based on a tabu search-based algorithm to find the best sequence of visiting the stops by preserving the first and last node (either AWG or MCO). From the AWG to the MBS, a disjoint DF as in the DFP scheme is proposed. This scheme requires the same components and has the same reliability block diagram (RBD) as the DFP but with different FF lengths.

Inter MBS DF Protection

The IMBSP scheme offers protection to an MBS using a disjoint DF from the protected MBS to the closest disjoint AWG. In this case, a disjoint AWG is the one that does not share any duct with the FF and DF of the protected MBS, as depicted in in Fig. 4b. This scheme requires one OS and one filter at each MBS, since the wavelengths used for working and protection may not be the same.

Ring Inter MBS Protection

The RIMSP scheme proposes connecting all the AWGs through a duct ring as proposed in RFFP, so FF protection is ensured by the ring (i.e. the shorter path in either the clockwise or anticlockwise direction is taken as the working path, and the other direction is allocated for the protection path). For DF protection a disjoint protection path to the nearest disjoint AWG is required. It is expected that by proposing this scenario, the solution space/probability of finding the nearer disjoint AWG to an MBS is increased; thus, the total DF required for protection paths will decrease. Similar to IMBSP, RIMBSP requires:

- One OS at each PON LT
- One coupler at each RN1
- One OS and one filter at each MBS

Microwave MBS Protection

The μWP protection scheme proposes wireless solutions to offer protection links for feeder and/or distribution segments depicted in Fig. 4c. It offers protection to MBS based on a microwave link between two disjoint MBSs subject to two constraints:

- MBSs are disjointly connected to the MCO (fiber sharing restriction).
- MBS have a clear line of sight (CLOS) (microwave communication restriction).

This scheme requires one microwave link for each pair of MBSs, and hence the capacity of the wave link should support the capacity of one MBS.

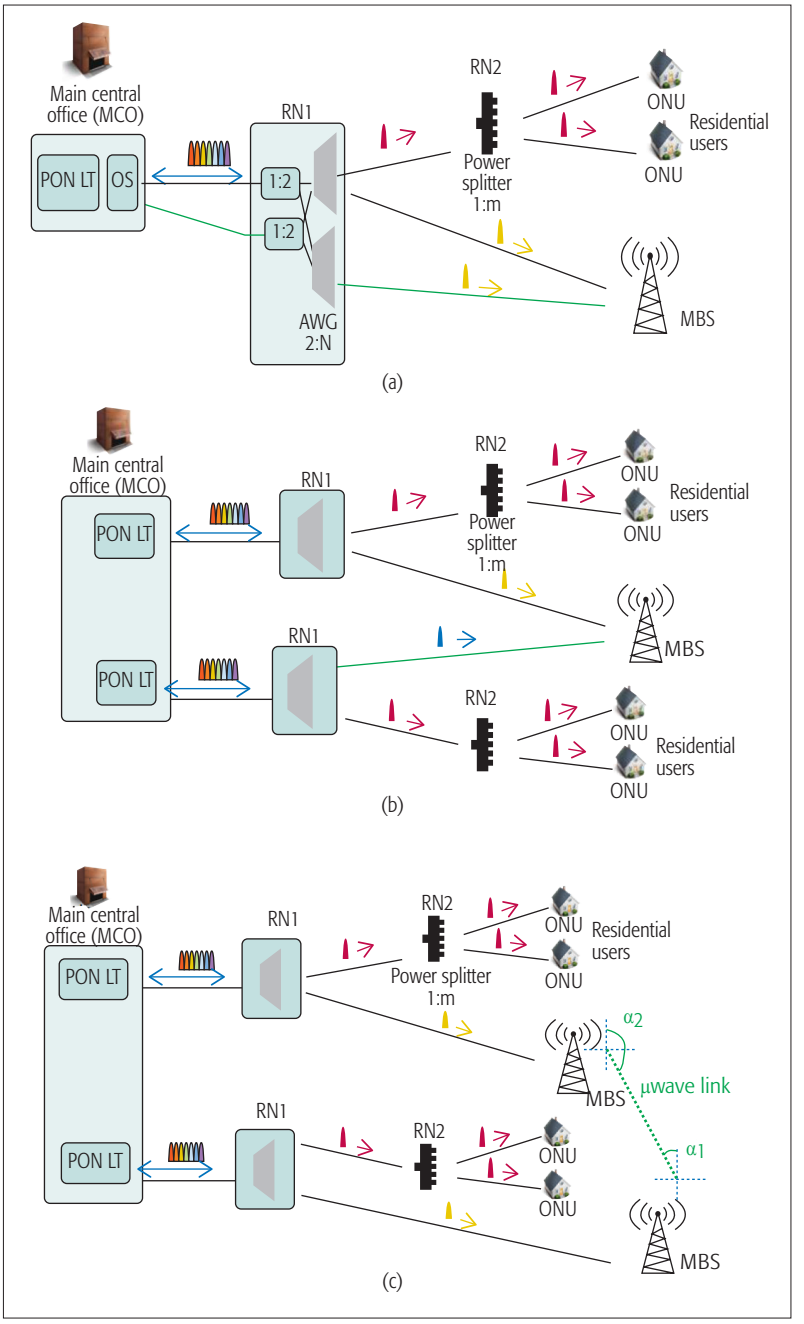


Figure 4. a) Disjoint Fiber Protection (DFP); b) Inter MBS Protection (IMBSP); c) μWave protection (μWP).

Hence, for N MBSs, $N/2$ microwave links are required, since the microwave link is considered to be bidirectional.

Assessment Methodology

This section extends the assessment methodology proposed in [15], which will be applied to compare the different proposed protection scenarios.

This section introduces the terms and parameters used in this assessment.

FF: Feeder fiber required for working paths.

DF: Distribution fiber required for working paths.

FF': Feeder fiber required for protection paths

DF': Distribution fiber required for protection paths.

DFP and RFFP have the same component costs since they only differ in fiber layout. RIMBSP has lower cost than DFP and RFFP due to less required equipment. IMBSP requires the minimum additional equipment, so it is the most economical. WP is the most expensive, but it gives more flexibility and offers quick installation.

ΔW: Increase of working feeder fiber with respect to the unprotected solution. The schemes based on FF rings have a non-zero ΔW value.

DUCT: Duct required by unprotected scenario.

DUCT′: Duct required by selected protection scheme.

Average Protection Fiber Required used for availability calculations:

$$\frac{FF'}{\#RN1}+\frac{DF'}{\#MBS}$$

Average protection fiber required used for cost calculations:

$$\frac{FF'+\Delta W+DF'}{\#MBS}$$

The total protection fiber required is the heart and soul of determining the efficiency of any protection scheme. More fiber requirement means more cost and less availability, which is not desired by any operator/customer. For calculation of working paths we have used Dijkstra's shortest path algorithm with duct sharing to reduce the initial investment; for protection paths we have used Dijkstra's shortest path without duct sharing to minimize the length of required fiber. The network analyst extension of ArcGIS has been used, and summarized results are shown in Table 1. It is highlighted that μWP does not require extra fiber, since it relies only on the microwave link between MBS (i.e., extra equipment cost).

Assessment Criteria

Different parameters have been considered.

Component Cost per MBS: This parameter considers the cost of the additional components required for the MBS protection (e.g., splitter, AWG, reach extender if required). The cost values are given in cost units (CUs) which are normalized to the cost of a GPON ONU (i.e., around €50).

Power Consumption per MBS: Since the power of access networks has been shown to be the dominant consuming segment, the power of the components required for protection should be evaluated. AWGs and power splitters are passive components.

Connection Availability: This is defined as the probability of the connection being operational at any point of time. In this study, it corresponds to the connection between the OLT and the MBS. The connection availability can be computed using the availability expression of the associated reliability block diagram [12].

Indirect Improvement in Connection Availability of Residential Users: Although the objective of these protection schemes is to increase the connection availability between MCO-MBS, some schemes also increase the connection availability between MCO-residential users.

Failure Impact Factor: The FIF is defined as the number of affected users/connections when a particular failure occurs [10]. The FIF of an unprotected component is computed as the product of its unavailability and its FPR. The FIF of any connection can be computed as the sum of the FIF of each involved unprotected component.

Protection Fiber Length Required per MBS: This is how much fiber should be installed in order to protect the endpoints. In general, the longer the fiber, the more expensive the solution.

ΔW (Additional Fiber Requirement for Working Paths): The protection schemes considering an FF ring require longer working FF than the other schemes, which consider working FF as the shortest path between MCO and RN1. This difference, denoted as ΔW, is important when aiming to compare the investment required for the different schemes.

Comparative Overall Performance

The comparison is based on two techniques.

Spider Net Diagram Comparison: The first step is to discretize the values of each parameter. The diagram will have as many axes as parameters. The parameters for one particular scenario/area will be plotted and compared: the smaller the diagram, the better the scheme for that area.

Pondered Assessment: Each operator may prioritize some parameters; hence, the importance of those should have higher weight than the others. For example, an operator could prioritize the required investments and thus select as the most important parameters the component cost, protection fiber length/MBS, and ΔW. Another operator could prioritize the customer satisfaction; hence, the parameters with higher weights would be connection availability and indirect improvement in connection availability of residential users.

Case Study

Let us perform a comparative assessment of the proposed protection schemes in three areas with different building and MBS densities:

- Dense urban (DU): 2863 buildings and 72 MBSs in a 3 km^2 area (Berlin)
- Urban (U): 2462 buildings and 70 MBSs in a 12 km^2 area (Helfenberg)
- Rural (R): 3103 buildings and 64 MBSs in a 45 km^2 area (Miesbach)

In this case, a two-stage optical access architecture has been considered with AWGs of 1:40 wavelengths at the first remote node and PSs of 1:32 splitting ratio at the second remote node. The maximum reach is 17 km for residential users and 43 km for MBS (D4.2.1 of the OASE project). The port utilization, that is, the maximum number/upper ceiling of ports which are allowed to be used, is set to 80 percent. The remaining 20 percent of the ports are left for protection or future use. The data considered in this study has been obtained from [14].

The values obtained for each of the proposed parameters are summarized in Table 1.

Component Cost per MBS: DFP and RFFP have the same component costs since they only differ in fiber layout. RIMBSP has lower cost than DFP and RFFP due to less required equipment. IMBSP requires the minimum additional equipment, so it is the most economical. μWP is the most expensive one, but it gives more flexibility and offers quick installation.

Power Consumption per MBS: Since the power consumption of optical switches are much lower than the power consumed by filters, DFP and RFFP consume much less power than the other schemes. The μWP has the highest power consumption despite the two modes of operation of the Wave link (sleep and active).

	Component cost/MBS (CU)	Power consumption/MBS (kWh)	Connection availability	Decrease residential users' unavailability	FIF	Prot. fiber (km)	ΔW (km)
DU							
DFP	5.19	0.001	0.999912809	6.3%	0.017735	0.87	0
RFFP	5.19	0.001	0.999912808	6.3%	0.017735	1.16	3.109
IMBSP	3.5	12.265	0.999948996	0.0%	0.000051	1.13	0
RIMBSP	3.79	12.625	0.999948995	5.6%	0.000051	1.33	3.109
μWP	75	17.522	0.999999987	0.0%	0.000033	0	0
U							
DFP	4.81	0.001	0.999912809	17.0%	0.017849	2.42	0
RFFP	4.81	0.001	0.999912808	17.0%	0.017849	2.85	4.962
IMBSP	3.5	12.265	0.999948996	0.0%	0.000051	2.8	0
RIMBSP	3.76	12.625	0.999948995	16.4%	0.000051	2.9	4.962
μWP	75	17.522	0.999999987	0.0%	0.000033	0	0
R							
DFP	5.08	0.001	0.999912809	14.3%	0.022314	5.74	0
RFFP	5.08	0.001	0.999912808	14.2%	0.022314	7.95	31.078
IMBSP	3.5	12.265	0.999948996	0.0%	0.000051	4.51	0
RIMBSP	3.78	12.625	0.999948995	13.7%	0.000051	7.28	31.078
μWP	75	17,522	0,999999987	0.0%	0.000033	0	0

Table 1. Assessment parameters for each protection scheme and area type.

The proposed tool has been used to compare different proposed protection architectures for converged access networks in different types of areas. The best protection scheme depends on the clear and concise requirements of the operator and the deployment area.

Connection Availability: The components and the fiber availability reference values have been taken from [3] and also explained in [12]. IMBSP, RIMBSP, and μWP schemes have higher connection availability due to the PON LT protection at the OLT. μWP offers even higher availability due to the duplication of all the components (including the ONU). Despite the different fiber lengths of DFP and RFFP, they show comparable connection availability because the fiber is protected, and hence, its length has very little impact on connection availability.

Indirect Improvement in Connection Availability of Residential Users (presented as a percentage with respect the unprotected case): DFP, RFFP, and RIMBSP increase the availability of residential users, because the protected FF is common to MBS as well as to residential users. However, IMBSP and μwave do not improve residential user availability. The degree of improvement depends on the area as the length of FF and FF′ is different. In U and R areas the availability improvement is higher due to the longer impact of protecting FF (they are longer than in DU areas). The resultant availability of residential users is almost four-nines compared to the three-nines unprotected availability.

Failure Impact Factor: The FIF of the μWP scheme is zero as all components are protected. The FIF of IMBSP and RIMBSP is very low as PON LT is protected in these schemes. DFP and RFFP have the highest FIF because they have a larger set of unprotected components. As both schemes use the same architectural scheme, the FIF values are the same. Compared to the unprotected scenario (FIF value = 0.0265186717), DFP and RFFP schemes decreased FIF by almost 50 percent, and IMBSP and RIMBSP decreased the FIF almost 50,000 times.

Protection Fiber Length Required per MBS: It can be observed that DFP is the most economical solution in DU and U areas. However, when the area becomes too sparse as in an R area, IMBSP turns to be the most economical solution.

ΔW: The schemes with ring protection show an increase of fiber of almost 40–50 percent in DU and U areas and 300 percent in R areas.

The assessment of the parameters in Table 1 is not straightforward; hence, we apply the two techniques proposed earlier.

Spider Net Diagram Comparison: In our study we have discretized the values of Table 1 to four (from 1-best to 4-worst) as proposed in [14]. Based on the values, the spider net diagrams can be gen-

erated (depicted in Figs. 5a and 5b for DU and U areas, respectively). The advantage of this technique is that this graphical representation helps compare schemes. In this case, RIMBSP is clearly better than RFFP (except for power consumption) since it covers a smaller area. This diagram also helps understand how each protection scheme is affected by the area, (e.g., μWP does not depend significantly on the area type, whereas RFFP does.)

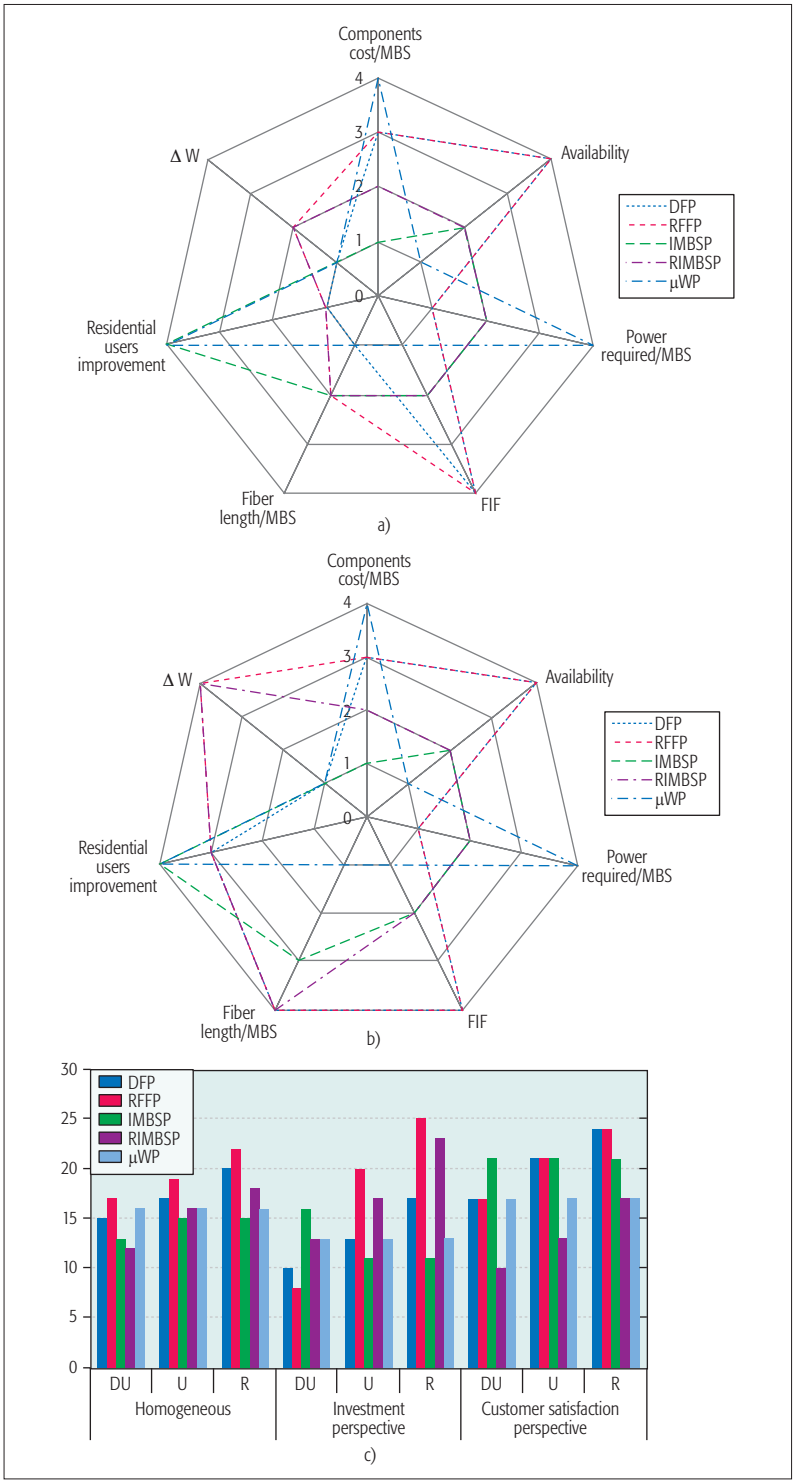


Figure 5. Assessment diagrams: a) spider net diagram for dense urban area; b) spider net diagram for rural area; c) pondered comparative diagram where the y-axis is the sum of all discretized parameters of each scenario (i.e., 8 is best and 25 is the worst).

Looking at the diagrams, the first conclusion is that there is no clear winner, and thus a compromise should be considered. We can also deduce that the connection availability and FIF do not vary significantly in the area since they are driven by the unprotected components, which do not include the fiber. The μWP scheme shows extreme values (either best or worst) and does not depend on the area type.

Pondered Assessment: Since there is no best solution, the priorities of each operator should be taken into account when evaluating the protection schemes. Figure 5c compares the schemes for the different interests (e.g., investment perspective prioritizes component cost, protection fiber length, and ΔW with respect to the other parameters, whereas the customer satisfaction perspective prioritizes connection availability to MBSs and residential users). This pondering should be adjusted based on the interests of each operator. In this case, an operator concerned with investment would choose RFFP in DU areas and IMBSP for U and R areas. An operator prioritizing customer satisfaction would choose RIMBSP for any type of area.

Discussion and Conclusion

A converged access network planning and dimensioning tool has been described. This tool incorporates a new clustering algorithm that is aimed at reducing the required infrastructure. The proposed tool has been used to compare different proposed protection architectures for converged access networks in different types of areas. The best protection scheme depends on clear and concise requirements of the operator and the deployment area. Comparative and consolidated performance analysis of each protection scheme has been carried out with even and uneven weights distribution to select the best protection scheme in a particular scenario/area. It has been shown that with even weights distribution RIMBSP is the best protection scheme in a dense urban area, and IMBSP is the best protection scheme in urban and rural areas. Besides, these weights can be adjusted by a service/network provider to meet any specific goal/ requirement. It is also shown that by changing these weights, the results significantly vary; therefore, the best solutions in the three types of areas depend on the criteria prioritized by the operator.

References

[1] M. Forzati *et al.*, "Next-Generation Optical Access Seamless Evolution: Concluding Results of the European FP7 Project OASE," *J. Opt. Commun. Networking*, vol. 7, no. 2, 2015, pp. 109–23.

[2] D. Gardan *et al.*, "Techno-Economics of Advanced Optical Subscriber Networks," *IEEE GLOBECOM and Expo, Communications Technology for the 1990s and Beyond*, 1989, vol. 3, Nov. 1989, pp. 1335–39

[3] K. Casier, *Techno-Economic Evaluation of a Next Generation Access Network Deployment in a Competitive Setting*, Ph.D. dissertation, Faculty of Engineering, Ghent Univ., Oct. 2009

[4] D. Maniadakis and D. Varoutas, "Incorporating Gabriel Graph Model for FTTx Dimensioning," *Photonic Network Commun.*, vol. 29, no. 2, 2015, pp. 214–26.

[5] B. Olsen *et al.*, "RACE 2087/TITAN: Tool for Introduction Scenarios and Techno-economic Studies for the Access Network," *Proc. RACE Open Wksp. Broadband Access*, 1993, pp. 7–8.

[6] A. Mitcsenkov *et al.*, "Geometric versus Geographic Models for the Estimation of an FTTH Deployment," *Telecommun. Sys.*, vol. 54, no. 2, 2013, pp. 113–27.

[7] O. Kipouridis *et al.*, "Street-Aware Infrastructure Planning Tool for Next Generation Optical Access Networks," *Proc. 2012 16th Int'l. Conf. Optical Network Design and Modeling*, Apr. 2012, pp. 1–6.
[8] C. Lange *et al.*, "Effects of Network Node Consolidation in Optical Access and Aggregation Networks on Costs and Power Consumption," *OPTO*, 2010, p. 76,210F.
[9] M. Mahloo, *Transport Solutions for Future Broadband Access Networks*, Ph.D. dissertation, KTH, Stockholm, Sweden, 2015.
[10] M. Mahloo *et al.*, "Toward Reliable Hybrid WDM/TDM Passive Optical Networks," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. S14–23.
[11] B. Kanj *et al.*, "Comparison of Wavelength-Routed and Wavelength-Split WDM-PON in Mobile x-Haul in Dense Urban Areas," *ITG-Fachtagung Photonische Netze 2016*, Leipzig, Germany, May 2016.
[12] A. Shahid, "Enhanced Dimensioning and Comparative Analysis of Different Protection Schemes for Hybrid PON Converged Access Networks (HPCAN)," Master's thesis, TRLKN-2015-02, Technical Univ. Munich, Germany, 2015.
[13] R. H. Nielsen *et al.*, "On the Potential of Using the Cable Trench Problem In Planning of ICT Access Networks," *Proc. 50th Int'l. Symp. ELMAR*, vol. 2, 2008, pp. 585–88.
[14] A. Shahid *et al.*, "Comparative Analysis of Protection Schemes for Fixed Mobile Converged Access Networks Based on Hybrid PON," *Proc. 12th int'l. Conf. Telecommun., Media and Internet Techno-Economics*, Nov. 2015.
[15] C. Mas Machuca, L. Wosinska, and J. Chen, "Assessment Methodology of Protection Schemes for Next Generation Optical Access Networks," *Optical Fiber Technology*, Dec. 2015, pp. 82–93.

Biographies

Arslan Shahid received his Bachelor's degree from National University of Sciences and Technology (NUST), Pakistan, in the field of electrical (telecommunication) engineering in 2007 and his Master's degree from Technical University Munich (TUM), Germany, in 2015. Presently he is on the faculty of the Military College of Signals, a constituent campus of NUST, as an assistant professor in the field of telecommunication networks, information security, and electronic warfare.

Carmen Mas Machuca [SM'12] has been a senior researcher at the Chair of Communication Networks, TUM, since December 2005. Her main research interests are in the area of converged optical access networks, network planning and resilience, and techno-economic studies. She has published more than 100 peer-reviewed papers. She chaired CTTE 2015 and co-chaired RNDM 2015.

ACCEPTED FROM OPEN CALL

High-Efficiency Device Positioning and Location-Aware Communications in Dense 5G Networks

Mike Koivisto, Aki Hakkarainen, Mário Costa, Petteri Kela, Kari Leppänen, and Mikko Valkama

Future 5G networks are expected to provide huge improvements in the capacity, number of connected devices, energy efficiency, and latencies when compared to the existing communications systems. These features will be enabled by the combination of higher bandwidths, advanced antenna technologies, and flexible radio access solutions, among others.

ABSTRACT

In this article, the prospects and enabling technologies for high-efficiency device positioning and location-aware communications in emerging 5G networks are reviewed. We will first describe some key technical enablers and demonstrate by means of realistic ray-tracing and map based evaluations that positioning accuracies below one meter can be achieved by properly fusing direction and delay related measurements on the network side, even when tracking moving devices. We will then discuss the possibilities and opportunities that such high-efficiency positioning capabilities can offer, not only for location-based services in general, but also for the radio access network itself. In particular, we will demonstrate that geometric location-based beamforming schemes become technically feasible, which can offer substantially reduced reference symbol overhead compared to classic full channel state information (CSI)-based beamforming. At the same time, substantial power savings can be realized in future wideband 5G networks where acquiring full CSI calls for wideband reference signals while location estimation and tracking can, in turn, be accomplished with narrowband pilots.

INTRODUCTION

Future 5G networks are expected to provide huge improvements in the capacity, number of connected devices, energy efficiency, and latencies when compared to the existing communications systems [1, 2]. These features will be enabled by the combination of higher bandwidths, advanced antenna technologies, and flexible radio access solutions, among others. Especially in urban environments, 5G networks are also expected to consist of densely distributed access nodes (ANs) [2] located, for example, in lamp posts above the streets, as illustrated in Fig. 1a. Consequently, a single user equipment (UE) in such dense networks is within coverage range to multiple closely located ANs at a time. Such short UE-AN distances provide obvious benefits for communications, for example, due to lower propagation losses and shorter propagation times, but interestingly can also enable highly accurate UE positioning. Altogether, 5G networks allow for many opportunities regarding acquisition and exploitation of UE location information in unforeseen manners [3, 4]. This is the leading theme of this article.

One of the improvements in 5G networks concerns positioning accuracy. For example, it is stated in [5–8][1] that 5G should provide a positioning accuracy in the order of one meter or even below. That is significantly better than the accuracy of a couple of tens of meters provided in long term evolution (LTE) systems by observed time difference of arrival (OTDoA)-based techniques. The required positioning accuracy in 5G networks will also outperform commercial global navigation satellite systems (GNSS) where the accuracy is around 5m, and wireless local area network (WLAN) fingerprinting resulting in 3–4 m accuracy. Another improvement that 5G networks may provide concerns the energy efficiency of positioning. This stems from the common assumption that 5G networks will exploit frequently transmitted uplink (UL) pilot signals for channel estimation purposes at the ANs. These signals can also be used for positioning in a network-centric manner where the UE location is estimated either independently in the ANs or in a centralized fusion center, assuming known AN locations, and thus no calculations are needed in the mobile UEs. Note that this is a considerable difference from device-centric positioning, for example, GNSS, where the mobile UEs are under heavy computational burden. Therefore, network-centric positioning techniques provide significant power consumption improvements and enable ubiquitous high-accuracy positioning that can run in the background continuously. Such a functionality also decreases the signaling overhead when the location information is to be used on the network side, but on the other hand, requires additional care for privacy as the positioning is not carried out at the UEs themselves. As a third improvement in 5G-based positioning, regardless of whether it is network-centric or device-centric, location information can be obtained in complete independence of UE-satellite connections everywhere under the network coverage area, including also challenging indoor environments.

The aim of this article is to discuss the technical enablers of envisioned device positioning in 5G networks, and to promote the prospects of

[1] See also 3GPP technical report 22.862, v.14.1.0.

Digital Object Identifier:
10.1109/MCOM.2017.1600655

Mike Koivisto, Aki Hakkarainen, and Mikko Valkama are with Tampere University of Technology;
Mário Costa, Petteri Kela, and Kari Leppänen are with Huawei Technologies Oy; Petteri Kela is also with Aalto University.

the obtained location-awareness. In this regard, focus is given to location-based communication and network management techniques such as location-based beamforming as well as mobility and radio resource management (RRM) [9].[2] We recognize that UE location information can be exploited by the UE itself as well as shared with third parties, thus allowing for innovative location-based applications to emerge. Particularly, we will focus on the connected car application, being identified, for example, in [5] as one key application and target for future 5G mobile communication networks, with a minimum of 2000 connected vehicles per km^2 and at least 50 Mb/s in downlink (DL) throughput. Now, facilitating such greatly enhanced connected vehicle applications, having a 5G network with built-in capability to localize and track vehicles is a very tempting prospect. Furthermore, location information is a central element toward self-driving cars, intelligent traffic systems (ITSs), and drones, as well as other kinds of autonomous vehicles and robots that are envisioned to be part of not only the future factories, but the overall future society within the next 5–10 years.

5G Networks and Positioning Prospects

Technical Properties of 5G Radio Networks

Generally, it is expected that network densification will play an important role in achieving the demanding requirements of 5G networks. The inter-site distance of ANs in such ultra-dense networks (UDNs) is envisioned to range from a few meters up to a few tens of meters, for example, assuming several ANs per room indoors and an AN on each lamp post outdoors [1]. Moreover, these 5G ANs are expected to be equipped with smart antenna solutions, such as antenna arrays supporting multiple-input multiple-output (MIMO) techniques [6]. Such antenna technologies are suitable for effective communications as well as accurate direction of arrival (DoA) estimation, which in turn allows for high-accuracy positioning. Furthermore, it is argued that devices tend to be in line of sight (LoS) condition with one or multiple ANs due to network densification, which is a favorable condition not only for communications but also for positioning purposes.

It is commonly agreed that 5G technologies will require wide bandwidths in order to meet the envisioned capacity requirements. Therefore, 5G networks will most likely operate at higher frequency bands, including mm waves (mmWave), where the availability of unallocated spectrum is considerably higher. Such high frequency bands together with UDNs can provide very high overall system capacity and enable an efficient frequency reuse [6]. However, with the envisioned high frequencies, the propagation conditions become more demanding due to, for example, larger propagation losses. Hence, the effective range between transmitting and receiving elements is relatively short, which also emphasizes the importance of expected UDNs. Furthermore, the utilization of effective antenna solutions becomes more practical as a result of shorter wavelengths, and consequently due to the smaller physical size of antenna elements. In addition to the potential frequency bands above 6 GHz, frequencies below 6 GHz are also expected to be used in 5G networks [5]. Apart from a communication perspective, the envisioned wide bandwidths also enable very accurate time of arrival (ToA) estimates, which in turn provide an opportunity for positioning with remarkably high accuracy [3].

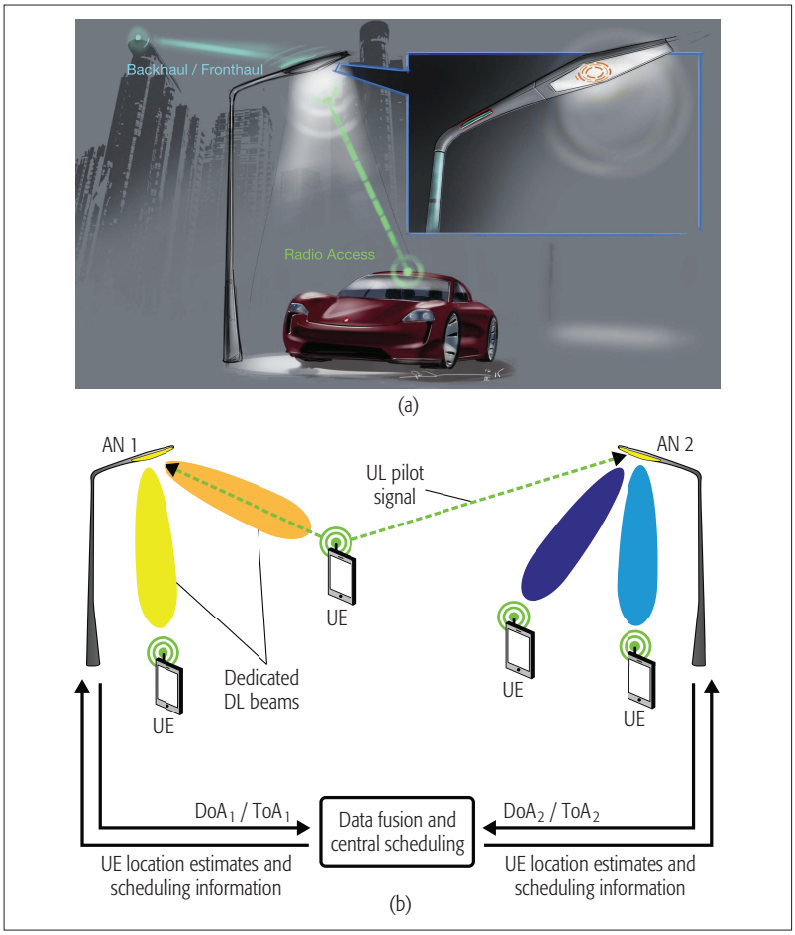


Figure 1. Illustration of a 5G network where a) AN, deployed in a lamp post, provides a LoS connection to a nearby UE, and b) ANs estimate DoAs/ToAs of the UEs based on UL pilot signals. The obtained estimates are then communicated to a fusion center providing the final location estimate which, in turn, enables geometric DL beamforming.

In contrast to the earlier cell-centric architectures, it is currently under discussion whether 5G networks will be developed in a more device-centric manner. Moreover, it is envisioned that 5G networks could also provide improved quality of experience (QoE) at cell borders with only a minimal system-performance degradation compared to earlier systems [10]. This development enables tailoring of a particular communication session and the functions of the associated ANs to a connected device or service instead of obtaining services from the AN commanding the specific cell. In such a device-centric architecture, a given device can periodically send UL signals to connected ANs in which UL reference signals are used for channel estimation, but they can also be employed for network-centric positioning, as illustrated in Fig. 1b. Furthermore, future 5G networks are expected to operate with relatively short radio frames, resulting in availability of frequent location information about a transmitting device.

[2] See also the WHERE and WHERE2 projects at ://www.ict-where.eu/ and http://www.ict-where2.eu/.

Leveraging Location-Awareness in 5G Networks

Continuous positioning provides awareness not only of the current but also of the past UE locations, and thus the network is able to carry out UE tracking. When the UE location and movement information is processed by predictive algorithms, the network can even predict the UE locations to some extent. The availability of such location information in turn enables a wide selection of entirely new features and services in 5G networks. First, location-awareness can be used for communications purposes by enhancing the utilization of spatial dimension, for example, by geometric beamforming [11] and sophisticated spatial interference mitigation. These features allow for multiplexing a high density of UEs and provide significant throughput improvements for high-mobility UEs, as illustrated below. Second, a combination of location information and measured radio parameters over a long time period enables the construction of radio environment maps (REMs), depicted in Fig. 2a, which, in turn, can open many opportunities in terms of proactive RRM [9]. In particular, the knowledge of large-scale fading and location-based radio conditions can be utilized for RRM purposes without the need to know the instantaneous channel information between the AN and UE. Therefore, the network is able to carry out proactive allocation of active UEs to nearby ANs such that, for example, power consumption, load balancing and latencies are optimized, as depicted in Fig. 2b. Location-awareness can also improve network functionalities by enabling proactive location-based backhaul routing such that the UE-specific data can be communicated with a high robustness and low end-to-end latency.

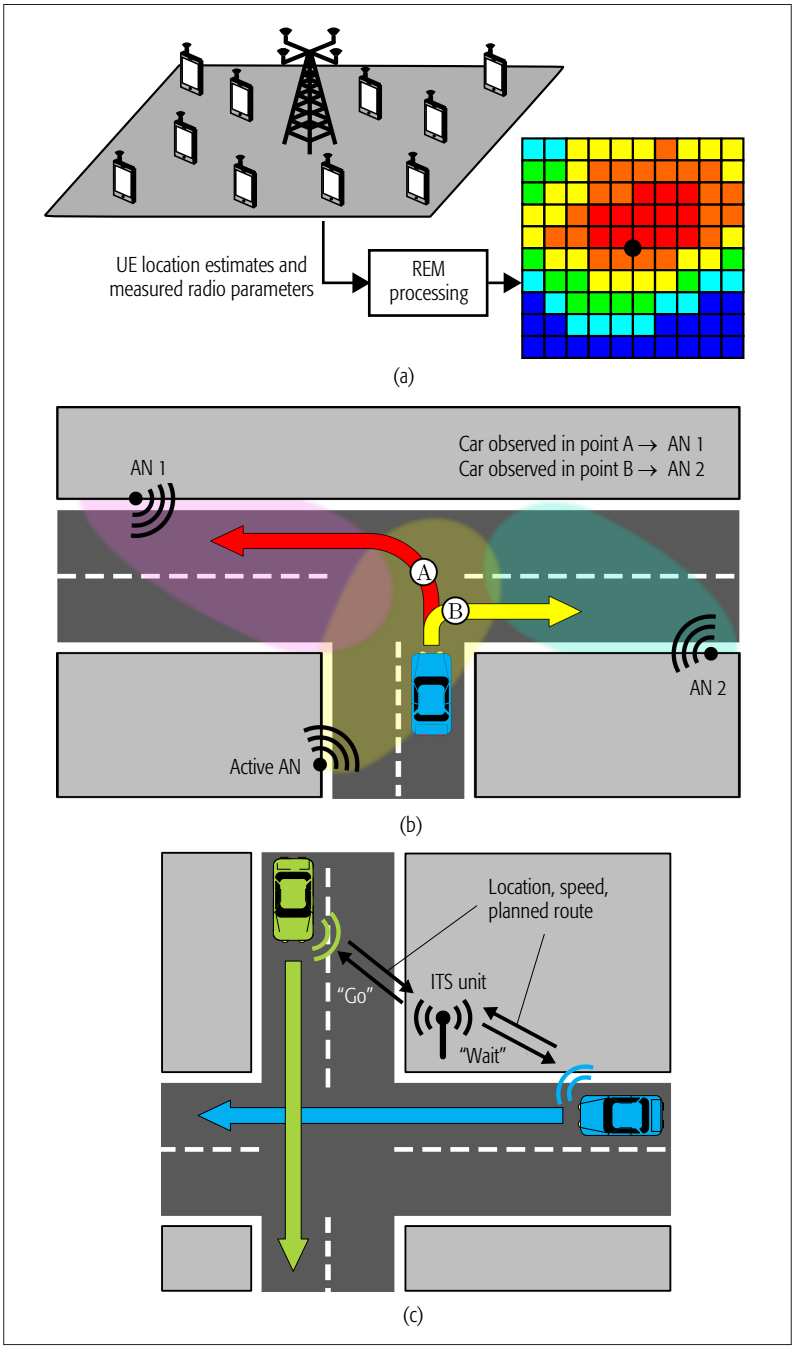


Figure 2. Illustrations of selected positioning prospects in 5G a) REM generation, b) proactive RRM for a car whose location is being tracked, and c) ITS-based traffic control and collision avoidance with self-driving cars.

The obtained location-awareness can also be exploited in the UEs as well as by third parties to provide other than purely communications type of services. Taking traffic and cars as an example, up-to-date location information and predicted UE trajectories can provide remarkable improvements, for example, in terms of traffic flow, safety and energy efficiency. When comprehensively gathered car location information is shared with ITSs, functionalities such as traffic monitoring and control can be enhanced. Accurate location information is also needed in the cars themselves, for example, for navigation purposes, especially when considering autonomous and self-driving cars. Location-awareness is also required for collision avoidance. Cars within communications range can report their location directly to other cars, but when the link between the cars is blocked, location notifications are transmitted in collaboration with ITSs, as illustrated in Fig. 2c. Naturally, the demands and functionalities regarding self-driving cars cannot be met everywhere and at all times by existing communications systems and satellite-based positioning. Consequently, advanced communications capabilities and network-based positioning in 5G is likely to play an important role in the development of self-driving car systems commonly available in the next decade.

Enabling Technologies for High-Efficiency Network-Centric Positioning

State-of-the-Art

Dense networks are characterized by radio channels that are dominated by the LoS-path. For example, the typical Rice-factor, being a power ratio between the LoS component and all other propagation paths, in urban micro-cell environments is around 10 dB, even in sub-6 GHz [12]. Additionally, network densification increases the LoS probability between UEs and ANs. As an example, 3GPP employs a channel model based on extensive measurements in which the LoS probability is higher than 0.7 for a maximum UE-AN distance of 35 m.

Determining the ANs that are in LoS condition to a given UE is important since it allows esti-

mating and tracking the directional parameters of the LoS-path, in addition to the time-of-flight and clock-offsets, thus greatly improving the UE positioning accuracy. In particular, the LoS condition of a radio link may be assessed by estimating the corresponding Rice-factor. A multichannel observation is obtained for each UL reference signal given that a multicarrier waveform and multiantenna ANs are employed. Sequential estimation of the Rice-factor can be accomplished, for example, with a particle filter due to the non-Gaussian nature of the amplitude distribution of the UL multicarrier channel. Finally, LoS detection can be accomplished using a likelihood-ratio test, or a model selection technique. In case all ANs are in non-LoS (NLoS) to the UE, coarse network-centric positioning can still be achieved using radio frequency fingerprinting, received signal strength indicator and cell-identifier, among others [9].

Multicarrier waveforms offer a versatile approach for estimating ranges between a given UE and multiple ANs [9]. Relying solely on UL reference signals makes it possible to synchronize the ANs as well as the UE, in addition to estimating the ToAs of the LoS-paths [3, 4]. The actual sequential estimation of the ToAs and clock-offsets can be accomplished with different Bayesian filters either in a cascaded or fully centralized manner depending on the network architecture, baseband processing capabilities of the ANs, and backhaul capacity. Note that the UL reference signals can also provide additional information for UE positioning when utilized, for example, for tracking Doppler-shifts.

ANs with multiantenna transceivers allow for estimating the DoA of the LoS-path from UL reference signals, and such information can be used for UE positioning. Planar or conformal arrays, such as circular or cylindrical antenna arrays, make it possible to estimate elevation and azimuth arrival angles, and enable 3D positioning. Bayesian filtering techniques can also be employed for tracking the DoAs of the LoS-paths from mobile UEs as well as fusing the ToAs and DoAs in order to allow for joint UE positioning and network synchronization [3, 4]. ANs with analog beamforming structures and sectorized antennas can also be exploited for UE positioning and tracking [13].

Due to the non-linear nature of the involved state-space models, estimation and tracking can be carried out with different non-linear Bayesian filtering techniques. In this article, the tracking processes are carried out using the extended Kalman filter (EKF) due to its highly accurate estimation performance and low computational complexity compared to, for example, particle filters and the unscented Kalman filter (UKF). In general, within the EKF, the state of a system is first propagated through a linearized state evolution model and this prediction is, thereafter, updated using the obtained measurements and a linearized measurement model, through which the state is associated with the measurements [4].

Finally, the techniques overviewed in this section for UE positioning can also be employed for estimating the locations of the ANs. For example, a few well-surveyed ANs can be used for finding the locations of neighboring ANs, which in turn may be used as new anchors. Such a procedure is useful since surveying all ANs would increase the deployment cost of UDNs significantly. Alternatively, joint UE tracking and ANs positioning can be achieved using techniques stemming from simultaneous localization and mapping (SLAM) [14]. These techniques are versatile but the cost is an increase in computational complexity due to the large number of parameters to be estimated.

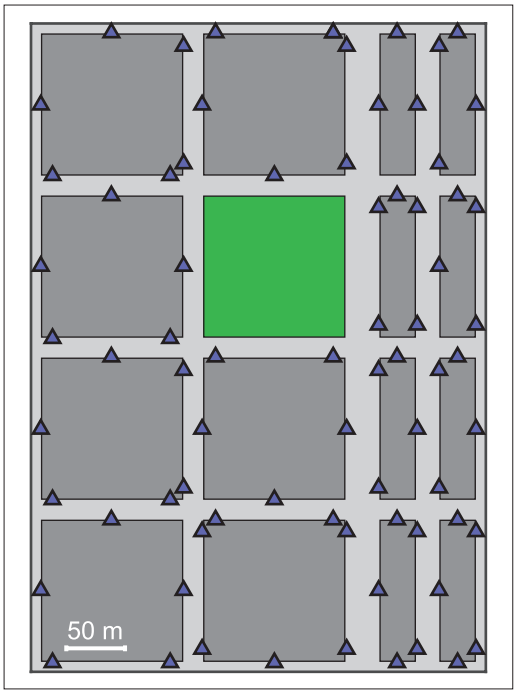


Figure 3. METIS Madrid grid layout, from [12], where ANs (blue triangles) are distributed densely along the streets.

The demands and functionalities regarding self-driving cars cannot be met everywhere and at all times by existing communications systems and satellite-based positioning. Consequently, advanced communications capabilities and network-based positioning in 5G is likely to play an important role in the development of self-driving car systems commonly available in the next decade.

Tracking of Directional Parameters using EKFs

We start by demonstrating the performance of EKFs in tracking the directional parameters of the LoS-path. We consider the case where both the ANs and UEs are equipped with multiantenna transceivers. Two schemes are considered, namely a network-centric approach and a decentralized scheme. In the network-centric approach, the arrival and departure angles of the LoS-path between a UE and an AN are tracked jointly at the AN.[3] The UE periodically transmits UL reference signals from all of its antenna elements. Each UE antenna element is assigned a single subcarrier, which is different from those used by the other antennas. The departure angles are transmitted to the UE on a DL control channel.

The decentralized scheme consists in tracking the double-directional parameters of the LoS-path independently at the AN and UE. Such a scheme is based on narrowband UL transmissions from a single antenna element of a UE. This allows the AN to track the arrival angles of the LoS-path. These arrival angles are used for designing a beamforming weight-vector that is exploited by the AN to transmit a beamformed DL reference signal toward the UE. This makes it possible for the UE to track the arrival angles, and thus design the receive beamforming weight-vector. The transmit and receive beamforming weight-vectors designed in this fashion are compared to the CSI at transmitter (CSIT)-based precoding schemes below.

[3] The departure angles can only be retrieved from the arrival angles if the orientation of the UE's array is known. The network-centric approach requires that the calibration data of the UE's array is acquired by the AN, for example, over a UL control channel.

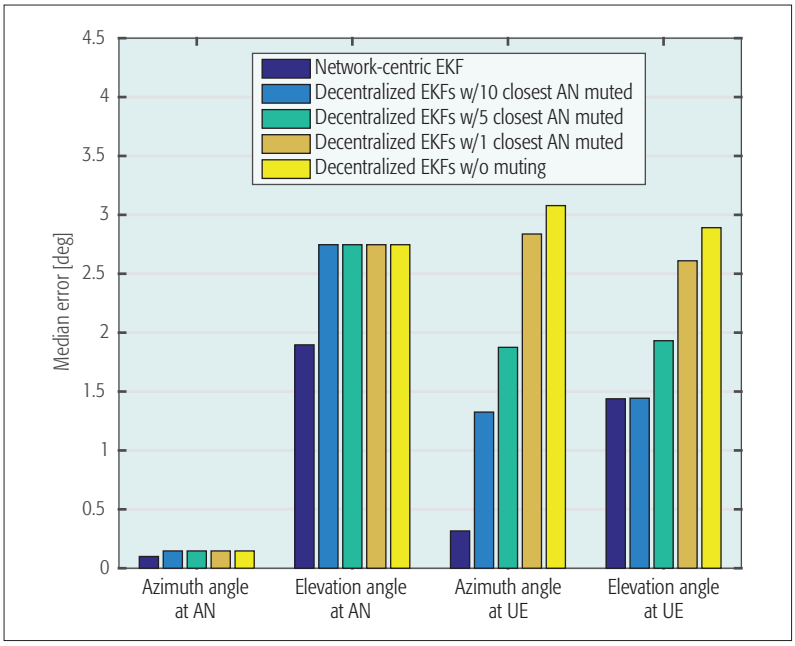


Figure 4. Accuracy of tracking the arrival and departure angles with EKFs in terms of the median error. In network-centric EKF, the UE transmits UL reference signals from all antenna elements and the AN tracks both arrival and departure angles of the LoS-path. In decentralized EKF, the UE transmits UL reference signals from a single antenna element which is used by the AN to track the arrival angles of the LoS-path with an EKF. Such directional parameters are employed in order to design a DL beamformed reference signal that then allows the UE to track and design a similar receive beamforming vector.

The performance of both the network-centric and decentralized approaches have been analyzed with a time division duplex (TDD) based 5G simulator. In particular, we have considered a UDN composed of 74 ANs with a deployment identical to that illustrated in Fig. 3. The ANs are equipped with circular arrays composed of 20 dual-polarized 3GPP patch elements 5 m above the ground. The UEs are equipped with circular arrays composed of four dual-polarized elements (cross-dipoles). The transmit power budget of the UEs is 10 dBm while that of the ANs is 23 dBm. The UEs take different routes through the Madrid grid (Fig. 3) with velocities of 30–50 km/h. The carrier-frequency is 3.5 GHz and the METIS map-based ray tracing channel model [12] has been employed. An orthogonal frequency division multiplexing (OFDM) waveform is used in both UL and DL. The subcarrier spacing is 240 kHz and the transmission time interval (TTI) equals 200 μs. The UL and DL reference signals are Zadoff-Chu sequences, similar to those used in LTE. The pilots employed by the network-centric and decentralized EKFs for tracking the double-directional parameters are transmitted on a single subcarrier in a frequency-hopping manner spanning 10 MHz. Such UL and DL pilots are transmitted on every 500th TTI. Hence, the UL and DL beaconing rate is 10 beacons/s. The latency between UL and DL pilots in the decentralized scheme is 2 TTIs.

Figure 4 illustrates the performance of both network-centric and decentralized EKFs in tracking the double-directional parameters of the LoS-path in terms of the median error. In the network-centric EKF, the UL beacons received at the ANs are impaired by uncoordinated interference due to UEs transmitting simultaneously roughly 250 m away from the receiving ANs. The performance difference in azimuth-angle estimation at the AN and UE is due to the larger array aperture of the former. However, the elevation angle estimates at the UEs outperform those obtained at the ANs. This is explained by the highly directive beampatterns employed at the ANs, which decrease the effective aperture of the ANs' arrays in the elevation domain. In particular, the beampatterns of the 3GPP patch elements composing the arrays at the ANs are characterized by a large attenuation at the poles, thus decreasing the estimation accuracy that can be obtained for the elevation angles.

In the decentralized EKF, the ANs transmit DL reference signals to eight UEs simultaneously (20 percent of the spatial degrees-of-freedom). Such DL reference signals are impaired by similar pilots transmitted by neighboring ANs (unless being muted). The results in Fig. 4 show that muting neighboring ANs leads to improved performance on the azimuth and elevation angles at the UEs due to reduced DL interference. Such an interference coordination does not influence the performance of the estimated azimuth and elevation angles at the ANs since these parameters are estimated from UL reference signals. The network-centric EKF outperforms the decentralized EKF since all parameters are estimated and tracked jointly. The cost is an increase of the computational complexity and required control channel capacity.

Positioning Accuracy Using Cascaded EKFs

Next we assume that the DoAs and ToAs are acquired using the network-centric EKF-based approach deployed at ANs as described previously with more details available in [4]. These spatial and temporal estimates from all the LoS-ANs can be thereafter fused into 3D UE location estimates using an additional positioning and synchronization EKF, thus assembling a cascaded EKF solution within a network as a whole [3, 4]. In addition to 3D location estimates, the latter EKF can be simultaneously used for tracking the valuable clock offset estimates of unsynchronized UEs and LoS-ANs. In order to demonstrate the performance of the cascaded EKF, two alternative scenarios for synchronization are considered. In the first scenario, the UEs have unsynchronized clocks with drifts whereas the ANs are assumed to be synchronized among each other. In the second scenario, the ANs also have mutual clock-offsets, which are not fundamentally varying over time, whereas the clocks within the UEs are again drifting as mentioned above. Such scenarios are later denoted as Pos&Clock EKF and Pos&Sync EKF, respectively [4].

Considering the radio interface numerology described above and exploiting a constant velocity (CV) motion model for the UEs attached to vehicles with a maximum speed of 50 km/h, the performance of the Pos&Clock and Pos&Sync EKFs are compared with the classical DoA-only EKF using both 4.8 MHz and 9.6 MHz reference signal (RS) bandwidths. Since only automotive applications are considered here, a more appealing 2D positioning approach was used in the evaluations. The 2D positioning results in terms of cumulative distribution functions (CDF) are depict-

ed in Fig. 5 after averaging over multiple random trajectories on the Madrid grid. Based on the results, the cascaded EKFs can provide extremely accurate location estimates for the UEs even in the case of unsynchronized ANs. As expected, Pos&Clock and Pos&Sync EKFs outperform the DoA-only EKF due to the additional ToA estimates. Because of a better time resolution, 9.6 MHz RS bandwidth implies more accurate ToA estimates, and consequently, more accurate positioning can be obtained. Despite the fact that the Pos&Clock EKF is more accurate than the Pos&Sync EKF due to the synchronized ANs, both methods can achieve the envisioned sub-meter positioning accuracy of future 5G networks [6, 7] with a probability of at least 93 percent when using the 9.6 MHz bandwidth. In addition to high-accuracy positioning performance, both Pos&Clock and Pos&Sync EKFs are able to also track the clock offsets of the UEs and ANs with extremely high accuracy. Finally, due to being able to estimate both azimuth and elevation DoAs in addition to ToAs, the positioning EKF can also facilitate 3D and single AN based positioning.[4]

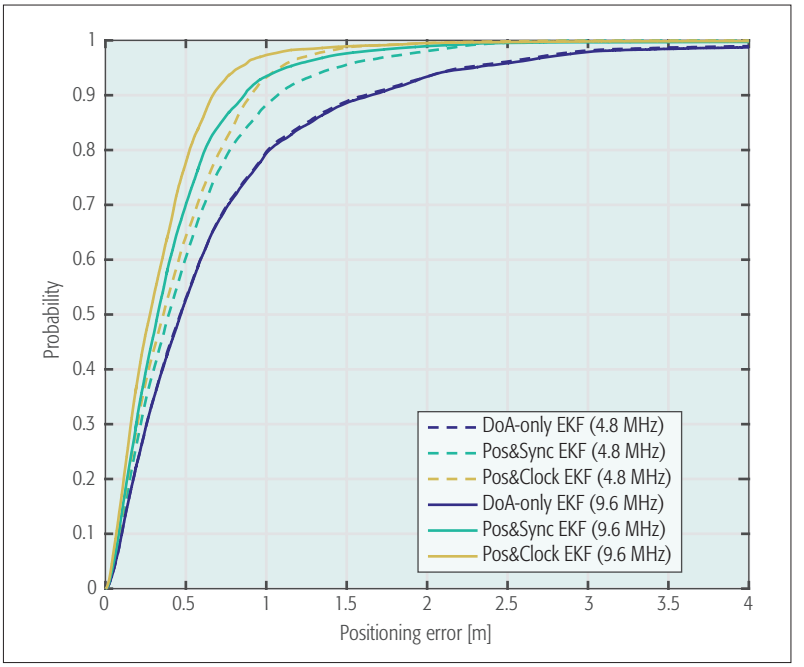


Figure 5. CDFs for 2D positioning errors with 4.8 MHz and 9.6 MHz RS bandwidths over random routes through the Madrid map. Pos&Clock EKF refers to synchronized ANs whereas Pos&Sync EKF refers to unsynchronized network elements.

Location-Based Geometric Beamforming and Mobility Management

Network densification and accurate UE positioning in 5G will also open new opportunities for RRM and MIMO. In particular, multi-user MIMO (MU-MIMO) is seen as a promising solution for 5G as it enables MIMO gains also with simple single antenna UEs. As discussed previously, UEs in UDNs are close to an AN with a high LoS probability. This makes it possible to design and adopt geometric beams at transmitters without the need to estimate the full-band CSIT [9–11]. This is enabled by using the estimated elevation and azimuth angles relative to the AN's coordinate system. The synthesized multi-user multiple input single-output (MU-MISO) matrix can then be formed comprising only LoS-paths for all served UEs. One significant benefit of such a beamforming scheme is that full-band UL reference signals, traditionally employed for obtaining CSIT, can be replaced with narrowband UL pilots. This will allow for substantial energy savings, especially on the UE side, which is a very important aspect in future wideband 5G networks. In addition to transmit beamforming, the location-based approach can also be used for calculating the receive filters at UEs when high-accuracy DoA estimates of the desired signals are available.

In addition to MU-MIMO beamforming, accurate positioning is also a key enabler for a paradigm shift from classical cellular networks toward device-centric borderless networks with centralized control entities. When the network is constantly keeping track of UE locations, it can assign a set of serving ANs for each UE. Then data for each UE is partially or fully available at some small set of nearby ANs as also outlined in [2]. This enables ultra-short latencies and borderless QoE with seamless mobility decreasing handover latencies [10]. Furthermore, such a device-centric mobility approach can reduce the energy and resource consuming cell measurement and reporting burden of legacy cellular systems.

Evaluation Setup

We consider a similar setup as above, with 43 ANs, user density of 1000 users/km2, and all users are dropped with a uniform distribution on the simulated street area. To follow the 3GPP requirements and scenarios for next generation studies [8], a single unpaired 200 MHz TDD carrier is assumed and 30 km/h velocity is used for the UEs. Additionally, the ratio between DL and UL is configured to 4.7:1 in the employed 5G TDD frame structure [11]. Every DL transmission is assumed to start with a precoded DL pilot and maximum ration combining (MRC) is used for calculating the receive filter according to the measured DL pilot. In case of location-based receive beamforming, estimated elevation and azimuth angles relative to the UE's coordinate system are used for calculating the receive filter toward the serving AN. For both location-based transmit and receive beamforming, a two degree measurement error in addition to the UL pilot measurement aging in both elevation and azimuth angles is assumed. UL pilots used for CSIT estimation and positioning are scheduled according to the round-robin scheme. Hence, in the simulated scenario the average CSIT latency is ~3.3 ms. UEs are assigned to be served by the closest AN, that is, a centralized mobility management scheme based on estimated UE locations is assumed.

Performance Results and Comparison of Location-Based and CSI-Based Beamforming

In [11], it was observed that both matched filter (MF) and zero forcing (ZF) precoders work rather well in UDNs, where LoS-paths are dominating over reflections and diffractions. Hence, for this study a block diagonalization (BD) algorithm [15], which can be understood to be an extension of ZF, is chosen instead of conventional ZF.

[4] Video of 3D and single AN-based positioning is available at http://www.tut.fi/5G/COMMAG16.

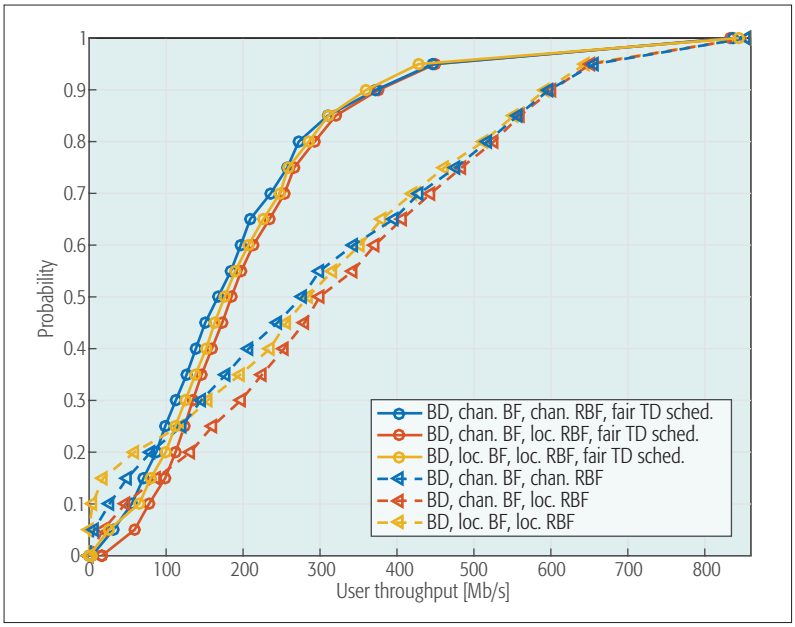


Figure 6. DL user throughput CDFs, over random routes through the Madrid map, with channel/CSI and location-based MU-MIMO transmit beamforming (BF) and receive BF (RBF). Relying only on location information is better on average than using only CSI measurements. The best overall performance is obtained by using channel-based BF and location-based RBF.

An especially attractive feature in BD is that the beams can be optimized for multiantenna receivers enabling better performance of receive filters.

In Fig. 6, CDFs of user experienced DL throughputs are shown with both CSI-based and location-based transmit and receive beamforming schemes. Due to high LoS probability and the dominance of LoS-paths, both CSI-based and location-based beamforming schemes obtain rather similar performance over the whole distribution. Additionally, focusing the receive filter only to LoS-path with location-based receive beamforming outperforms DL pilot based receive beamforming. Furthermore, a 100 percent increase in 5-percentile throughput can be obtained when compared to the CSI-based approach. Since ANs are using the same physical resources for transmitting beamformed DL pilots, DL pilot contamination degrades the performance of CSI-based receive beamforming. In the case of transmit beamforming with ZF-based precoders like BD, better performance at 5-percentile can be obtained with channel-based transmit beamforming due to the fact that there are still a few UEs in NLoS condition toward the serving AN. Thus, the best overall performance is obtained by using channel information for transmit beamforming and location information for the receive filter. Note that the pilot overhead here is the same for all beamforming schemes. However, if pilot overhead caused by full-band reference signals needed in CSI-based beamforming was reduced in the corresponding location-based schemes, the performance would improve in terms of the mean throughput and area capacity as shown in [11]. This is because location-based beamforming schemes do not require full-band reference signals, while narrowband, even single-subcarrier, pilots suffice.

In this example, in order to increase the fairness of BD precoding and to reach the throughput requirement of 50 Mb/s for all users all the time, stated in [5], the scheduling method introduced in [10] is used. This fair time domain (TD) scheduling approach is applied in a way that in every other subframe only a subset of users is chosen as scheduling candidates, in particular the users with the lowest past average throughput. In other subframes the number of simultaneously served users is maximized to increase the total system throughput. The results in Fig. 6 indicate that such scheduling provides less variation in throughputs across the UEs. Moreover, the fair TD scheduling with channel-based transmit beamforming and location-based receive beamforming decreases the simulated area throughput from 1 Tbps/km^2 to 0.65 Tbps/km^2. Hence, when more fair TD scheduling is applied, the total system throughput suffers to a certain extent from favoring users with poor channel conditions over users with high signal-to-interference-plus-noise ratio.

Conclusions and Future Work

The prospects and enabling technologies for high-efficiency device positioning and location-aware communications in dense 5G networks were discussed. It was demonstrated that very high-accuracy 2D/3D positioning and tracking can be accomplished, by adopting DoA and ToA estimation in the ANs together with appropriate fusion filtering in the form of EKF, for example. In general, outdoor positioning accuracies below one meter were shown to be technically feasible. It was also shown that location information can be used efficiently in the radio network, for example, for geometric location-based beamforming, where the needed reference signal overhead is substantially smaller compared to the basic CSI-based beamforming approaches. Thus, extracting and tracking the locations of the user devices in the 5G network can offer substantial benefits and opportunities for location-based services, in general, as well as for enhanced and more efficient communications and radio network management.

References

[1] A. Osseiran *et al.*, "Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project," *IEEE Commun. Mag.*, vol. 52, no. 5, May 2014, pp. 26–35.
[2] Huawei Technologies Co., "5G: New Air Interface and Radio Access Virtualization," 2015; available: http://www.huawei.com/minisite/has2015/img/5g radio whitepaper.pdf; accessed: Nov. 16, 2016.
[3] J. Werner *et al.*, "Joint User Node Positioning and Clock Offset Estimation in 5G Ultra- Dense Networks," *Proc. 2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, Dec. 2015, pp. 1–7.
[4] M. Koivisto *et al.*, "Joint Device Positioning and Clock Synchronization in 5G Ultra-Dense Networks," *IEEE Trans. Wireless Commun.*, vol. 16, May 2017, pp. 2866–81.
[5] NGMN Alliance, "NGMN 5G white paper," 2015; available: https://www.ngmn.org/uploads/media/NGMN 5G White Paper V1 0.pdf; accessed: Nov. 16, 2016.
[6] 5G-PPP, "5G Vision," Feb. 2015; available: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf; accessed: Nov. 16, 2016.
[7] 5G Forum, "5G white paper: New Wave Towards Future Societies in the 2020s," Mar. 2015; available: http://kani.or.kr/5g/whitepaper/ 20155G Forum White Paper Service.pdf; accessed: Nov. 16, 2016.
[8] 3GPP TR 38.913, "Study on Scenarios and Requirements for Next Generation Access Technologies (V1.0.0)," Oct. 2016; available: http://www.3gpp.org/DynaReport/38913.htm; accessed: Nov. 16, 2016.
[9] S. Sand, A. Dammann, and C. Mensing, *Positioning in Wireless Communication Systems*, 1st ed. John Wiley & Sons Ltd., 2014.

[10] P. Kela, J. Turkka, and M. Costa, "Borderless Mobility in 5G Outdoor Ultra-Dense Networks," *IEEE Access*, vol. 3, 2015.
[11] P. Kela *et al.*, "Location Based Beamforming in 5G Ultra-Dense Networks," *Proc. IEEE 84th Vehicular Technology Conference (VTC2016-Fall)*, Montréal, Canada, Sept. 2016.
[12] V. Nurmela *et al.*, "METIS Channel Models," 2015; available: https://www.metis2020.com/wp-content/uploads/METIS D1. 4 v3.pdf; accessed: Nov. 16, 2016]
[13] J. Werner *et al.*, "Performance and Cramer-Rao Bounds for DoA/RSS Estimation and Transmitter Localization using Sectorized Antennas," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, May 2016, pp. 3255–70.
[14] L. Bruno and P. Robertson, "WiSLAM: Improving FootSLAM with WiFi," *Proc. Int'l. Conf. Indoor Positioning and Indoor Navigation (IPIN)*, Sept. 2011, pp. 1–10.
[15] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-Forcing Methods for Downlink Spatial Multiplexing in Multiuser MIMO Channels," *IEEE Trans. Signal Process.*, vol. 52, no. 2, Feb. 2004, pp. 461–71.

Biographies

Mike Koivisto [S'16] (mike.koivisto@tut.fi) received the M.Sc. degree in mathematics from Tampere University of Technology (TUT), Finland, in 2015, where he is currently pursuing the Ph.D. degree. From 2013 to 2016, he was a research assistant with TUT. He is currently a researcher with the Laboratory of Electronics and Communications Engineering, TUT. His research interests include positioning, with an emphasis on network-based positioning and the utilization of location information in future mobile networks.

Aki Hakkarainen received the M.Sc. and Ph.D. degrees in communication engineering from Tampere University of Technology (TUT), Tampere, Finland, in 2007 and 2017, respectively. From 2007 to 2009, he was an RF design engineer with Nokia, and from 2009 to 2011, a radio system specialist with Elisa. He is currently a researcher with the Laboratory of Electronics and Communications Engineering, TUT. His research interests include digital signal processing methods for localization and RF impairment mitigation.

Mário Costa [S'08, M'13] (mariocosta@huawei.com) received the M.Sc. degree (Hons.) in communications engineering from the Universidade do Minho, Portugal, in 2008, and the D.Sc. (Tech.) degree in electrical engineering from Aalto University, Finland, in 2013. In 2014, he was a visiting post-doctoral research associate at Princeton University. Since 2014, he has been with Huawei Technologies Oy (Finland) Co., Ltd., as a senior researcher. His research interests include statistical signal processing and wireless communications.

Petteri Kela [M'15] (petteri.kela@huawei.com) received the M.Sc. degree at the University of Jyväskylä, Finland in 2007. From 2001 to 2007 he was with the Department of Mathematical Information Technology at the University of Jyväskylä. Since graduation, he has been working for companies such as Nokia and Renesas. Since July 2013 he has been with Huawei Technologies Oy (Finland) Co. Ltd as a senior researcher. Besides daily research work he is also a part-time doctoral student with Aalto University School of Electrical Engineering.

Kari Leppänen received the M.Sc. and Ph.D. degrees from Helsinki University of Technology, Finland, in 1992 and 1995, respectively, majoring in space technology and radio engineering. He was with the National Radio Astronomy Observatory, USA, with the Helsinki University of Technology, Finland, with the Joint Institute for VLBI, The Netherlands, and the Nokia Research Center, Finland. He currently leads the 5G Radio Network Technologies Team at Huawei Technologies Oy (Finland) Co., Ltd, Stockholm and Helsinki.

Mikko Valkama [S'00, M'01, SM'15] received his M.Sc. and Ph.D. degrees (both with honors) in electrical engineering from Tampere University of Technology in 2000 and 2001, respectively. In 2003, he worked as a visiting researcher with the Communications Systems and Signal Processing Institute at San Diego State University, California. Currently, he is a full professor and department vice-head at the Laboratory of Electronics and Communications Engineering at Tampere University of Technology. His general research interests are in radio communications and radio networks.

Extracting and tracking the locations of the user devices in the 5G network can offer substantial benefits and opportunities for location-based services, in general, as well as for enhanced and more efficient communications and radio network management.

ACCEPTED FROM OPEN CALL

QoE-Aware Scalable Video Transmission in MIMO Systems

Soo-Jin Kim, Gee-Yong Suk, Jong-Seok Lee, and Chan-Byoung Chae

The authors summarize the latest video transmission technologies that are based on SVC over MIMO systems with cross-layer designs. To provide insight into video transmission in wireless networks, they investigate UEP solutions in the delivering of video over massive MIMO systems.

ABSTRACT

An important concept in wireless systems has been QoE-aware video transmission. Such communications are considered not only connection-based communications but also content-aware communications, since the video quality is closely related to the content itself. It becomes necessary, therefore, for video communications to utilize a cross-layer design (also known as joint source and channel coding). To provide efficient methods of allocating network resources, the wireless network uses its cross-layer knowledge to perform UEP solutions. In this article, we summarize the latest video transmission technologies that are based on SVC over MIMO systems with cross-layer designs. To provide insight into video transmission in wireless networks, we investigate UEP solutions in the delivering of video over massive MIMO systems. Our results show that in terms of QoE, SVC layer prioritization, which was considered important in prior work, is not always beneficial in massive MIMO systems; consideration must be given to the content characteristics.

INTRODUCTION

With smart mobile devices dominating the world, wireless data traffic has increased exponentially. Keeping pace with such growth has been video traffic consumption, inlcuding video on demand (VoD), IPTV, video call, video streaming, video sharing, and so on. An important research topic then is how to best maximize users' satisfaction with delivered video content.

In the past, physical and application layer technologies have been considered as separate dimensions. Physical layer technologies for fourth generation (4G) and 5G have been developed mostly as a way of increasing capacity; application layer technologies for video coding have been developed as a way to increase coding efficiency. This is not, however, the optimal way to increase efficiency in terms of the quality of transmitted video over wireless communications.

The degradation of video quality is caused by two major factors: coding artifacts and network artifacts. Coding artifacts are caused by the application of lossy video data compression, which includes blurring, blockiness, and ringing artifacts. Network artifacts are caused by packet losses preventing packets of video data from reaching their destinations. Such losses are caused by packet jitter, delay, dropping, and so forth. These two types of artifacts are simultaneously involved in determining end-user video quality. Therefore, it is important to first understand their combinational impact and then develop an optimal way of allocating resources to maximize users' satisfaction in video transmission. A natural choice to enhance the overall efficiency of video transmission in wireless networks is a cross-layer design.

In the physical layer, one way of expanding bandwidth and reducing error rate is with multiple-input multiple-output (MIMO) along with the aid of techniques known as spatial multiplexing and diversity [1]. A powerful video compression technique that is well associated with MIMO systems is scalable video coding (SVC). In the application layer, SVC organizes the video data into a layered structure, enabling extraction of multiple video streams having different bit rates and levels of quality. For example, the base layer presents base quality; enhancement layers — relying on the base layer's quality — provide higher quality. The adaptability and scalability of SVC allow the selection of desirable target quality within the network constraints. Based on these two technologies, many studies have tried to develop video transmission frameworks that can find the optimal balance between efficiency and quality. In the prior work, cross-layer-designed video transmission frameworks, which are described later, often adopted unequal error protection (UEP) solutions to efficiently allocate the resources.

Popularly used UEP techniques are summarized below.

Adaptive Modulation and Coding (AMC): controls modulation order and coding rate per time slot, sub-block, or sub-channel. The modulation order of a digital communication scheme is determined by the number of different symbols that can be transmitted using it. A higher modulation order refers to a higher throughput, although it is more vulnerable to error than a lower modulation order. The code rate or error correction code (ECC) normally refers to the proportion of the data stream that is not redundant. A higher code rate means higher throughput but lower error correction.

Adaptive Channel Selection (ACS): assigns sub-channels for certain data transmissions. A certain SVC quality layer is often assigned to a specific sub-channel of the user. The ACS technique makes it easy to give priority to an SVC layer.

Digital Object Identifier:
10.1109/MCOM.2017.1600279

The authors are with Yonsei University; C.-B. Chae and J.-S. Lee are co-corresponding authors.

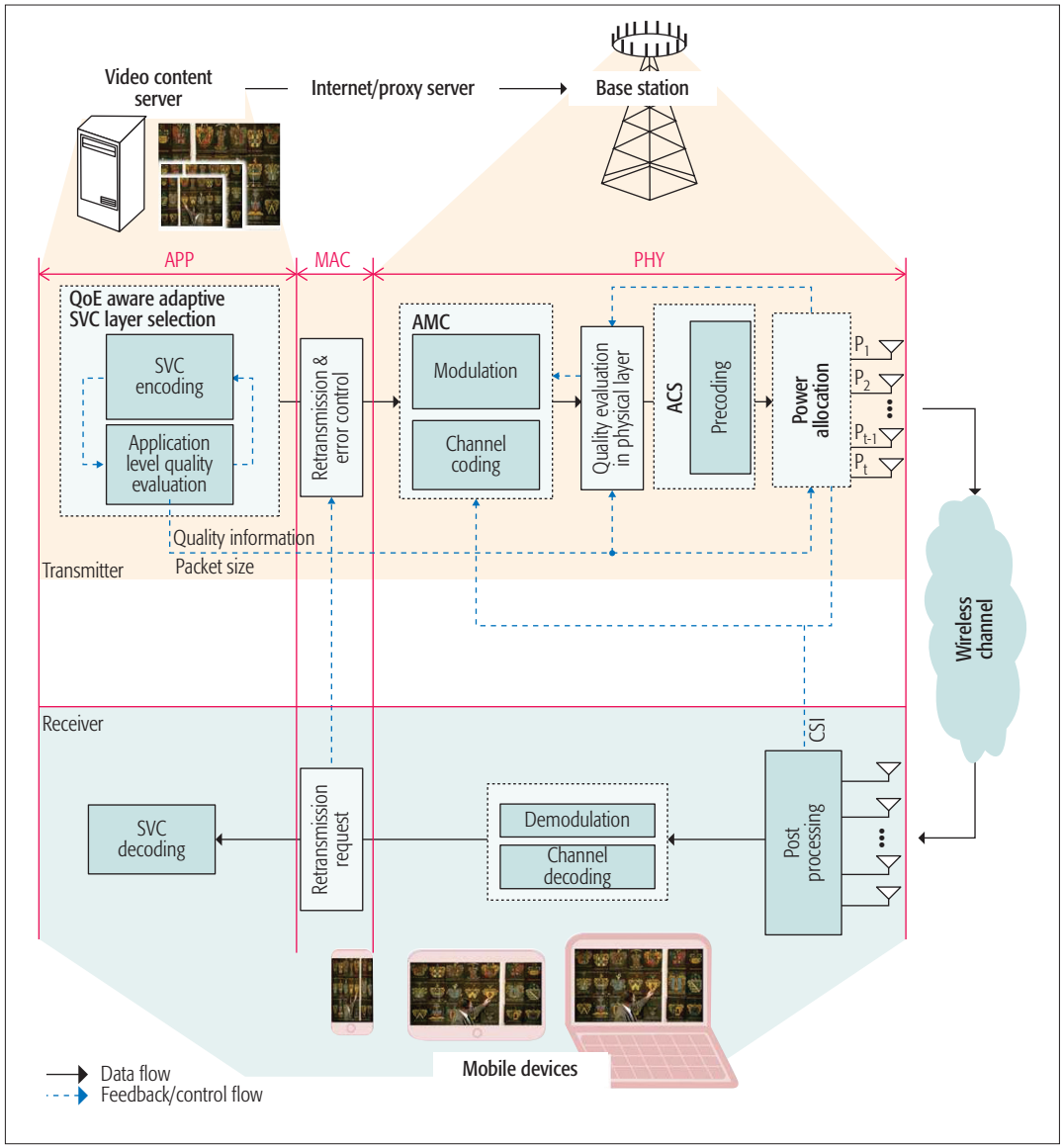


Figure 1. Overview of a QoE-aware video transmission system based on the cross-layer design.

Blocks for quality evaluation are located in the application and physical layers to predict the video quality before sending. These can, however, be located at any place between the physical and application layers depending on the purpose of the video transmission framework.

Power Allocation: assigns different transmit powers to the channels, sub-channels, or users. Assigning a larger power to a channel or user results in lower error rate or higher throughput of the channel or user.

Figure 1 illustrates a QoE-aware video transmission system based on the cross-layer design. In the figure, blocks for the aforementioned UEP techniques are shown on the transmitter side. In addition, blocks for quality evaluation are located in the application and physical layers to predict the video quality before sending. These can, however, be located at any place between the physical and application layers depending on the purpose of the video transmission framework.

In this article, we deal with the issue regarding how to optimize quality of experience (QoE) of end users for SVC transmission over massive MIMO systems. In particular, our contributions are summarized as follows:

•We provide a broad discussion about video transmission algorithms for MIMO systems based on cross-layer design. This enables our readers to understand current trends in this field.

•Unlike prior work, this work conducts SVC transmission in massive MIMO systems, which is unique and the first of its kind in the literature.

•We investigate the error characteristics of massive MIMO systems under a Rayleigh fading channel, which turns out to be different from that of MIMO systems. We derive the bit error probability formulation in massive MIMO systems with a zero-forcing (ZF) precoder. This allows the estimation of the error rate prior to transmission without any additional feedback, which saves resources that would otherwise have been used for limited feedback.

•We show that different approaches should be considered when applying UEP techniques to massive MIMO systems. Unlike conventional MIMO systems, in massive MIMO systems, the priority exists not only at the base layer but also at other layers. With our simulation of unequal power allocation in massive MIMO systems, we show that to take full advantage of UEP for improved video quality at the user side, engineers must consider "unconventional" power allocation between the layers.

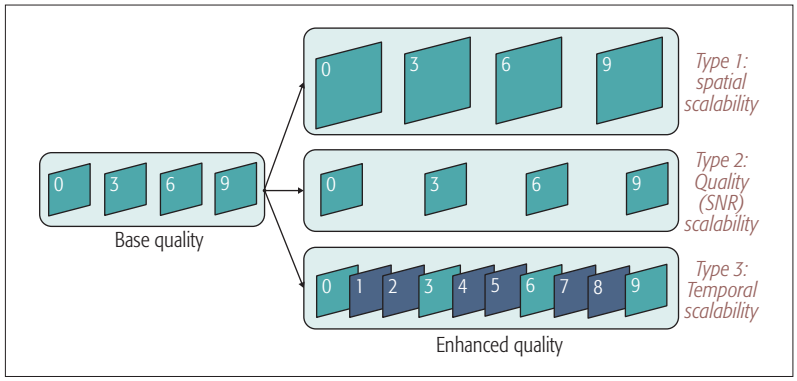


Figure 2. Three representative types of scalability.

•Additionally, we introduce regression analysis as a possible approach to better clarify the relationship between video quality and assigned transmit power per SVC layer with content information. We believe this would serve as a basic guideline for future research.

The rest of the article is organized as follows. The following section describes the basic concepts of MIMO, SVC, and error control methods in cross-layer design. Then we explain video transmission techniques in MIMO systems. Following that, we present our error rate analysis and a power allocation scheme in massive MIMO systems. Finally, we conclude the article.

Basic Concepts

Depending on the system optimization approaches, different methods can be selected for cross-layer design. This section explains the background of multiple antenna techniques and briefly goes over error control methods and QoE-related knowledge of SVC.

MIMO

In MIMO systems, the base station (BS) transmits a message signal to one or more users by using multiple antennas [2]. It is important to suppress signal interference among channels. Precoding techniques are popularly used for this. Here, availability of the channel state information at the transmitter (CSIT) is considered important, particularly in video transmission, because a key to predicting the amount of video quality degradation is prior knowledge of network parameters, making it possible to utilize UEP solutions. Thus, perfect or partial availability of CSIT is usually assumed for video transmission in MIMO systems.

A popular method of precoding based on CSIT is singular value decomposition (SVD). In this approach, the channel matrix is diagonalized by taking SVD and removing the two unitary matrices through multiplication as a precoder and post-processing to the transmitter and receiver, respectively.

Data streams are then sorted in decreasing order without creating any interference. To maximize system capacity, SVD is often combined with power allocation algorithms, for example, water-filling (WF). WF implies allocating more power to the channels with higher signal-to-noise ratios (SNRs).

There are other precoding techniques commonly used in multiuser MIMO systems. One example is ZF. ZF often involves channel inversion, using the pseudo-inverse of the channel matrix or other generalized inverses. Then only diagonal terms remain, and the removed are off-diagonal terms, which are interference. As a result, this nulls the inter-user interference and achieves, when equal power is allocated, an equal received SNR for each data stream.

SVC

SVC is a useful technique to compress video content into a bitstream from which several decodable video streams can be extracted. It basically adopts a layered structure for compression, that is, a bitstream is composed of a base layer representing the lowest quality version of the video data and one or more enhancement layers used to produce enhanced quality versions. Figure 2 illustrates three types of scalability: spatial scalability, quality (or SNR) scalability, and temporal scalability [3]. These refer to the possibility of extracting video sequences having different spatial resolutions, different image quality levels, and different frame rates, respectively. Combinations of the three scalability options provide various versions of the video sequence with the corresponding bit rates and quality.

Once video content has been encoded with SVC, the bitstream can, without the need for re-encoding, be used for efficient and adaptive transmission over error-prone networks. Suppose that the network condition from the server to the client is too poor to transmit the whole bitstream, or that the client's device is incapable of decoding and displaying the highest-quality version of the content. In such cases, only part of the bitstream can be transmitted to the client to reduce the bit rate (and consequently quality) and meet the network or device constraint. Furthermore, if the network condition changes over time, the amount of the video data to be kept or discarded can be adaptively adjusted.

Error Control Methods in Cross-Layer Design

In the physical layer, the likely data rate and error robustness of the system may be determined by using modulation and coding (MC) scheme index values. If too many errors are being experienced, the MC value can be lowered, thus reducing the error rate but at the cost of slower data rate. An AMC scheme is performed to find the optimal modulation order and coding rate.

In the application layer, erroneous packets need to be corrected for decoding. A simple way to do this is to replace the erroneous frame with a copy of the previous frame.

Video Transmission Techniques in MIMO

Table 1 summarizes state-of-the-art video transmission algorithms for MIMO systems based on cross-layer design. Generally, according to the MIMO option one chooses, different error and transmission rates would be achieved. Unlike SVD-WF, which, by the MIMO option itself, determines power control, ZF beamforming (ZFBF) is able to independently control its power allocation. Thus, using ZFBF would guarantee a high degree of freedom and also yield advantages of being able to control the error rate of a channel. Given a MIMO option, whether to use ACS or adaptive modulation depends on the target system and

Ref.	MIMO options	UEP	Channel coding	Scalability	Quality metric	Optimization approaches
[4]	SVD-WF (perfect CSI)	ACS, AM, power allocation	Reed-Solomon	S, Q, T	PSNR	Maximizing the total transmission rate by selecting power and modulation within the target bit error rate constraint
[5]	SVD, Codebook (partial CSI)	AMC, subcarrier allocation	None	Q, T	PSNR	Maximizing the average SINR at the receivers and maximizing the transmission rate of each subcarrier by selecting MC within the SINR constraint
[6]	ZFBF	AM, power allocation	None	Q, T	PSNR	Maximizing the network efficiency by selecting bit rate, power, and modulation within the total transmit power constraint
[7]	SVD-WF	ACS, AMC, power allocation	RCPC	S, Q, T	PSNR	Minimizing the total amount of distortions by selecting MC within the total transmit power constraint
[8]	SVD	ACS, AM, power allocation	Reed-Solomon	Q, T	PSNR, SSIM	Maximizing the quality by finding optimal power per channel within the total transmit power constraint

Table 1. Summary of video transmission technologies with SVC in MIMO systems. (S: spatial scalability, Q: quality scalability, T: temporal scalability, AM: adaptive modulation, RCPC: rate-compatible punctured convolution codes).

trade-off issue. In the case of ACS, because high code rate means high redundancy, there is some decrease in transmission rate. On the other hand, in the case of AM, error rate increases when modulation order gets higher and vice versa.

In [4], the authors presented a quality of service (QoS)-aware SVC transmission framework in MIMO systems. In this framework, the authors made two assumptions. First, the data rate of the base layer should be maintained at all times to guarantee the minimum video QoS. Second, different protection levels are implemented between the enhancement layers, as they have different priorities. To maximize the QoS of SVC video, adaptive modulation and power allocation were adopted. As a result, the MIMO capacity is fully enhanced, and different channel quality between the sub-channels is allowed. To guarantee the data rate of the base layer, the authors suggested to always assign the best quality sub-channel to the base layer and allocate power with fixed modulation. The rest of the power, which subtracts the assigned power from the total transmit power, is adaptively allocated to the enhancement layers. Adaptive modulation is only implemented for the enhancement layers. Their optimization approach maximizes the total transmission rate by selecting power and modulation orders within the target bit error rate constraint. The power allocation step for the base and enhancement layers is repeated until the optimization approach bounds to the maximum data throughput based on a target bit error rate. They measured the performance of the framework in terms of the average peak SNR (PSNR), which is a typical image quality metric.

In [5], the authors also proposed a cross-layer framework for efficient broadcasting of scalable video over downlink MIMO orthogonal frequency-division multiplexing (OFDM) systems. They considered the heterogeneity of both video sources and wireless channels of users. That is, they allocated resources not only between users but also between video layers using UEP. The goal was to maximize the average PSNR of all users while meeting the base layer's bandwidth constraint, where PSNR of a video stream is calculated using a rate-quality model. For this, AMC, subcarrier allocation, and selection of SVD (with or without a codebook technique) were performed per user and per SVC video layer.

Another multiuser MIMO-OFDM framework was proposed in [6]. These authors, unlike in [5], used adaptive modulation and power allocation to maximize network efficiency and fairness between users. They employed ZFBF since it supports close-optimal capacity and is simple to implement. The authors also considered MAX-MIN fairness for the base layer for every user. This way all users fairly receive their base layers. The authors then exploited a throughput-maximizing scheme for the enhancement layers. To reflect the visual experience for multiple users, a utility function was used, which takes into account the characteristics of different video content. The utility function was maximized by selecting an optimal power and modulation order of the enhancement layer sub-channels within the constraint of the total transmit power. It was shown that the framework yields better video quality in terms of average PSNR than other frameworks such as round-robin, link gain-based resource allocation, and multicarrier maximum sum rate.

The authors in [7] sought an optimal solution for SVC video transmission over MIMO channels. They developed a distortion model for SVC by considering loss of enhancement quality layers, drift error by loss of enhancement quality layers, and loss of the base quality layer. In the model, three physical layer parameters — power allocation parameters (w), ECC rates (r), and modulation order (m) — are related to the total distortion in terms of the sum of the mean square error (MSE) over pixels of each video frame. A solution minimizing the total distortion is obtained by choosing optimal combinations (w, r, m). The authors also developed a power allocation algorithm with rapid convergence using a fixed modulation order and ECC rate.

The authors in [8] laid out an approach for a cross-layer design for video delivery to optimize QoE of end users. The scheme jointly considers both transmission errors in the physical layer and video source coding characteristics in the application layer. To maximize the QoE, they defined a utility function that multiplies an SVC quality function and a frame correction rate function. A

It is mostly assumed that the base layer contains the most important information and thus must have the highest priority. However, we wonder whether the SVC layer priorities still hold for massive MIMO systems. Studies have yet to be carried out on SVC video transmission over massive MIMO systems.

	Adaptive modulation (AM)	Adaptive coding rate (AC)	Adaptive channel selection (ACS)	Power allocation or subcarrier allocation	MIMO configuration
[4]	○	×	Not specified	○	4 × 4 MIMO
[5]	○	○	Not specified	○ (subcarrier)	OFDM-MIMO (multiuser)
[6]	○	×	Not specified	○	OFDM-MIMO (multiuser-fairness)
[7]	○	○	○	○	4 × 4 MIMO
[8]	○	×	○	○	4 × 4 MIMO

Table 2. Usage of UEP methods in introduced MIMO systems.

near-optimal solution determining parameters of ACS, adaptive modulation, and power allocation was achieved by decomposing the original optimization problem into several convex optimization sub-problems. The authors showed the near optimality of their proposed scheme, in terms of measured utilities, by comparing it to the exhaustively searched optimal solutions. Simulations demonstrated the effectiveness of their scheme in terms of PSNR and structural similarity (SSIM) [9], which is a representative perceptual quality metric.

The aforementioned studies have been developed as a way to enhance the quality for end users. It was believed that maximizing transmission rate (capacity) is equivalent to maximizing the quality (e.g., [4–6]). However, the discrepancy between them has been recognized, and thus direct measures of video quality have been adopted recently (e.g., minimizing distortions [7], maximizing QoE [8]). In addition, PSNR was frequently used as a measure of video quality, whereas more perceptually meaningful measures such as SSIM began to be used (e.g., [8]).

In summary, Table 2 clearly distinguishes which UEP methods are used in the introduced frameworks. Combination of multiple UEP methods might increase adaptability, but it surely increases computational complexity. The service operator should have a choice among video delivery frameworks by considering not only the performance of the framework but also user scenarios, MIMO configurations, computational complexities, and so on.

As discussed above, it is mostly assumed that the base layer contains the most important information and thus must have the highest priority [4–8]. However, we wonder whether the SVC layer priorities still hold for massive MIMO systems. Studies have yet to be carried out on SVC video transmission over massive MIMO systems. The next section describes our initial studies on this issue. We first discuss error behavior in massive MIMO systems, which differs from that in (non-massive) MIMO systems. Then we examine the effectiveness of UEP solutions based on the SVC layer priorities in massive MIMO systems.

Video Transmission in Massive MIMO

Error Characteristics in Massive MIMO Systems

Massive MIMO systems have been proposed such that each BS is equipped with orders of magnitude more antennas (e.g., 32, 64, 128, or more). More dramatic multiplexing or diversity gains are possible when the number of antennas at the BS (N_t) is significantly larger than the number of users (K), that is, $K \ll N_t$. We consider that a massive MIMO system consists of $KN_r \times N_t$ channels with K users and N_r receive antennas for each user. With an increase in the number of antennas at the BS, linear precoders are shown to be near-optimal in terms of throughput [10]. Thus, for simplicity, ZF is used as a precoder.

For massive MIMO systems, using the law of large numbers, the received SNR for each data stream of the kth mobile station (MS) is expressed in terms of the number of antennas, transmit power, and number of users: that is, $P_{k,i}(N_t - KN_r)$, while $P_{k,i}$ means transmit power in the ith stream for the kth MS [11]. Furthermore, the bit error probability ($\overline{P}_b$) in massive MIMO systems with a ZF precoder can be expressed as follows:

$$\overline{P}_b \approx \frac{1}{\log_2 M}\operatorname{erfc}\left\{\sqrt{\frac{P_{k,i}(N_t - KN_r}{KN_r}}\sin\frac{\pi}{M}\right\}$$

where M is the modulation order. Thus, the error probability in massive MIMO systems is sensitive to changes with respect to power ($P_{k,i}$).

This error probability can be transformed into packet error rate (PER) by merging the effect of the length of an SVC video packet; that is, PER = $1 - (1 - P_b)^L$, where L is the packet length [12]. The size of each packet inherently varies depending on the amount of information in a video frame. Since the packet length has an exponential influence on PER, the PER rapidly increases as the packet length increases.

Perceived Quality by Using Unequal Power Allocation

To examine the effectiveness of UEP in a massive MIMO system [13], we used six original video sequences that have different spatial and temporal content complexities. They were chosen from the SVT High Definition Multi Format Test Set [14] (*CrowdRun* and *ParkJoy*) and the Live Video Quality Database [15] (*pa1*, *mc1*, *sf1*, and *sh1*). In our work, we encoded the base layer with a resolution of 176 × 144 pixels at 15 fps, where the quantization parameter (QP) value was set to 28. For the enhancement layer we used a resolution of 352 × 288 pixels at 30 fps and a QP value of 26. These two layers are received through separate receive antennas (i.e., $N_r = 2$).

We applied ACS and power allocation and used ZF precoding. In our simulation, we set

P_k = 5.50 dB, which corresponds to the total PER around 1 percent when equal powers are allocated (i.e., $P_{k,1} = P_{k,2}$ = 2.48 dB). The power range for UEP was set as 1.05 dB to 3.58 dB, which results in PER in the range of 1 to 3 percent. This PER range can often be obtained in the typical wireless channels. We simulated several combinations of $P_{k,1}$ and $P_{k,2}$ in the chosen power range for giving unequal protection to the SVC layers.

Figure 3 shows representative results of our simulation in terms of SSIM for measuring video quality. In Fig. 3a, the maximum SSIM is obtained when the base layer power is higher than the other. In Fig. 3b, the maximum SSIM is obtained when a higher power is allocated to the enhancement layer than to the base layer. In Fig. 3c, on the other hand, UEP never results in better quality than the equal power allocation. Among the three sequences, *ParkJoy* and *mc1* have the largest and smallest average packet sizes of the base layer, respectively. This implies that the sizes of packets of the base layer play an important role in determining the video quality with respect to the power allocated to each SVC layer. As shown previously, the massive MIMO system shows a large change in bit error probability even for a slight change in power. Furthermore, the effect of a bit error, in terms of PER, increases exponentially with respect to the packet size.

Hence, it is true that the base layer is important, but this does not mean that the base layer always needs more power, as suggested by the previous work in MIMO systems, to maximize the overall quality. Thus, the effectiveness of a priority-based power allocation algorithm for SVC could, in practice, be interfered with by other factors such as network characteristics and content information.

Next, we attempt to model the relationship between the transmit power and the perceived quality based on the results in Fig. 3. We note that the curves in the figure can be modeled by quadratic functions. Then the three curves can be considered as horizontal translations depending on the content characteristics. Therefore, we use the following function for regression:

$$SSIM = a \cdot P_{k,1}^2 + b \cdot P_{k,1} + c \cdot SI + d \cdot TI + e \qquad (1)$$

where, $P_k = P_{k,1} + P_{k,2}$ is the total transmit power of the kth user, and spatial information (SI) and temporal information (TI) are measures of content complexity in the spatial and temporal domains, respectively [16].

The five model parameters were determined as a = –9.8301, b = –8.5383, c = 0.3045, d = –0.0042, and e = 15.3376. The performance of the regression model was measured as 0.92 in terms of Pearson correlation coefficient. This model can be used to obtain the optimal power allocation between the two SVC layers for the given content in order to maximize the perceived quality of the user. Figure 4 shows the snapshots of the transmitted video, ParkJoy, when transmitted with unequal power allocation and with conventional equal power allocation. From this result, we can see that the proposed approach is applicable for finding the best quality for given P_k by allocating different power per SVC layer (i.e., $P_{k,i}$). By demonstrating the quality difference between the video transmitted with the proposed algorithm and the other without the algorithm, we clarify the significance of the issue.[1] Note that this is our preliminary result for the regression model with only three contents. For our future work, we will advance our study with various parameters, network conditions, contents, and so forth.

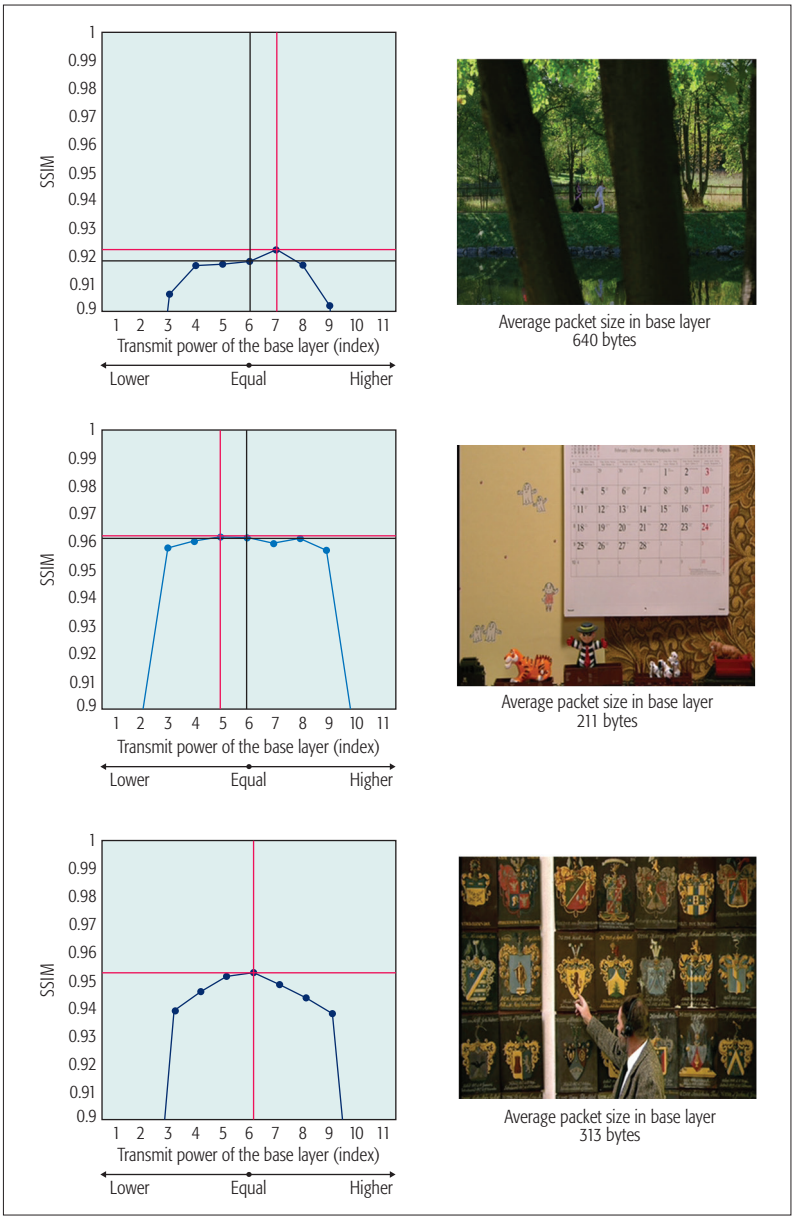


Figure 3. SSIM vs. transmit power of the base layer when the total transmit power is 5.50˜dB. The cross point of the black vertical and horizontal lines indicates equal power allocation (2.48dB) for the base layer and the enhancement layer. The cross point of the red vertical and horizontal lines indicates the case showing the highest SSIM value. A 'lower' (or 'higher') region means that the transmit power of the base layer is lower (or higher) than the transmit power of the enhancement layer. Thumbnails of the corresponding video sequences are also shown. (a) *ParkJoy* (b) *mc1* (c) *sh1*.

Conclusion

In this article, we have investigated the problem of QoE-optimized SVC video transmission over massive MIMO systems. We have first reviewed the state-of-the-art methods for SVC transmis-

[1] The full video comparison is available at http://www.cbchae.org/

Figure 4. Example snapshots of the transmitted video, ParkJoy: a) with the proposed algorithm (which showed the best quality); b) without the algorithm.

sion in MIMO, which mostly adopted UEP based on SVC layer priority. However, we argue that such approaches may not be optimal for massive MIMO systems. Although massive MIMO channels provide a dramatic increase in spectral efficiency and error robustness, with only a small change in the amount of transmit power, PER changes drastically. The massive MIMO channel error characteristic and the amount of information of content have been combined to yield the formula of PER. Our experimental results suggest that priority between SVC layers does exist, but the highest priority must not necessarily be given to the base layer. Depending on the content characteristics, the base or enhancement layer has priority, or both layers have the same priority. Unlike MIMO systems, both system and content characteristics impact the effectiveness of UEP solutions.

This work represents an initial study into SVC transmission in massive MIMO systems, providing guidelines for developing cross-layer video transmission frameworks in massive MIMO systems. Starting with this result, we need to find optimal resource allocation solutions for SVC transmission in massive MIMO systems. It is also necessary to explore various scenarios. In this article, for example, we have only considered video transmission based on broadcasting. However, if the BS has to support heterogeneous devices or is multicasting, where data are sent from multiple sources to multiple destinations, we should consider UEP methods for multi-user or multi-content scenarios while SVC layer priority per user is considered simultaneously. To elevate the video transmission in massive MIMO systems, we will more thoroughly investigate the relationship between error probability and QoE in our future work.

Acknowledgment

This work was in part supported by the MSIP under the "ICT Consilience Creative Program" (IITP-2017-2017-0-01015), the ICT R&D Program of MSIP/IITP (2015-0-00294).

References

[1] D. Gesbert *et al.*, "Shifting the MIMO Paradigm: From Single User to Multiuser Communications," *IEEE Sig. Proc. Mag.*, vol. 24, no. 5, Oct. 2007, pp. 36–46.
[2] E. Larsson *et al.*, "Massive MIMO for Next Generation Wireless Systems," *IEEE Commun. Mag.*, vol. 52, no. 2, Feb. 2014, pp. 186–95.
[3] J.-S. Lee *et al.*, "Quality Assessment of Multidimensional Video Scalability," *IEEE Commun. Mag.*, vol. 50, no. 4, Apr. 2012, pp. 38–46.
[4] D. Song and C. W. Chen, "Maximum-Throughput Delivery of SVC-Based Video over MIMO Systems with Time-Varying Channel Capacity," *J. Visual Commun. Image Represent.*, vol. 19, no. 8, Dec. 2008, pp. 520–28.
[5] Z. Yang and X. Wang, "Scalable Video Broadcast over Downlink MIMO-OFDM Systems," *IEEE Trans. Circuits Systems Video Tech.*, vol. 23, no. 2, Feb. 2013, pp. 212–23.
[6] M. Li, Z. Chen, and Y.-P. Tan, "Scalable Resource Allocation for SVC Video Streaming over Multiuser MIMO-OFDM Networks," *IEEE Trans. Multimedia*, vol. 15, no. 7, Nov. 2013, pp. 1519–31.
[7] W. Hamidouche *et al.*, "Optimal Resource Allocation for Medium Grain Scalable Video Transmission over MIMO Channels," *J. Visual Commun. Image Represent.*, vol. 24, no. 3, Apr. 2013, pp. 373–87.
[8] X. Chen *et al.*, "A Near Optimal QoE-Driven Power Allocation Scheme for Scalable Video Transmissions over MIMO Systems," *IEEE J. Sel. Topics Sig. Proc.*, vol. 9, no. 1, Feb. 2015, pp. 76–88.
[9] W. Zhou *et al.*, "Image Quality Assessment: From Error Visibility to Structural Similarity," *IEEE Trans. Image Proc.*, vol. 13, no. 4, Apr. 2004, pp. 600–12.
[10] G. Caire and S. Shamai, "On the Achievable Throughput of a Multiantenna Gaussian Broadcast Channel," *IEEE Trans. Info. Theory*, vol. 49, no. 7, July 2003, pp. 1691–1706.
[11] Y.-G. Lim, C.-B. Chae, and G. Caire, "Performance Analysis of Massive MIMO for Cell-Boundary Users," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, Dec. 2015, pp. 6827–42.
[12] A. Goldsmith, *Wireless Communications*, Cambridge Univ. Press, 2004.
[13] S.-J. Kim, C.-B. Chae, and J.-S. Lee, "On Unequal Power Allocation for Video Communications Using Scalable Video Coding in Massive MIMO Systems," *Proc. IEEE Int'l. Symp. Multimedia*, Dec. 2014, pp. 147–50.
[14] The SVT High Definition Multi Format Test Set, IETF; http://www.its.bldrdoc.gov/vqeg.
[15] A. K. Moorthy *et al.*, "Video Quality Assessment on Mobile Devices: Subjective, Behavioral and Objective Studies," *IEEE J. Sel. Topics Sig. Proc.*, vol. 6, no. 6, Oct. 2012, pp. 652–71.
[16] ITU-T Rec. P.910, "Subjective Video Quality Assessment Methods for Multimedia Applications," 2008.

Biographies

Soo-Jin Kim received her B.S. degree in computer engineering from Kwangwoon University, Korea, in 2005. She has been a graduate student in the School of Integrated Technology, Yonsei University, in Korea since 2012. Before joining Yonsei, she was with LG Electronics and KT for 7.5 years as a research engineer from 2005 to 2012. Her research interests include the cross-layer optimizations between the channel coding and source coding for multimedia delivery in mobile communications.

Gee-Yong Suk received his B.S. degree in electrical and electronics engineering from Yonsei University in 2016. Now, he is a graduate student in the School of Integrated Technology, Yonsei University. His research interests include millimeter-wave communications, MIMO communications, 5G networks, molecular communications, and estimation theory.

Jong-Seok Lee [SM'14] received his Ph.D. degree in electrical engineering and computer science from the Korea Advanced Institute of Science and Technology. He was a research scientist with the Swiss Federal Institute of Technology (EPFL), Lausanne, Switzerland. He is currently an associate professor with the School of Integrated Technology, Yonsei University. He has authored or coauthored more than 100 publications. His research interests include multimedia signal processing and machine learning. He currently serves as an Editor for *IEEE Communications Magazine* and *Signal Processing: Image Communication*.

Chan-Byoung Chae [SM'12] is the Underwood Distinguished Professor in the School of Integrated Technology, Yonsei University. Before joining Yonsei University, he was with Bell Labs, Alcatel-Lucent, Murray Hill, New Jersey, as a member of technical staff, and Harvard University, Cambridge, Massachusetts, as a postdoctoral research fellow. He received his Ph.D. degree in electrical and computer engineering from the University of Texas at Austin in 2008. He was the recipient/co-recipient of the Best Young Professor Award from Yonsei University (2015), the IEEE INFOCOM Best Demo Award (2015), the IEIE/IEEE Joint Award for Young IT Engineer of the Year (2014), the KICS Haedong Young Scholar Award (2013), the *IEEE Signal Processing Magazine* Best Paper Award (2013), the IEEE ComSoc AP Outstanding Young Researcher Award (2012), the IEEE VTS Dan. E. Noble Fellowship Award (2008), and two Gold Prizes (1st) in the 14th/19th Humantech Paper Contest. He currently serves as an Editor for *IEEE Transactions on Wireless Communications*, *IEEE Communications Magazine*, *IEEE Wireless Communications Letters*, *IEEE/KICS Journal of Communications Networks*, and *IEEE Transactions on Molecular, Biological, and Multi-Scale Communications*.

ACCEPTED FROM OPEN CALL

Toward Interoperability of Smart Grids

Dae-Kyoo Kim, Alaa Alaerjan, Lunjin Lu, Hyosik Yang, and Hyuksoo Jang

There has been growing interest in adopting publish-subscribe communication for improved quality of communication in smart grids. However, adopting publish-subscribe communication requires resolving potential interoperability issues with the client-server communication in the traditional power grid. The authors explore interoperability issues in smart grids and discuss how they can be addressed from data and communication perspectives.

ABSTRACT

Smart grid has emerged as the next generation of power grids for improved control and efficiency of power production, delivery, and consumption. Unlike the traditional power grid, a smart grid involves significant data communication across the grid. However, in the current practice, different areas of the power domain use different data semantic models, which has caused significant interoperability issues among systems and become a major barrier toward smart grids. Interoperability issues can also arise in communication. There has been growing interest in adopting publish-subscribe communication for improved quality of communication in smart grids. However, adopting publish-subscribe communication requires resolving potential interoperability issues with the client-server communication in the traditional power grid. In this article, we explore interoperability issues in smart grids and discuss how they can be addressed from the data and communication perspectives.

INTRODUCTION

Smart grid has attracted significant attention as the next generation of power grids for efficient energy use. Per the report by The World Bank (http://data.worldbank.org/indicator/EG.ELC.LOSS.ZS; accessed on January 28, 2016), many countries experience significant energy loss in power grids. The U.S loses 6 percent of its total power in the transmission and distribution process, the U.K loses 8 percent, China loses 12 percent, and Iraq loses more than 35 percent. Unlike the traditional power grid, a smart grid is based on data communication among various entities [e.g., intelligent electronic device (IED), supervisory control and data acquisition (SCADA) systems, energy management system (EMS)] across different areas of the grid.

However, in the current practice, different areas of the power domain use different data semantic models. There are two major standards in the power domain: IEC 61850 (http://www.iec.ch/smartgrid/standards/; accessed on February 13, 2016); and IEC 61970 (http://www.iec.ch/smartgrid/standards/; accessed on February 13, 2016). IEC 61850 provides the data model for substation automation [e.g., substation automation system (SAS)] and it has been recently extended to power consumption [e.g., electric vehicle supply equipment (EVSE)]. On the other hand, IEC 61970 defines the data model for power management (e.g., EMS, SCADA) and provides a set of guidelines for application integration and data exchange. However, these standards have been developed and evolving independently from each other by different communities, which has widened their differences in semantics and notations. This has led to significant interoperability issues among systems based on these standards [1]. To address this, there have been collaborative initiatives for developing a common semantic model that has been identified as a high priority by NIST (https://www.nist.gov/sites/default/files/documents/public affairs/releases/smartgrid interoperability final.pdf; accessed on January 17, 2016). The common semantic model allows systems to speak "the same language" and have a consistent understanding of exchanged data. We refer to it as *data-driven interoperability*.

Interoperability issues can also occur in communication. There has been growing interest in adopting publish-subscribe communication in power grids for improved quality of data communication. Some researchers (e.g., [2, 3]) have studied the possible adoption of Message Queueing Telemetry Transport (MQTT — http://mqtt.org; accessed on February 16, 2016) and Data Distribution Service (DDS — http://www.omg.org/spec/DDSI-RTPS/; accessed on February 18, 2016) which are widely used publish-subscribe protocols in the IoT domain. However, the traditional power grid is client-server based. Furthermore, different vendors use different client-server protocols [e.g., Manufacturing Message Specification (MMS) [4], Distributed Network Protocol (DNP — http://www.dnp.org; accessed on 0February 18, 2016) , OLE for Process Control Unified Architecture (OPC UA) — https://opcfoundation.org/about/opc-technologies/opc-ua/; accessed on March 2, 2016], which aggravates the issue. This leads to the need for a communication model that can support both client-server and publish-subscribe communication. We refer to this as *communication-driven interoperability*.

An effective solution for these issues is to develop a novel communication platform that empowers both data-driven interoperability and communication-driven interoperability. We call it *Smart Grid Interoperability Platform (SGIP)*. The development of the SGIP requires the following questions to be addressed.

•What are functional and non-functional requirements for the SGIP? How can they be identified? Smart grids have many domain-specific requirements imposed by various devices, equipment, standards, and domains. The development of the SGIP should be based on a rigorous analysis of these requirements.

•How should the common semantic model be

Digital Object Identifier:
10.1109/MCOM.2017.1600392

Dae-Kyoo Kim, Alaa Alaerjan, and Lunjin Lu are with Oakland University; Hyosik Yang is with Sejong University; Hyuksoo Jang is with Myongji University.

defined? What should be the underlying design principles? Addressing these questions requires a clear understanding of the involved domains in smart grids and data modeling practices in the domains.

•Can existing publish-subscribe protocols be adopted for smart grids? If so, what are the tailoring points? And how should they be tailored? A smart grid involves many quality of service (QoS) requirements that are important for control and protection, and the adopted protocol should be able to support them.

•How should the SGIP be designed? Two major communication paradigms in smart grids are client-server and publish-subscribe. The SGIP should be designed to support both to facilitate the development and communication of applications that participate in both paradigms. A smart grid involves many kinds of applications running on various types of devices with different computing capabilities. The design should address how such variability can be accommodated.

•How should the SGIP be validated? The validation should include not only functional and non-functional requirements, but also data-driven and communication-driven interoperability.

Smart Grid Interoperability Platform

The SGIP is built upon a common semantic model which enables applications to speak the same language and hence guarantees data-driven interoperability. On top of data-driven interoperability, communication-driven interoperability is supported through communication middleware that supports both client-server and publish-subscribe communication. Ultimately, they all together enable data-centric communication in smart grids. Figure 1 shows the infrastructure of the SGIP. The rest of this section describes the SGIP in terms of functional and non-functional requirements, common sematic models, tailoring DDS, SGIP architecture, and validation.

Functional and Non-Functional Requirements

The functional requirements of the SGIP are greatly influenced by the types of communication protocols. The protocols used in the traditional power grid are mostly client-server based with limited data communication due to data inconsistency. However, as power grids evolve to have increasing data communication toward smart grids, more scalable, flexible, and reliable protocols enabling data-centric communication are needed. In the efforts to address this, there has been growing interest in adopting publish-subscribe protocols such as DDS in smart grids. DDS is node-based where each node is capable of publishing and subscribing data. DDS is reliable as it has no broker that can be a single point of failure. DDS provides 22 QoS attributes that can be very effective for protection and control in smart grids. However, DDS might be heavy for some devices that have limited computing capability, which can be addressed by configurable DDS.

Publish-subscribe communication is heterogeneous to client-server communication which is heavily used in the traditional power grid. We propose to support both client-server and publish-subscribe communication, so that the development and communication of the applications that participate in both communications can be more efficient. The following are the functional requirements for the SGIP.

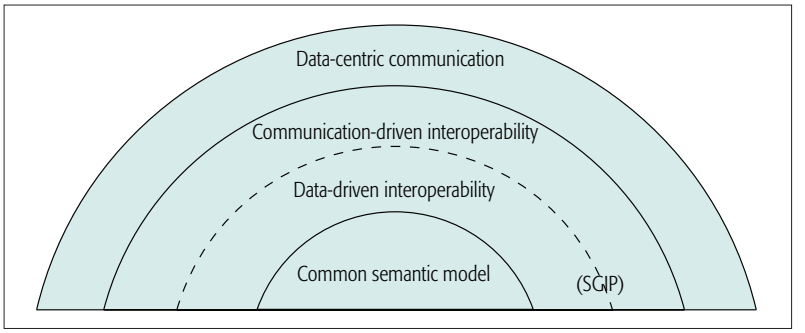


Figure 1. SGIP infrastructure.

•The participants in client-server communication should be able to register and identify services. For the participants in publish-subscribe communication, they should be able to publish and subscribe topics and identify other participants. This also includes connection management (e.g., creating sessions).

•The SGIP should support reconstructing data objects for received data. This involves memory allocation for data per its type and size. In publish-subscribe communication, it can be managed through QoS policies (e.g., frequency of message receiving). An object repository should be also considered for storing and accessing data objects.

•For reliable communication, QoS attributes should be configurable. In client-server communication, this enables a client to query on a server about its reliability level before requesting a service. In publish-subscribe communication, communication can be limited to only the participants who agree on the configured QoS.

•The SGIP should support content-based subscription in publish-subscribe communication. This can be done by filtering out the contents of received data per the criteria (e.g., specific values in topics) set by the subscriber.

Different devices and equipment in smart grids have different computing capabilities, which imposes critical non-functional requirements for QoS. An important QoS is latency. For example, a breaker in a substation is required to transmit its update within 2 seconds after the triggering event has occurred. Another example is a protection relay which is required to detect an event in less than 3 milliseconds to avoid a fault that might lead to blackouts. The IEDs that are responsible for protection and control must transmit data within 12–20 milliseconds. A phasor measurement unit (PMU), which measures the health of the grid, is required to send measured data to the control center at the rate of 6–60 samples per second. The SGIP should be able to support such various latency QoS of different devices in smart grids.

Reliability is another important QoS in smart grids. Consider wireless sensors that monitor equipment for its health. They communicate with each other to detect a fault in the equipment. Harsh environmental conditions such as wind and rain can cripple sensors and hence impair reliability. In power consumption, smart meters and wireless energy monitors communicate with power utilities, e.g., to report power usage and

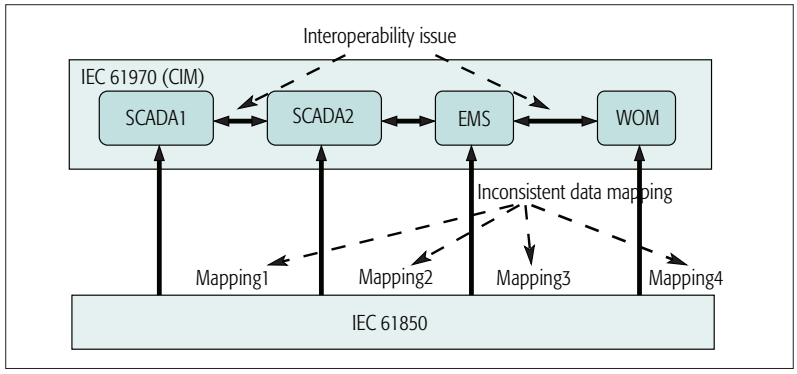


Figure 2. Data mapping inconsistency and interoperability issues [4].

receive pricing information. This requires continuous and accurate updates on a regular basis. The SGIP should be designed to address such reliability requirements. Other quality aspects such as access control [5] also need to be considered.

Common Semantic Model

IEC 61850 and IEC 61970 (which is also known as CIM) are two major standards in the power domain for data modeling. IEC 61850 defines data models for substation automation, while IEC 61970 provides data models for operation management. Systems based on these standards communicate with each other for exchanging data. IEC 61850-based systems (e.g., SAS) send field data to CIM applications (e.g., SCADA, EMS) for CIM applications to make operational decisions. This is called bottom-up data flow.

However, IEC 61850 and IEC 61970 have been developed and evolving independently of each other by different communities. As such, they have different architectures, semantic entities, and notations. Because of that, vendors developing applications based on these standards have to come up with their own mappings between the standards. This has resulted in significant interoperability issues among applications based on the standards. Figure 2 illustrates the problem. In the figure, each CIM application has a different mapping to IEC 61850 and the same CIM entity might be mapped to different IEC 61850 entities. This has been a major hindrance to data-driven interoperability in smart grids. To address the problem, NIST has identified it as a high priority task to define a common semantic model to unify IEC 61850 and IEC 61970.

There have been some efforts (e.g., [6, 7]) toward unifying IEC 61850 and IEC 61970. The general approach in the existing work is that the two standards are analyzed to identify common entities and a correspondence is established between the common entities. Non-common entities are added as extensions. While the approach is intuitive, it lacks underlying principles as to how common entities can be identified and merged and how extensions should be defined. To address that, we have developed a metamodeling method that provides a set of design principles for defining a common semantic model (CSM) of the two standards [1, 8, 9]. The method is based on a three-tier infrastructure that aligns the two standards in terms of metamodel level (M2), model level (M1), and object level (M0). M2 defines the abstract syntax for models at M1 whose elements are instances (classes) of the metaclasses at M2. A model at M1 captures the abstraction of object models at M0 whose elements are instances (objects) of the classes at M1. With that said, the top-down describes instance relationships and the bottom-up specifies metamodel relationships. Given the infrastructure, unification is carried out at M1. Figure 3 depicts the three-tier infrastructure.

Tailoring DDS

DDS is data-centric middleware for data sharing in a wide range of computing environments from small local networks to large scale systems. Based on a point-to-point publish/subscribe protocol with a variety of QoS policies, DDS enables scalable, dependable, and real-time data exchange between different components with minimal overheads. With these advantages, it has emerged as a potential solution for publish-subscribe communication in smart grids. However, adopting DDS for smart grids requires tailoring in several areas: QoS attributes need be tailored to accommodate reliability and time constraints in smart grids, and discovery services need be tailored to support the dynamic configuration of devices and equipment in smart grids.

Tailoring QoS Attributes: DDS provides a set of QoS attributes that can be configured on an entity basis. Communication can be established only if both parties agree on their QoS. QoS is particularly important for smart grids to ensure quality communication because they involve various types of devices and equipment with different computing capabilities. We propose the following tailoring for DDS QoS to be adopted for smart grids.

Latency (Deadline): This attribute specifies time constraints on publishing and receiving data between a publisher and a subscriber. It needs to be tailored by considering listener objects to maintain and keep track of deadline contracts of devices. For example, listener objects are necessary for SAS to ensure that critical data (e.g., transformers' temperature) is received on time from the devices it monitors.

Latency Budget: This attribute specifies the maximum acceptable latency for a subscriber to receive data. The maximum acceptable latency refers to the delay between the time the data is written and the time the data is inserted into the subscriber's cache. It needs to be tailored to define communication rules related to time constraints on devices. One way of tailoring is to use it in conjunction with a priority-based transport protocol and set a higher priority on data with lower latency budget.

Reliability: This attribute is used to ensure reliable data reception on data readers. There are two settings: *reliable* and *best effort*. The *reliable* setting enforces reliable data exchanges by retransmitting data until received. This setting can be tailored for the data receivers (e.g., smart meters) that can tolerate a certain level of latency. On the other hand, the *best effort* setting sends data without a guarantee of delivery. This is useful for sensor communication where a data sample is periodically published without guaranteeing delivery. Therefore, this setting can be used for the devices that can be vulnerable to natural environmental factors (e.g., wind, storms). Nevertheless, tailoring is necessary for the *best effort* setting for

reliable communication. One way of tailoring is to use acknowledgment mechanisms equipped with buffers.

Tailoring Discovery Mechanism: DDS provides the Real-Time Publish Subscribe (RTPS) protocol for discovering entities, which supports dynamic configuration of devices and equipment in smart grids. RTPS includes two discovery protocols: Participant Discovery Protocol (PDP) and Endpoint Discovery Protocol (EDP). PDP allows discovering the participants in the same domain using multicasting, while EDP enables identifying communication endpoints (i.e., DataReader, DataWriter). These protocols involve a large amount of data exchanges, which takes a significant amount of computing power for participating entities. However, many devices (e.g., sensors, IEDs) in smart grids have limited computing capability which limits the application of RTPS. To address this, we propose the following tailoring:

Multiple Discovery Strategies: While the discovery mechanisms of DDS require participating entities to have sufficient computing power for handling data exchanges, DDS does not place any restriction on how the discovery mechanisms should be implemented. That is, devices with limited computing power may use an alternative lightweight discovery mechanism within the DDS infrastructure. For instance, Simple Service Discovery Protocol (SSDP) can be used for IEDs and sensors which in general have low computing capability. For those devices that communicate with fixed servers, a static discovery mechanism can be used. That being said, RTPS should be implemented in various ways to support multiple discovery mechanisms.

Communication Guides: The dynamic nature of communication in smart grids requires communication guides as part of discovery mechanisms. The guides help subscribers identify the IP addresses and port numbers of publishers. The group membership provided by DDS is an example of communication guides. Using the group membership, a device playing the publisher role can be efficiently identified by the identifier (e.g., IP addresses) of the group to which the device belongs.

SGIP Architecture

The goal of the SGIP is to support data-driven and communication-driven interoperability for smart grid systems. Based on the requirements identified previously and the common semantic model defined, we propose the SGIP architecture as shown in Fig. 4. The architecture is composed of two layers: *data management* and *communication logic*. The data management layer is concerned with managing data sending and receiving. It consists of the *API*, *resource management*, and *object reconstruction* modules. The *API* module provides SGIP services to applications, including data sending and receiving, resource management, QoS configuration, and discovery mechanisms. The *resource management* module is responsible for allocating memory for data management. Different strategies can be used for memory allocation per the computing capability of devices. The *object reconstruction* module is concerned with reconstructing data objects for received data and making them available to applications. The original data objects are reconstructed from the serialized messages and stored in a global data repository. When needed, they are loaded into local memory and made available to applications for use. The reconstruction process is facilitated by the common semantic model above as both the original objects and the reconstructed objects are instances of the same semantic entities in the common semantic model, which empowers data-driven interoperability. *Object reconstruction* is also responsible for mapping data objects to topics in publish-subscribe communication.

The *communication logic* layer is composed of the *client-server communication*, *publish-subscribe communication*, *discovery mechanism*, and *communication establishment* modules. The *client-server communication* module supports message sending and receiving in client-server communication, while the *publish-subscribe communication* module manages topic publishing and subscribing in publish-subscribe communication. Supporting the two different communication paradigms in the same platform facilitates the development and communication of the applications running on the devices that participate in both communications. For example, SCADA interacts with various types of devices and other systems where it plays both the client role and the subscriber role and using the same platform, the development and communication of applications in respective roles becomes more integrative and efficient. A key function in this layer is the *discovery mechanism* module. In client-server communication, it allows servers to register their services and clients to search for available services. In publish-subscribe communication, it is used for publishers to identify subscribers and publish a topic. For subscribers, it allows them to register topics of their interests.

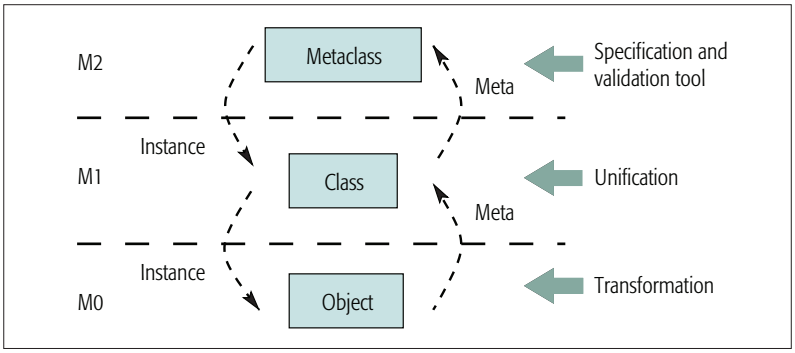


Figure 3. Three-tier infrastructure [4].

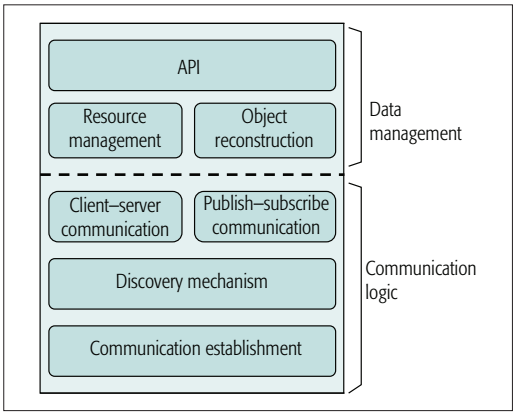


Figure 4. SGIP architecture.

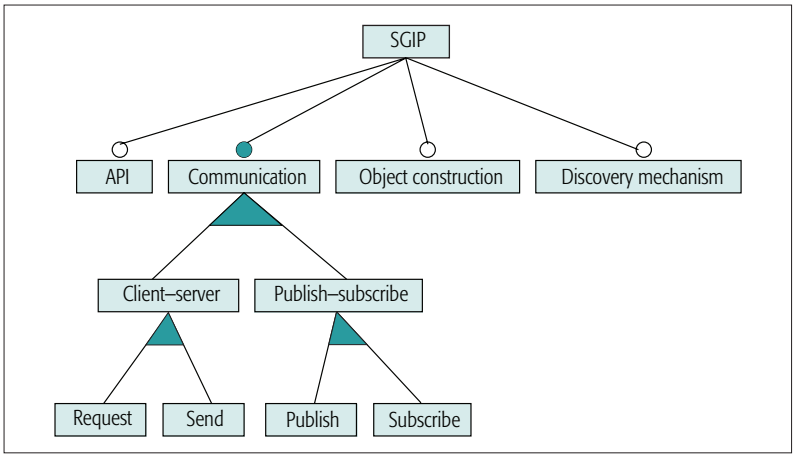


Figure 5. Feature model of SGIP.

If a publisher and a subscriber share a topic, *discovery mechanism* evaluates whether they satisfy the QoS of each other. An agreement for data exchange is established only if both satisfy each other's QoS. *Discovery mechanism* also supports *object reconstruction* for mapping topics to data objects. The *communication establishment* module establishes a communication instance including session creation, socket connection, channel establishment, and synchronization.

The SGIP is designed to be configurable to support various types of devices and equipment with different computing capability and resource capacity. Based on the SGIP architecture, Fig. 5 shows a feature model for the SGIP. In the model, filled circles denote required features, open circles represent optional features, and the filled triangle underneath *communication* specifies inclusive-or. Given the model, the SGIP can be configured on a device basis. For example, a simple sensor playing the publisher role can be configured to have only the *publish* feature; an IED with limited computing capability playing the server role can be configured to have the API and *send* features; and an EMS running on highly capable computing equipment can be configured to have the full features.

The *discovery mechanism* feature can be implemented using an API that provides naming and directory services (e.g., JDNI — http://docs.oracle.com/javase/7/docs/technotes/guides/jndi; accessed on February 12, 2016) based on a network architecture for distributed systems (e.g., JINI — https://river.apache.org/release-doc/2.2.2/specs/html/jini-spec.html; accessed on March 5, 2017). Through the API, the network architecture would provide look-up services for discovering objects and other fundamental network services such as security and transaction management. For the *client-server communication* feature, a framework for asynchronous event-driven network applications (e.g., Netty — http://netty.io; accessed on February 12, 2016) can be adopted. This requires the development of interfaces to the *publish-subscribe communication* feature for seamless integration with client-server communication. With respect to the *publish-subscribe communication* feature, an implementation of MQTT (e.g., HiveMQ — http://www.hivemq.com; accessed on March 14, 2016) or DDS (OpenDDS — http://opendds.org; accessed on 03/16/2016) can be used as a base.

Validation Requirements

The validation of the SGIP can be carried out in terms of functional requirements, non-functional requirements, data-driven interoperability, and communication-driven interoperability.

Validating Functional Requirements: Functional requirements can be validated by conducting a series of test cases based on use cases. The use case repository provided by Electric Power Research Institute (EPRI — http://smartgrid.epri.com/Repository/Repository.aspx; accessed on February 17, 2016) for smart grids is a great resource for test case development. Use cases can be structured, to facilitate incremental testing (e.g., from sub-use cases to main use cases). Use cases can also be prioritized based on criticality. For example, control and protection related use cases should be given a higher priority, while maintenance related use cases can be given a lower priority.

Validating Non-Functional Requirements: Non-functional requirements can be validated through QoS testing. Many QoS policies in smart grids are concerned with time, which requires time synchronization. For example, per IEC 61850, control data sent from a SCADA system to an IED must be received within 20-30 millisecond, which is a latency QoS policy in publish-subscribe communication. Another example is the stability of a server for a client to determine if the server is stable enough to carry out a service request, which is a reliability QoS policy in client-server communication. If a controlled environment is used, potential overheads that would occur in a real environment should be also considered.

Validating Data-Driven Interoperability: Data-driven interoperability can be validated through communication between different domains in smart grids. Three cases can be considered: (a) between the substation domain and the management domain; (b) between the management domain and the distribution domain; and (c) between the distribution domain and the substation domain. Examples are the SAS and SCADA/EMS communication for (a), the EMS and DMS communication for (b), and the DMS and SAS communication for (c).

Validating Communication-Driven Interoperability: Communication-driven interoperability can be validated using various types of devices with different levels of computing capability. The SGIP can be configured for individual devices per their resources and performance and the role (e.g., publisher, server) they play in communication. For example, for a simple device such as sensors in publish-subscribe communication, the SGIP can be configured to have only the publishing feature. On the other hand, for a larger device such as protection IEDs which can participate in both publish-subscribe and client-server communication, it can be configured to have both sending and publishing features.

Case Studies

We applied the metamodeling method to develop a common semantic model of IEC 61850 and IEC 61970. Figure 6 shows the common seman-

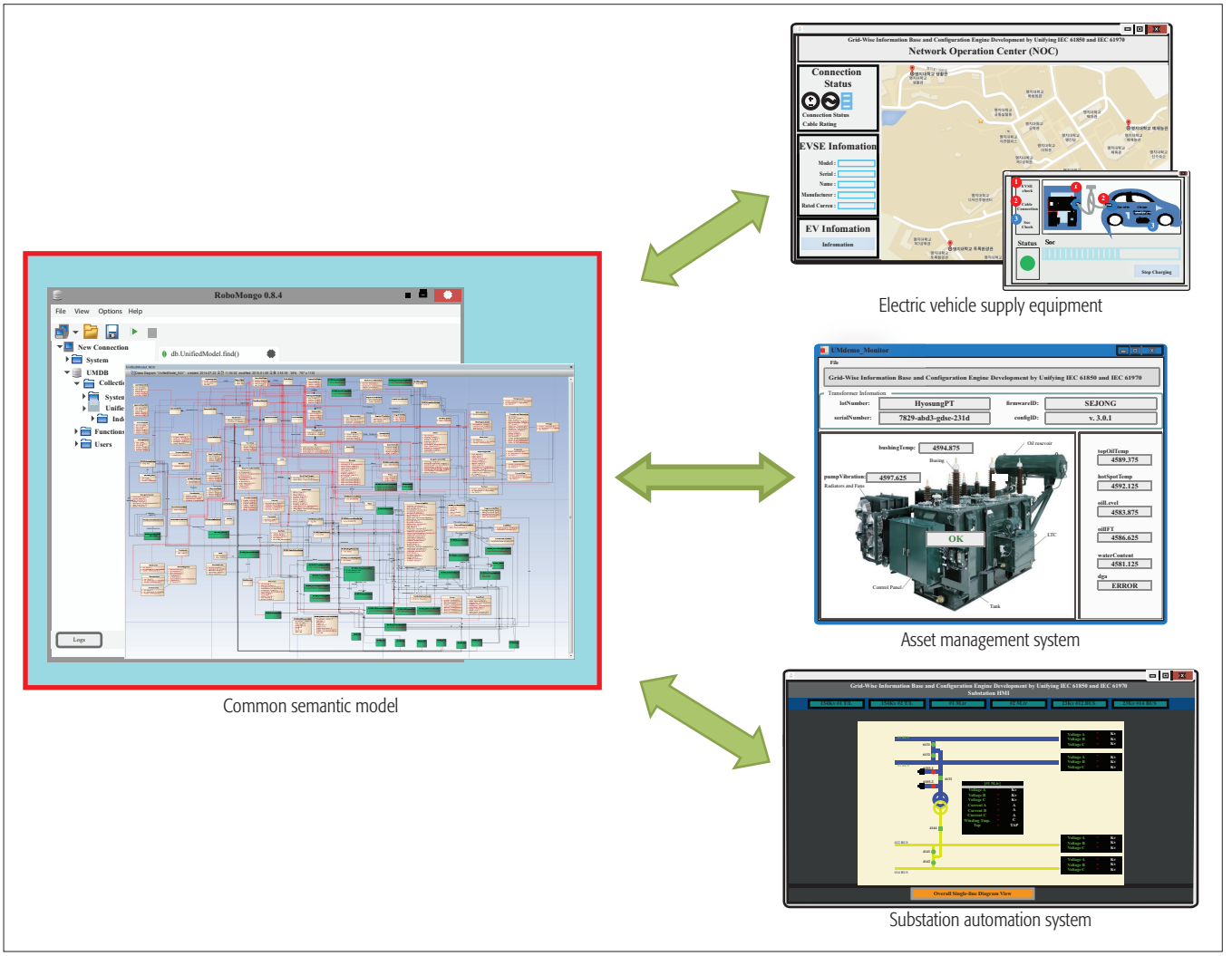


Figure 6. Application development using the common semantic model.

tic model defining 128 classes covering the substation, distribution, and consumption domains of smart girds. The model is represented in Enterprise Architect (http://www.sparxsystems.com; accessed on January 23, 2016) and implemented using MongoDB (https://www.mongodb.com; accessed on February 19, 2016), a NoSQL database. Based on the model, three prototype applications of EVSE, asset management systems (AMS), and SAS are developed to evaluate the adoptability of the model and data-driven interoperability.

EVSE is a power supply unit for recharging electric vehicles. The developed application reads in the charging status of an electric vehicle (EV) and stores the data in the database for other systems (e.g., DMS, EMS) to use. We also simulated sending data to the control system which is also based on the common semantic model. The development was based on a profile built upon the common semantic model for the E-mobility aspect in IEC 61850-90-8.

AMS is concerned with inventory control and property management, providing comprehensive information (e.g., ownership, venues, connectivity, status) on assets. The developed prototype focuses on monitoring the status of a small set of assets and storing the data in the database. The stored data is then accessed by EMS for checking the status of critical devices (e.g., power transformers). The prototype was developed based on a profile for the asset aspects in IEC 61968 which is an extension of IEC 61970.

SAS is responsible for monitoring and controlling the devices and equipment in a substation and collecting their data. The developed prototype is a human machine interface (HMI) system for displaying the status of substation devices and equipment. The application was developed based on a profile that covers the substation aspects in IEC 61850.

The EVSE and SAS applications are developed in Java, while the AMS application is developed in C#. We also developed a profiling tool as an Eclipse plug-in. In the studies, we witnessed seamless data sharing among the three applications through the database which is eminent evidence of data-driven interoperability supported by the common semantic model.

Case studies for communication-driven interoperability require the SGIP architecture to be implemented. A major challenge in implementation is the configurability of the SGIP which is a key to support various types of devices with different computing capabilities. A prerequisite to configurability is to identify features to be configured and their dependencies per the role

We have proposed the SGIP to address interoperability needs for smart grids in terms of data-driven interoperability and communication-driven interoperability. Data-driven interoperability is supported by the common semantic model and communication-driven interoperability is realized by the communication architecture of the SGIP.

(e.g., publisher, subscriber) of devices and their computing capability. From an architectural perspective, features are realized by different sets of SGIP modules (see Fig. 4). For the features that are composed of heterogeneous modules (e.g., server modules, publish modules), the interactions of the composing modules should be analyzed, which is important for the applications that participate in both client-server and publish-subscribe communication. Some domains (e.g., substations) in smart grids have domain-specific protocols (e.g., Generic Object-Oriented Substation Events [GOOSE]) that might require protocol layers to be configured (e.g., Ethernet-based publish-subscribe communication). We refer to it as heavyweight configuration. Further study on the extent to which the SGIP can support heavyweight configuration needs to be carried out.

Conclusion

A smart grid is comprised of various types of devices, equipment, and systems with different computing capability and requirements. A successful realization of a smart grid requires seamless interoperability among involved components. In this article, we have proposed the SGIP to address interoperability needs for smart grids in terms of data-driven interoperability and communication-driven interoperability. Data-driven interoperability is supported by the common semantic model and communication-driven interoperability is realized by the communication architecture of the SGIP. We have also presented case studies to demonstrate the use of the common semantic model and its support for data-driven interoperability. We are currently implementing the proposed SGIP architecture and the simulation environment for validating communication-driven interoperability.

References

[1] D. Kim *et al.*, "QVT-Based Model Transformation to Support Unification of IEC 61850 and IEC 61970, *IEEE Trans. Power Delivery*, vol. 29, no. 2, Apr. 2014, pp. 598–606.

[2] A. Alaerjan and D. Kim, "Tailoring DDS to Smart Grids for Improved Communication and Control," *Proc. 5th Int'l. Conf. Smart Cities and Green ICT Systems*, Rome, Italy, 2016, pp. 127–36.

[3] A. Alkhawaja, L. Ferreira, and M. Albano, "Message Oriented Middleware with QoS Support for Smart Grids," *Proc. Conf. Embedded Systems and Real Time*, Caparica, Portugal, 2012, pp. 1–13.

[4] P. Pleinevaux, "An analysis of the MMS Object Model," *IEEE Trans. Industrial Electronics*, vol. 41, no. 3, Jun. 1994, pp. 265–68.

[5] B. Lee *et al.*, "Role-Based Access Control for Substation Automation System Using XACML," *Information Systems*, vol. 53, Nov. 2015, pp. 237–49.

[6] Y. Pradeep *et al.*, "CIM and IEC 61850 Integration Issues: Application to Power Systems," *Proc. IEEE Power Energy Society General Meeting*, 2009, pp. 1–6.

[7] R. Santodomingo, J. A. Rodriguez-Mondejar, and M. A. Sanz-Bobi, "Ontology Matching Approach to the Harmonization of CIM and IEC 61850 Standards," *Proc. IEEE Int'l. Conf. Smart Grid Commun.*, 2010, pp. 55–60.

[8] D. Kim *et al.*, "A Metamodeling Approach to Unifying IEC 61850 and IEC 61970," *Proc. 4th IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Washington, D.C., 2013, pp. 1–6.

[9] B. Lee *et al.*, "Unifying Data Types of IEC 61850 and CIM," *IEEE Trans. Power Systems*, vol. 30, no. 1, Jan. 2014, pp. 448–56.

Biographies

Dae-Kyoo Kim [SM] (kim2@oakland.edu) is an associate professor in the Department of Computer Science and Engineering at Oakland University. He received a Ph.D. in computer science from Colorado State University in 2004, an M.S. in computer science from Western Michigan University in 1997, and a B.S. in information and communication engineering from Myongji University, Korea in 1995. During his Ph.D. he worked as a technical specialist at the NASA Ames Research Center.

Alaa Alaerjan (asalaerjan@oakland.edu) is a Ph.D. student in the Department of Computer Science and Engineering at Oakland University. He received B.S. and M.S. degrees in computer science from Al-Jouf University (Saudi Arabia), and from Ball State University in 2009 and 2013, respectively. Before joining OU he worked as a lecturer in the Department of Computer Science at Al-Jouf University. His research interests include distributed systems and smart grids.

Lunjin Lu (l2lu@oakland.edu) is an associate professor in the Computer Science and Engineering Department at Oakland University. His broad research areas are programming languages and software engineering. His research interests include semantic-based program analysis, program semantics, logic programming, UML modeling, software design patterns, software refinement, UML model refinement, and pattern conformance.

Hyosik Yang (hsyang@sejong.ac.kr) is an associate professor in the department of Computer Science and Engineering at Sejong University, Seoul, Korea. He received his B.E. degree from the Department of Information and Communication Engineering, Myongji University, Yongin, Korea, in 1998, and his M.S. and Ph.D. degrees in electrical engineering from Arizona State University in 2000 and 2005, respectively. His research interests include WDM all optical networks, mobile ad-hoc networks, and smart grid.

Hyuksoo Jang (hyuks.jang@gmail.com) is a professor in the Department of Computer Science and Engineering, Myong-Ji University, Korea. He received a B.S. degree from Seoul National University, Korea in 1983, and the Ph.D. degree in computer and information science from Ohio State University, Columbus, Ohio, USA in 1990. He has been engaged in numerous research and standardization projects on ICT based electric power grid, IEC 61850, electric vehicle, and smart grid.

ACCEPTED FROM OPEN CALL

NFV: Security Threats and Best Practices

Shankar Lal, Tarik Taleb, and Ashutosh Dutta

ABSTRACT

Network function virtualization (NFV) yields numerous benefits, particularly the possibility of a cost-efficient transition of telco hardware functionalities on the software platform to break the vendor lock-in problem. These benefits come at the price of some security flaws. Indeed, with NFV, virtual mobile networks become vulnerable to a number of security threats. These threats can be leveraged using some available mitigation techniques and also through other emerging solutions. This article presents critical security threats that exist in the NFV infrastructure, proposes best security practices to protect against them.

INTRODUCTION

The telecommunication infrastructure is experiencing great structural changes in the way it used to be deployed, thanks to emerging technologies such as network functions virtualization (NFV). NFV is a great development in the process of network evolution which uses modern virtualization platforms and commercial of-the-shelf (COTS) hardware to deploy network functions for mobile networks. It has undoubtedly a significant impact on network operations. An important contribution of NFV is to turn network functions, which traditionally rely on hardware appliances, into software modules such as network firewalls and gateway routers/switches.

Traditional network functions are coupled with underlying dedicated hardware, which are, in turn, vendor proprietary. When it comes to scaling the network, the deployment of new network functions and services becomes increasingly cumbersome and expensive. It is also difficult to provision them when there are dynamic network traffic and constantly changing requirements. NFV defines a promising approach to overcome these problems, enabling easy and fast network function deployment [1, 2]. In comparison with traditional network infrastructures, NFV delivers the following promises among others:

- Lowering the cost of ownership by moving network functions from dedicated boxes into virtual resources (i.e., virtual machines, VMs or containers).
- Enabling fast and cost-efficient deployment of network functions for better service agility.
- Supporting agile and flexible deployment of network functions along with their lifecycle management.
- Reducing energy consumption.

Contrary to common belief, NFV does not depend on software defined networking (SDN) and can be implemented stand-alone. SDN and NFV are complementary to each other and bring significant advantages when used together. NFV can bring the benefits of virtualizing SDN controllers and thus allowing dynamic mobility of SDN controllers to desired locations. SDN can bring value to NFV allowing dynamic network connectivity by programming the network to be optimal based on network traffic monitoring and analysis [1]. Some practical examples of VNF are vRouters, vFirewalls, virtual content delivery servers, vIPS/vIDS, vDNS servers, and virtual VPN servers.

In this article, we review the security challenges that pose threats to NFVI. We explain the ways by which these security attacks can be carried out on NFVI. Based on the severity of these security attacks, we propose some best security practices to cope with these attacks. The rest of this article is organized as follows. We list the gains and pains of adopting NFV. This section also explains the security implications of adopting NFVI and also the opportunities arising to build a secure and vibrant NFVI-based ecosystem. We present some related work and ongoing research projects. We briefly discuss the ETSI NFV architecture. We discuss the main security risks associated with NFVI and highlight the most popular security attacks that can be executed on NFVI. We propose best security practices that should be followed to protect against these attacks. We further discuss the open security challenges. Finally, the article concludes.

GAINS AND PAINS OF NFVI

NFV provides the means to install new network functions on demand without needing any installation of new hardware equipment. For example, a mobile operator can run any software-based network function in a specific format of virtual resources (e.g., VMs or containers) at any time. This certainly enables agile networking and cost-effective deployment of network functions. By enabling these features, NFV promises a decrease in time to market for network functions through software-based services and facilitating custom deployment of services based on customer's requirements.

Security in NFV raises important concerns about its adaptability in the underlying telecommunication infrastructure. It largely impacts the system resiliency [16] as well as the overall quality of the offered services [17]. Some of these security concerns apply to the key architectural components of NFV infrastructure such as virtual infrastructure manager (VIM). Hypervisor is the main element of VIM and is already under various

Network function virtualization (NFV) yields numerous benefits, particularly the possibility of cost-efficient transition of telco hardware functionalities on the software platform to break the vendor lock-in problem. These benefits come at the price of some security flaws. Indeed, with NFV, virtual mobile networks become vulnerable to a number of security threats.

Shankar Lal is with Nokia Bell Labs/Aalto University; Tarik Taleb is with Sejong University/Aalto University; Ashutosh Dutta is with AT&T.

Digital Object Identifier:
10.1109/MCOM.2017.1600899

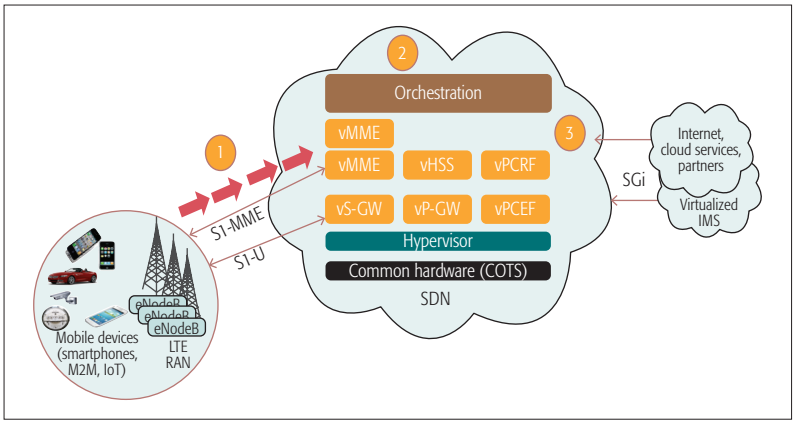


Figure 1. NFVI- DDoS resiliency.

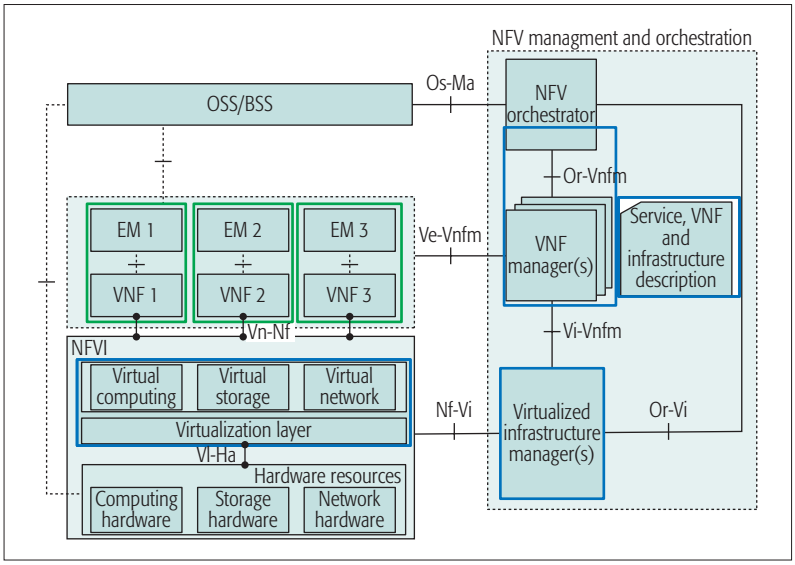


Figure 2. The ETSI NFVI reference architecture.

security attacks such as VM/guest OS manipulation and data exfiltration/destruction. Therefore, when the hypervisor is compromised, other vulnerabilities can arise exponentially. Since NFV delivers software enabled automated provisioning of network functions, it can also open security vulnerabilities such as automated network configuration exploits, orchestration exploits, malicious misconfiguration, and SDN controller exploits. Due to the elastic and flexible nature of NFVI elements, some security attacks can also become amplified. One type of such an attack is called a DNS amplification attack, which is discussed in a later section. In addition, VNFs are likely to be provided by many different vendors, which can possibly result in interoperability issues causing security loopholes in the infrastructure [3].

In addition to these security risks, the flexible and scalable nature of NFV helps to improve the incident response time, provides better resiliency against distributed denial of service (DDoS) attacks and enables on-demand firewalling and intrusion detection/prevention systems (IDS/IPS) to block or reroute malicious traffic. Figure 1 depicts an example of an attack on NFVI. In the envisioned scenario, the mobility management entity (MME) is virtualized and the orchestrator is capable of instantiating new vMME instances on demand. In this scenario, an attacker could create a botnet army by infecting many mobile devices with a "remote-reboot" malware, enabling the attacker to instruct the malware to reboot all devices at the same time (step 1 in Fig. 1). The simultaneous rebooting of all devices causes excessive "malicious" attach requests and results in a signaling storm (step 2 in Fig. 1), putting vMME under DDoS attack. In response to the attack, the orchestrator may instantiate a new VM to scale-out the vMME function to sustain the surge in the signaling traffic and to ensure service availability while the attack is being investigated (step 3 in Fig. 1).

Related Work and Ongoing Projects

Security concerns have been raised in [4] where the authors identified security challenges in managing security of virtual appliances in cloud service provider's infrastructure along with the introduction of additional entities such as orchestrators which can be vulnerable to security threats. The authors in [5] presented two security risks that need to be taken care of during NFV design. The first is the isolation and protection of two network functions from different subscribers. The second is the security and resiliency of physical and virtual resources of NFVI. In [6], the authors provided a security framework for virtualized networks based on the use of a root trusted module.

There are a number of ongoing research projects in the NFV security domain aiming to provide security and resiliency of the NFV infrastructure. The European H2020 Arcadia project[1] has the objectives of detecting, exploring, and understanding security events in NFVI by service chain performance analytics to detect anomalistic behavior of the network functions. The 5G Ensure project[2] envisions securing future 5G networks that will rely on NFVI. It aims at developing security enablers consisting of privacy, trust, and virtualization isolation functions for 5G networks. OPNFV, an open source project from the Linux Foundation[3], has a dedicated security group working on vulnerability management to develop network security functions for NFV.

Brief Overview of NFV Infrastructure

NFVI provides the infrastructure that consists of all the hardware and software resources that are required to deploy VNFs. Figure 2 shows the NFVI reference architecture as defined by the European telecommunications standards institute (ETSI). The hardware resources consist of compute, storage, and network elements that basically provide the processing, storage, and connectivity capabilities to VNFs through a virtualization layer. The virtualization layer provides an abstraction to the hardware resources and enables the software to use the virtualized infrastructure instead. Examples of the virtualization layer are the hypervisor and container based virtualization solutions such as Docker. Beyond the NFVI, the NFVI architectural framework also includes the following functional building blocks [7].

Virtual Network Functions: VNFs are software packages that can implement the network functions using the infrastructure provided by NFVI. Virtualizing the network functions reduces hardware usage, improves the scalability, and reduces

[1] http://www.arcadia-framework.eu

[2] http://www.5gensure.eu

[3] https://wiki.opnfv.org/display/security/Security+Home

implementation costs. This enables easy upgrades, reduced power consumption, and equally reduced maintenance.

NFV Orchestrator: Responsible for onboarding the new network services and their lifecycle (e.g., instantiation, scaling in and out, performance measurement, and termination). The NFV orchestrator also performs global resource management and authorization to resource requests in the NFV.

VNF Manager(s): In charge of lifecycle management of VNFs from instantiating, updating, scaling, and terminating, and also performing other functions that are necessary for the entire VNF lifecycle. It also performs coordination and event reporting to other NFVI components.

Virtual Infrastructure Manager(s) (VIM): The VIM functionality includes controlling and managing the interaction of VNFs with NFVI. Basically, it performs resource management, which involves management and allocation of NFVI resources such as compute, storage, and network resources to VNFs. It also analyzes the performance of NFVI and logs if there is any fault information. Other functions of VIM involve collecting and forwarding performance and measurement events.

Additionally, there exists a VNF descriptor (VNFD) in the NFV management and orchestration stack, which is a VNF deployment template and contains descriptions regarding VNF operational and deployment requirements.

Security Risks Associated with NFV

VNFs run over virtual resources such as VMs. The security threats associated with VNFs are the combination of the security threats on physical networking and on virtualization technologies where NFV specific threats emerge when the two sets of threats intersect each other [8]. In the following, we discuss the potential security risks associated with NFVI, considering some potential attack scenarios.

Isolation Failure Risk

Here, we consider the case when an attacker manages to break into a hypervisor by compromising some VNFs running over it. This attack can impose great risk once successfully carried out. This is called a VM escape attack and is depicted in Fig. 3. In this attack scenerio, the attacker first compromises one VNF by gaining access to its operating system (step 1 in Fig. 3). Using tools and VNF network connectivity with the cloud management network, the attacker gains access to the hypervisor management API (step 2 in Fig. 3) and then the attacker breaks into the hypervisor to cause great impact (step 3 in Fig. 3). These attacks are possible due to the improper isolation between hypervisors and VNFs. A practical example of this attack could be launched by an application, running in a VNF and sending crafted network packets in order to exploit heap overflow with a compromised virtualization process and resulting in the execution of arbitrary code on the hypervisor to gain access to the host.

In another attack scenario, a VNF may orchestrate other VNFs, which can be achieved by granting the VNF API access to the virtualization infrastructure to instantiate new VNFs. The API can be misused by an attacker who can break in by compromising the VNF and gaining full access to all infrastructure resources [9].

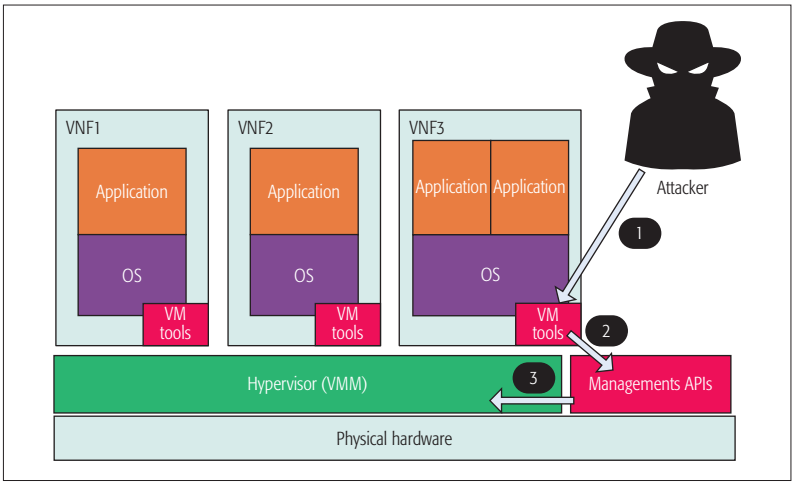


Figure 3. A VM escape attack scenario.

Network Topology Validation and Implementation Failure

Using NFV, virtual networking components (e.g., virtual routers and virtual networks) can be easily created. Quick and dynamic service decisions can result in human error when a virtual router is created and used to interconnect virtual networks without the use of any firewall. Compared to physical network appliance deployments, the dynamicity of virtual network appliances and its connectivity can lead to improper separation between the network and its subnets. Using the above mentioned VM escape attack, an attacker can compromise virtual firewalls to restrict firewall functionality while allowing enough access to carry out the attack. In a similar attack scenario, an attacker may acquire knowledge about a multi-site network infrastructure using the elastic nature of NFVI. Effectively, an attacker can trigger the VNF instantiation or migration in another NFVI point of presence with lower security protection (i.e., without any IDS/IPS/deep packet inspection (DPI) capabilities) [9].

Regulatory Compliance Failure

Attacks aiming to place and migrate workload outside the legal boundaries were not possible using traditional infrastructure. Using NFV, violation of regulatory policies and laws becomes possible by moving one VNF from a legal location to another illegal location, as depicted in Fig. 4. The consequences of violating regulatory policies can be in the form of a complete banning of service and/or exerting a financial penalty, which may be the original intention of the attacker to harm the service provider. One possible attack scenario can be when an attacker exploits the insecure VNF API to dump the records of personal data from the database to violate user privacy.

Denial of Service Protection Failure

DoS attacks may be directed to virtual networks or VNFs' public interfaces to exhaust network resources and impact service availability. A huge volume of traffic from a compromised VNF can be generated and sent to other VNFs that would be running on the same hypervisor or even on different hypervisors. Similarly, some VNF applications can consume high CPU, hard disk, and

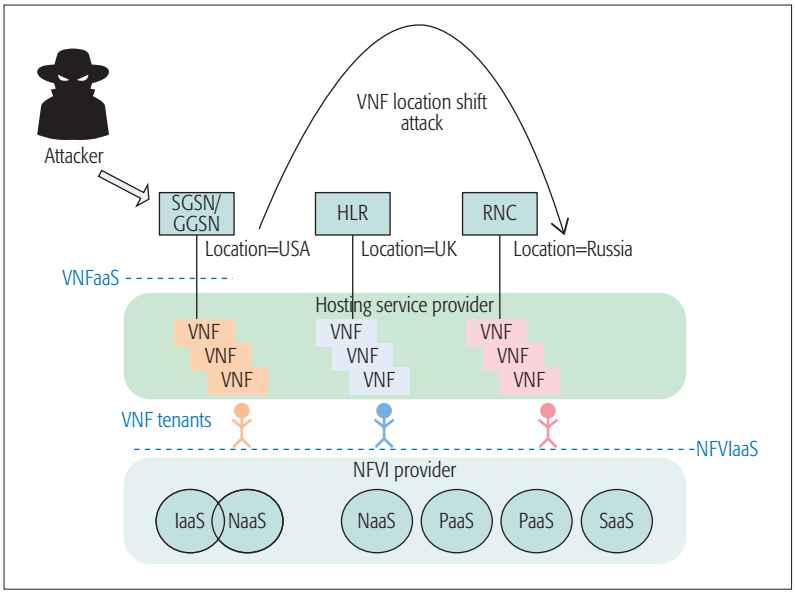


Figure 4. VNF location shift attack.

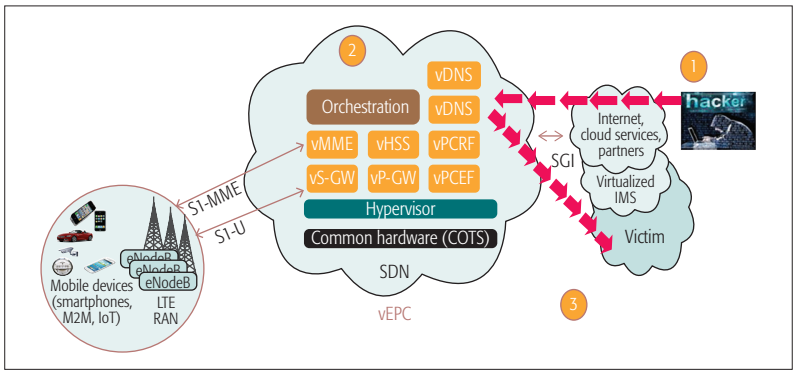


Figure 5. DNS amplification attack.

memory resources in order to exhaust the hypervisor [9]. In this vein, Fig. 5 depicts one practical scenario of DNS amplification attack. In this scenario, a NFVI infrastructure hosts a virtual DNS server as a component of a virtual evolved packet core (vEPC). The NFVI orchestrator is able to deploy additional virtual DNS servers if the traffic load increases. An attacker may spoof IP addresses of a number of victims and launches a high number of malicious DNS queries using the spoofed IP addresses (step 1 in Fig. 5). In response to such an attack, the orchestrator will instantiate new VMs to scale-out the vDNS function to accommodate more queries (step 2 in Fig. 5). Accordingly, multiple recursive DNS servers will respond to the victims that will ultimately receive amplified DNS query responses (step 3 in Fig. 5), which can result in its service disruption or unavailability.

Security Logs Troubleshooting Failure

In this security attack, compromised VNFs can generate a huge amount of logs on the hypervisor, making it difficult to analyze logs from other VNFs, especially when the initial entries in the log files are deleted. There is also risk when the infrastructure logs are leaked, which consequently enables cross relating of logs from one VNF operator with another to extract sensitive information [10].

Malicious Insider

These risks are classified as internal security risks and are caused by vicious actions of internal administrators. In one attack scenario, a malicious administrator takes the memory dump of a user's VM. Since the malicious administrator has the root access to the hypervisor and by using a search operation, they can extract the user ID, passwords, and SSH keys from the memory dump, which in turn violates user privacy and data confidentiality. In a second attack scenario, an internal attacker may extract a user's data from the hard-drive volume, managed by the cloud storage devices. To execute this attack, the attacker first creates a backup copy of the VM drive and then uses open source tools, such as kpartx and vgscan, to extract sensitive data from it [11].

NFV Best Security Practices

In this section, we shed light on best security practices that should be followed in order to achieve reasonably better security protection against the above mentioned threats in a NFV environment. It should be noted that these practices do not guarantee foolproof security of NFVI, but will provide better resiliency against these threats.

Boot Integrity Measurement Leveraging TPM

Using trusted platform module (TPM) as a hardware root of trust, the measurement of system sensitive components such as platform firmware, BIOS, bootloader, OS kernel, and other system components can be securely stored and verified. The platform measurement can only be taken when the system is reset or rebooted; there is no way to write the new platform measurement in TPM during the system run-time. The validation of the platform measurements can be performed by TPM's launch control policy (LCP) or through the remote attestation server [12]

Hypervisor And Virtual Network Security

The hypervisor enables virtualization between underlying hardware and VMs. Virtual networks in the cloud use SDN to enable connectivity among VMs and also with outside networks. Security of these elements is a must in order to protect the whole infrastructure [15]. One of the security best practices is to keep the hypervisor up-to-date by regularly applying the released security patches. Failure to do that would result in exposure to security risks in the future. Another best practice is to disable all services that are not in use. For example, SSH and remote access service may not be needed all the time; therefore, it would be a good idea to enable these services only when needed [13]. Cloud administrators are the gatekeepers of the whole infrastructure and their accounts are the keys. It should be mandated to secure admin accounts by applying a strong password policy along with strictly following an organization's security guidelines.

Security Zoning

To prevent a VM from impacting other VMs or hosts, it is a good practice to separate VM traffic and management traffic. This will prevent attacks by VMs tearing into the management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs

that are not in use. Likewise, VMs of similar functionalities can be grouped into specific zones and their traffic should be isolated. Each zone can be protected using access control policies and a dedicated firewall based on its needed security level. One example of such zones is a demilitarized zone (DMZ) [13, 15].

Linux Kernel Security

In virtualized platforms, the kernel of the host systems is a highly important component that provides isolation between the applications. The SELinux module, developed by the National Security Agency (NSA), is implemented in Kernel and provides robust isolation between the tenants when virtualization technology is used over the host. Secure virtualization (sVirt) is a new form of SELinux, developed to integrate mandatory access control security with Linux based hypervisors. sVirt provides isolation between VM processes and data files. Beyond these tools, other kernel hardening tools can be useful to secure the Linux kernel. A notable example is hidepd, which can be used to prevent unauthorized users from seeing other users' process information. Another example is GRSecurity, which provides protection against attacks on corrupted memory [10].

Hypervisor Introspection

Hypervisor introspection can be used to scrutinize software running inside VMs to find abnormal activities. It acts as a host-based IDS that has access to the states of all VMs, so that the root kit and boot kit inside VMs cannot hide easily. Using introspection capabilities, the hypervisor's functionalities are enhanced, enabling it, among other things, to monitor network traffic, access files in storage, and read memory execution. Hypervisor introspection APIs are powerful tools to perform deep VM analysis and potentially increase VM security. However, they can also be used as an exploit that makes it possible to break and bypass the isolation between VMs and the hypervisor. LibVMI is the library for hypervisor introspection for various platforms, implemented in C language with Python bindings. It gives the hypervisor the means to perform deep inspection of VMs (e.g., memory checking, vCPU register inspection, and recording trapping events) [14].

Encrypting VNF Volume/Swap Areas

Virtual volume disks associated with VNFs may contain sensitive data. Therefore, they need to be protected. The best practice to secure the VNF volume is by encrypting them and storing the cryptographic keys at safe locations. The TPM module can also be used to securely store these keys. In addition, the hypervisor should be configured to securely wipe out the virtual volume disks in the event a VNF is crashed or intentionally destroyed to prevent it from unauthorized access [6]. VM swapping is a memory management technique used to move memory segments from the main memory to disk, which is used as a secondary memory in order to increase system performance in case the system runs out of memory. These transferred memory segments can contain sensitive information such as passwords and certificates. They can be stored on the disk and remain persistent even after system reboot. This enables an attack scenario whereby a VM swap is copied and investigated to retrieve any useful information. One way to avoid this kind of attack is to encrypt VM swap areas. Linux based tools such as dm-crypt can be used for this purpose [10].

VNF Image Signing

It is easy to tamper with VNF images. It requires only a few seconds to insert some malware into a VNF image file while it is being uploaded to an image database or being transferred from an image database to a compute node. Luckily, VNF images can be cryptographically signed and verified during launch time. This can be achieved by setting up some signing authority and modifying the hypervisor configuration to verify an image's signature before they are launched [9].

Security Management and Orchestration

One best practice consists of designing a NFV orchestrator incorporating security and trust requirements of the NFVI. The orchestration and management of security functions requires integration by enabling interaction among the security orchestrator, the VNF manager, and the element management systems (EMS). This type of protection can be achieved by setting scaling boundaries in the VNFD or network service descriptor (NSD), for example, and having the NFVO enforce these restrictions to protect from attacks such as a DNS amplification attack.

Remote Attestation

The remote attestation technique can be used to remotely verify the trust status of a NFV platform. The concept is based on boot integrity measurement leveraging TPM, as mentioned earlier. Remote attestation can be provided as a service, and may be used by either the platform owner or a consumer to verify if the platform has booted in a trusted manner [12]. Practical implementations of the remote attestation service include the open cloud integrity tool (openCIT), an open source software hosted on GitHub.

Table 1 provides a summary of the security risks associated with NFVI as discussed above, and lists the targets of these risks along with possible mitigation techniques.

Open Security Challenges

Despite the best practices described above, there are still open security challenges that are yet to be addressed. One of the security challenges is to define the standard interface in the ETSI NFV architecture to deploy virtual security functions to react to various threats in real time. Such functionalities should be able to communicate with the orchestration modules and follow the provided instructions. Another challenge is to securely manage and monitor VNFs by maintaining their configuration and state information during migration. This can be difficult to perform due to the dynamicity and elasticity of VNF operations in cloud environments. Another challenge is to perform the trust management between different vendors who build NFV hardware and software. The challenge is to efficiently manage the trust chain among vendors and provide trustiness of the final VNF products.

To prevent a VM from impacting other VMs or hosts, it is a good practice to separate VM traffic and management traffic. This will prevent attacks by VMs tearing into management infrastructure. It is also a good idea to separate the VLAN traffic into groups and disable all other VLANs that are not in use.

	Security risk	Target	Best practices
1	Compromised hypervisor	Platform	Separation of VM and management traffic, regular hypervisor patching
2	Isolation failure	Platform/VNFs	Hypervisor introspection, security zoning
3	Platform integrity	Platform	TPM boot integrity, remote attestation
4	DDoS attack	VNFs	Flexible VNF strategic deployment to defend against DDoS
5	Malicious insider	VNFs	Volume/swap encryption, VNF image signing, strict operational practices
6	Regularity compliance failure	VNFs	Geo-tagging using remote attestation

Table 1. NFVI security risks and best practices.

At the moment, attestation technologies only provide the boot time attestation. This does not guarantee run time modification or prevent tampering with the system's critical components, and such modification would only be detected when the system is rebooted. Run time attestation is still an open research area that needs to be explored further. There is also a strong need to develop a comprehensive security architecture to take care of these security challenges in NFVI. To achieve these goals, network operators and vendors need to work together to form a vibrant security ecosystem. New standards, testbeds, and proofs of concept would serve as a catalyst for securing the NFV infrastructure. The services in this new virtualized environment are rapidly evolving, and in turn create new opportunities for innovation.

Conclusion

NFV undoubtedly provides great benefits for telecom service providers in terms of cost efficiency and dynamic service deployability. However, it is extremely necessary to understand the security implications for these benefits. It is essential to know the difference between general cloud computing infrastructure and NFV infrastructure and its needs and requirements. Previous studies presented analysis on security threats that exist in cloud computing along with mitigation techniques. It is equally required that similar studies have to be carried out for security in NFVI. Indeed, NFVI hosts highly sensitive workloads, and accordingly needs to be highly secured and protected. In this article, we identified security attacks on NFVI. We also presented best security practices to protect against these attacks. Admittedly, security in NFVI is still in its infancy, and there are still many open security challenges to tackle. This defines one of the future research directions of the authors. Future work also includes putting into practice the proposed solutions by means of implementations and experimental testbed setups.

Acknowledgement

This article is issued within the research activities of the Finnish Dimecc Cyber Trust Program. It was also partially supported by the ANASTACIA project, which has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 731558, and from the Swiss State Secretariat for Education, Research and Innovation. The authors would like to thank Dr. Ian Oliver from Nokia Bell Labs Finland and Deon Ogle and Shawn Hiemstra from AT&T, for useful discussions.

References

[1] T. Taleb *et al.*, "EASE: EPC as a Service to Ease Mobile Core Network," *IEEE Network*, vol. 29, no. 2, Mar. 2015, pp. 78–88.
[2] T. Taleb, "Towards Carrier Cloud: Potential, Challenges, & Solutions," *IEEE Wireless Commun.*, vol. 21, no. 3, June 2014. pp. 80–91.
[3] W. Yang and C. Fung. "A Survey on Security in Network Functions Virtualization," *2016 IEEE NetSoft Conf. and Wksps. (NetSoft)*, 2016.
[4] B. Han *et al.*, "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, 2015, pp. 90–97.
[5] R. Mijumbi *et al.* "Network Function Virtualization: State-of-the-Art and Research Challenges," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 1, 2015, pp. 236–62.
[6] Z. Yan *et al.*, "A Security and Trust Framework for Virtualized Networks and Software-Defined Networking," *Security and Communication Networks*, 2015.
[7] ETSI Group Specifications: Network Functions Virtualization (NFV); Architectural Framework.
[8] ETSI Published Specifications ETSI GS NFV-SEC 001 V1.1.1: Network Functions Virtualisation (NFV); NFV Security; Problem Statement
[9] Building Secure Telco clouds, Nokia white paper
[10] NFV Security in Practice Series — 9 Top Security Impacting Choices ALCATEL-LUCENT Bell Labs WHITE PAPER
[11] F. Rocha and M. Correia. "Lucy in the Sky Without Diamonds: Stealing Confidential Data in the Cloud," *2011 IEEE/IFIP 41st Int'l. Conf. Dependable Systems and Networks Wksps. (DSN-W)*, 2011.
[12] ETSI GS NFV-SEC 009 Network Functions Virtualisation (NFV); NFV Security; Report on Use Cases and Technical Approaches for Multi-Layer Host Administration, page 34.
[13] R. L. Krutz and R. D. Vines, *Cloud Security: A comprehensive Guide to Secure Cloud Computing*, Wiley Publishing, 2010.
[14] T. Garfinkel and M. Rosenblum. "A Virtual Machine Introspection Based Architecture for Intrusion Detection," NDSS, vol. 3. 2003.
[15] ETSI Published Specifications ETSI GS NFV-SEC 002: Network Functions Virtualisation (NFV); NFV Security; Cataloguing Security Features in Management Software.
[16] T. Taleb, A. Ksentini, and B. Sericola, "On Service Resilience in Cloud-Native 5G Mobile Systems," *IEEE JSAC*, vol. 34, no. 3, Mar. 2016. pp. 483–96.
[17] T. Taleb and Y. Hadjadj-Aoul, "QoS2: A Framework for Integrating Quality of Security with Quality of Service," *Wiley J. Security & Communication Networks*, vol. 5, no. 12, Dec. 2012. pp. 1462–70.

Biographies

Shankar Lal (shankar.lal@aalto.fi) received his B.E degree in electronics enginerring and M.Sc. degree in communication engineering-networking technology from Mehran University, Jamshoro, Pakistan and Aalto University, Espoo, Finland in 2008 and 2015, respectively. He is currently pursuing a doctoral degree at Aalto University, Espoo, Finland since May 2016. He has also been working with Nokia Bell Labs, Finland (previously Nokia Networks) as a research assistant since November 2014. Prior to his work at Nokia, he worked as an IT security engineer at Sapphire Consulting Services in Karachi, Pakistan for three and a half years. His main research interests revolve around security and integrity of NFV components, trusted telco cloud, secure placement of NFV MANO elements, and platform security leveraging the TPM module.

Tarik Taleb [S'04, M'05, SM'10] (tarik.taleb@aalto.fi) received his B.E. degree (with distinction) in information engineering, and M.Sc. and Ph.D. degrees in information science from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is a professor with the School of Electrical Engineering, Aalto University, Finland. He was a senior researcher and 3GPP standardization expert with NEC Europe Ltd. He was then leading the NEC Europe Labs Team, working on research and development projects on carrier cloud platforms. Prior to his work at NEC, he worked as an assistant professor at the Graduate School of Information Sciences, Tohoku University. His current research interests include archi-

tectural enhancements to mobile core networks, mobile cloud networking, mobile multimedia streaming, and social media networking. He has also been directly engaged in the development and standardization of the evolved packet system as a member of 3GPP's System Architecture Working Group. He is an IEEE Communications Society (ComSoc) Distinguished Lecturer. He is a board member of the IEEE ComSoc Standardization Program Development Board. He is serving as the Chair of the Wireless Communications Technical Committee, the largest in IEEE ComSoC. He founded and has been the General Chair of the IEEE Workshop on Telecommunications Standards: From Research to Standards, which is a successful event that received the "Best Workshop Award" from IEEE ComSoC. He is/was on the editorial board of *IEEE Transactions on Wireless Communications*, *IEEE Wireless Communications Magazine*, *IEEE Transactions on Vehicular Technology*, *IEEE Communications Surveys and Tutorials*, and a number of Wiley journals. He has received many awards, including the IEEE ComSoc Asia Pacific Best Young Researcher Award in June 2009. Some of his research work has also received Best Paper Awards at prestigious conferences.

ASHUTOSH DUTTA [SM] (ad5939@att.com) is currently Lead Member of Technical Staff at AT&T's Chief Security Office in Middletown, New Jersey. His career, spanning more than 30 years, includes Director of Technology Security at AT&T, CTO of Wireless at cybersecurity company NIKSUN, Inc., Senior Scientist at Telcordia Research, Director of the Central Research Facility at Columbia University, adjunct faculty at NJIT, and computer engineer with TATA Motors. He has more than 90 conference and journal publications, three book chapters, and 30 issued patents. He is co-author of the book *Mobility Protocols and Handover Optimization: Design, Evaluation and Application*, published by IEEE and John & Wiley, that was recently translated into Chinese. An active IEEE and ACM volunteer, he served as the chair for IEEE Princeton/Central Jersey Section, Industry Relation Chair for Region 1 and MGA, Pre-University Coordinator for IEEE MGA, and vice chair of Education Society Chapter of PCJS. He co-founded the IEEE STEM conference (ISEC) and helped implement EPICS (Engineering Projects in Community Service) projects in several high schools. He currently serves as the Director of Industry Outreach for the IEEE Communications Society and is the co-lead for the IEEE 5G initiative. He was the recipient of the prestigious 2009 IEEE MGA Leadership Award and the 2010 IEEE-USA Professional Leadership Award. He obtained his B.S. in electrical engineering from NIT Rourkela, India, an M.S. in computer science from NJIT, and a Ph.D. in electrical engineering from Columbia University under the supervision of Prof. Henning Schulzrinne. He is a senior member of ACM.

ACCEPTED FROM OPEN CALL

Drone-Assisted Public Safety Networks: The Security Aspect

Daojing He, Sammy Chan, and Mohsen Guizani

With enhanced functionalities and capabilities, unmanned aerial vehicles, commonly referred to as drones, can be equipped with communication hardware and sent to suitable positions in the field to augment the operation of public safety networks. Security is of primary importance in such drone-assisted public safety networks because sensitive or critical information could be transmitted among these network entities.

ABSTRACT

Public safety networks are based on wireless communication technologies, and are particularly important in field operations to support the mobility of first responders. With enhanced functionalities and capabilities, unmanned aerial vehicles, commonly referred to as *drones*, can be equipped with communication hardware and sent to suitable positions in the field to augment the operation of public safety networks. Security is of primary importance in such drone-assisted public safety networks because sensitive or critical information could be transmitted among these network entities. This article examines the cyber security issues of such networks.

INTRODUCTION

Public safety (PS) has the important role of maintaining a stable and secure environment in our society. PS services aim to protect people, assets and the environment from a wide range of threats such as natural disasters, acts of terrorism and technological accidents. Public safety networks are wireless communication networks, which are particularly important in field operations to support the mobility of first responders. Traditionally, they have been based on TETRA (terrestrial trunked radio) and APCO (Association of Public-Safety Communications Officials) systems.

It has been increasingly recognized that effective communications is key to the successful management of emergency and disaster situations [1]. For example, the exchange of multimedia information (e.g., data, voice and video) improves the coordination of PS officers and response efforts during an emergency. This is reflected in increasing efforts to develop broadband public safety networks by governments, standards bodies and academia. Recently, a bill from U.S. Congress and the FCC has laid the groundwork for creating a nationwide broadband public safety network based on technologies such as LTE (Long Term Evolution) and its foreseen 5G successor. The 3GPP has recently started developing the capabilities in LTE-Advanced to support the specific requirements of public safety networks. Moreover, WiFi-based ad hoc networks have also been proposed by the research community [2].

It should be noted that base stations in mobile telecommunications networks could possibly break down due to natural disasters or malicious attacks, or it could be impossible or too risky to allow first responders to set up an ad hoc network in some areas. In either case, communications among first responders is disabled. To address these issues, unmanned aerial vehicles (UAVs), commonly referred to as drones, can be equipped with communication hardware and sent to suitable positions in the field so they can act as aerial mobile stations, intermediate nodes to expand coverage through relaying or multi-hop communication methods, or end terminals [1, 3–6]. This results in drone-assisted public safety networks, as shown in Fig. 1.

The addition of drones into public safety networks can help reduce coverage gaps and network congestion. Compared to terrestrial communication systems or those based on high-altitude platforms, low-altitude drone-assisted systems are in general faster to deploy, more cost-effective by enabling on-demand operations, more flexibly reconfigured due to their fully controllable mobility, and likely to have better communication channels due to line-of-sight links. Moreover, drones can provide great assistance in observing and analyzing certain disaster situations because they can get into areas that are difficult or impossible for first responders to reach.

With the function of facilitating law and order maintenance, life and property protection, and emergency response, public safety networks are required to carry extremely sensitive data, e.g., criminal records, vehicular telemetry and medical records of patients, reliably and securely. Since drone-assisted public safety networks often operate in adverse situations in which the normal functioning of a society has been disrupted, maintaining security becomes most important and difficult.

Although drone-assisted public safety networks have attracted the interest of researchers [1, 3–6], to the best of our knowledge, little attention has been paid to the security of such networks. In the literature, the focus is on conventional problems and solutions to improve performance in terms of coverage, quick mobility, and reliability.

Besides cyber attacks, drone-assisted public safety networks are obviously also subject to physical attacks. For example, the attacker can shoot down a drone and gain access to the sensitive or critical information carried by the drone. However, in this article we focus on the cyber

Digital Object Identifier:
10.1109/MCOM.2017.1600799CM

Daojing He (corresponding author) is with East China Normal University; Sammy Chan is with City University of Hong Kong; Mohsen Guizani is with the University of Idaho.

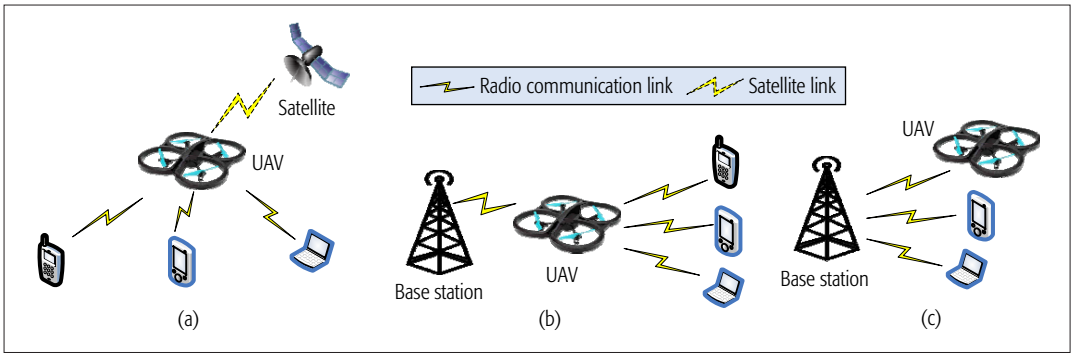


Figure 1. Typical drone-assisted public safety networks: a) s drone acts as the aerial mobile station; b) a drone acts as a routing node, and c) a drone acts as an end terminal.

The involvement of drones raises new security issues in public safety networks. Primarily, the complexity of network infrastructure is increased, introducing more opportunities for security attacks. This dramatically increases the efforts required to analyse and defend the system.

security aspects of drone-assisted public safety networks. We discuss general threats that are inherent to wireless networks. We also describe specific attacks due to the involvement of drones, along with some example implementations.

Why Drone-Assisted Public Safety Networks are Vulnerable?

The involvement of drones raises new security issues in public safety networks. Primarily, the complexity of network infrastructure is increased, introducing more opportunities for security attacks. This dramatically increases the effort required to analyze and defend the system. Also, PS officers relying on UAVs to carry their traffic need to send all packets to the UAVs. Thus, they are subject to privacy invasions.

Moreover, generally, UAV platforms comprise various modules to enable proper functioning, but this also makes them vulnerable to potential malicious attacks. One such attack exploits the sensor inputs of UAVs. In some cases, UAVs are equipped with sensors to monitor parameters in the environment in order to search for specific items. If an attacker manages to manipulate such parameters to mis-guide the sensors, the efficacy of the mission will be compromised. This could cause the PS officers to react wrongly to some false events, or prevent them from identifying the item being searched. For example, many UAVs are equipped with a global positioning system (GPS) module. If an adversary somehow is able to feed wrong GPS signals to the module, the reliability of the UAV system would be seriously hindered.

Another potential vulnerability exists in the communication module of UAVs. Since UAVs are controlled by the ground station, most of them are equipped with wireless communication modules to exchange data and commands with the ground station. Commonly, Zigbee or Wi-Fi technologies are used. While this feature is important to UAV functionality, it also introduces a potential risk as adversaries may possibly intercept or interfere the wireless signals. This could cause an imminent danger. For example, an enemy can block critical information to prevent the PS officers from maneuvering away from a danger zone. Another possible threat is a denial-of-service attack. An adversary could keep a server busy by sending it large number of meaningless packets so that it is not able to receive any relevant data from UAVs. This could cause the PS officers to lose control of the UAVs.

Security Challenges in Drone-Assisted Public Safety Networks

From the perspective of security and threat analysis, it should be noted that a typical drone-assisted public safety network is different from traditional wireless networks such as wireless sensor networks (WSNs) and mobile ad-hoc networks (MANETs). For example, a WSN carries less information and consumes less power than a drone-assisted public safety network. Moreover, the coverage area for a drone-assisted public safety network is much larger than that of a WSN. Also, while nodes in WSNs usually transmit their sensed data to the sink node, the UAVs in drone-assisted public safety networks communicate with both the ground control station and mobile devices independently.

The security mechanisms in drone-assisted public safety networks should at least guarantee confidentiality, integrity, authenticity, and availability of communication channels. Often, information exchange among UAVs as well as between UAVs and the ground station requires low latency. The security challenges to drone-assisted public safety networks are due to the resource constraints of UAVs and the delay constraint.

General Security Threats and Their Countermeasures

The basic security properties of drone-assisted public safety networks should include confidentiality, integrity, availability, authenticity, privacy preservation and non-repudiation. They ensure:

1. Information carried in the networks (e.g., camera data in the UAVs) are not disclosed to unauthorized parties.
2. Information cannot be modified by unauthorized users.
3. Resources (e.g., the communication bandwidth) are available for authorized users whenever they are needed.
4. Users (e.g., first responders) are exactly whom they claim to be.
5. Information of users is not disclosed.
6. Users cannot deny the actions they have executed.

These security properties could be breached by different attacks. For example, eavesdropping on communication channels can break confiden-

tiality. Another example of attacks is to jam the channel such that the functionalities of UAVs is not available to the ground control station. As shown in Fig. 2, similar to other communication networks such as WSNs, attacks on drone-assisted public safety networks can be classified into four general categories. Interruption means that a message from/to a particular service is blocked. For example, an adversary can launch routing attacks such as black hole or grey hole attacks. In a black (grey) hole attack, a malicious node announces itself on the lowest-cost path to the destination node and drops all (some selected) received packets. Interception can be achieved by eavesdropping on channels. This facilitates traffic analysis and disclosure of message contents. Modification means replacing an original message to a particular service with a modified one. Fabrication includes message forgery, UAV spoofing, mobile user spoofing and base station spoofing.

Cryptographic mechanisms are commonly used to tackle the above categories of attacks. Encryption techniques are used to ensure confidentiality. Integrity can be checked by the use of hash functions such as message authentication codes. Authenticity is ensured by the use of passwords, which may involve a certification agent. Privacy can be preserved by privacy-aware cryptographic primitives such as blind signature and group signature. Non-repudiation can be enforced by using digital signatures. Table 1 lists the identified threats and the commonly used countermeasures for them.

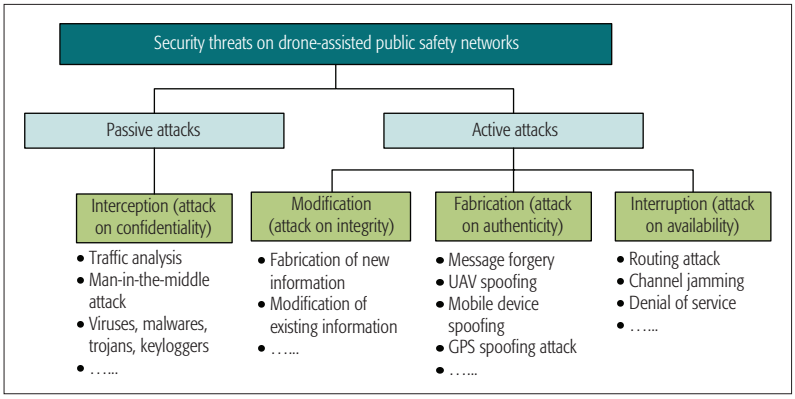


Figure 2. Security threats on the drone-assisted public safety network.

	Threat	Categories	Countermeasures
1	An adversary compromises security of communication links between various network components through network attacks such as hacking, eavesdropping, identity spoofing and cross-layer attacks	Attacks on confidentiality	Encryption of the data
2	An adversary alters the data during transit or while in storage.	Attacks on integrity	Hash functions such as message authentication code
3	An adversary jams the channel or performs DoS attacks against the networks	Attacks on availability	Strong authentication and incident detection and reporting mechanisms
4	An adversary gains the necessary privilege to access and modify the data stored on the network components such as UAVs.	Attacks on authenticity	Authentication and encryption of the data

Table 1. General security threats and countermeasures.

Some Specific Security Threats

WiFi Attacks

WiFi is a wireless communication technology commonly used in drones for remote control or data communications. Kamkar has proposed a WiFi attack, SkyJet, that enables an attacker to look for drones in its vicinity and take control of those drones [7], turning them into zombie drones. SkyJet is implemented by using off-the-shelf software tools such as *aircrack-ng* and *node.js*. Essentially, SkyJet uses aircrack-ng to detect nearby wireless networks and clients, deactivate the controller connected to the target drone, and connect the attacker with the victim drone as its new controller. Then, node.js enables the attacker to feed commands to the victim drone.

SkyJet can be further extended such that it is still an effective attack even when encryption is used in data communications between a drone and its controller. Here, we describe and implement such an extension. As specified in the IEEE 802.11 standards, the original data confidentiality mechanism for WiFi is provided by the Wired Equivalent Privacy (WEP) protocol, which is based on the stream Rivest Cipher RC4. The standard key length is 40 bits, plus 24 bits of initialization vector (IV). The expanded key length of WEP is 104 bits. To increase the security strength, WEP is replaced by the Wi-Fi Protected Access (WPA) protocol, which is still based on RC4, but uses 128 bits of cipher key and 48 bits of IV.

A replay attack intercepts data in transmission and retransmits them at a later time. As a WiFi attack, replaying ARP (Address Resolution Protocol) requests can be used to crack the encryption key. The attacker first eavesdrops an ARP request and then starts repeatedly replaying it. Each time a replayed ARP request reaches the drone with IP address as specified in the request, an ARP response is returned by the drone. Each ARP response contains a newly generated IV. By replaying a large number of requests and hence collecting a sufficient number of new IVs, the attacker can crack the encryption key. Aircrack-ng is a WEP and WPA-PSK cracker based on such an approach. As shown in Fig. 3, in our implementation, the attacker (based on a Raspberry Pi computer) first surveys, selects and attacks Wi-Fi networks, and then joins compromised networks and controls the targeted UAV.

There are three attack phases in Aircrack, each realized by an individual module. The first nodule is a wireless sniffing tool, airdump, which aims to discover WEP-enabled networks. The second module is an injection tool, airplay, which increases traffic. Finally, the third module is aircrack-ng, which makes uses of collected IVs to crack WEP keys.

Also, the attacker can launch a deauthentication attack, in which a series of deauthentication frames are generated, with the purpose of disrupting a WiFi connection protected by WPA2 encryption. Aircrack is the suite of penetration testing tools that can be used to implement this attack. First, the wireless network interface card of the attacker is set to monitoring mode. Subsequently, as shown in Fig. 4, the attacker finds all the wireless networks by using Aircrack, and then

disrupts the communication connection between the network KYJJ-TEST and the mobile terminal (with MAC address F4:8B:32:27:3D:37).

GPS Spoofing

Today, the location of a mobile device is determined by a GPS signal. It is important to ensure that the data received through the GPS receivers is legitimate. Otherwise, if GPS data is spoofed, a false estimation of the device's position will be made. Furthermore, if a UAV is fully automated, it will be led to a false target location by its on-board guidance system. This type of attack leads to failed missions and possibly loss of assets, such as the recent claimed theft of an RQ 170 Sentinel by Iranian forces. In [8], Humphreys postulates a GPS-spoofing-attack is used to affect the navigation system of the UAV. The attack overlays a high-power spoofed GPS signal generated by a local transmitter on the GPS satellite signal, falsifying the estimation of the current position and leading the drone to land on an Iranian airfield. Note that GPS attacks are mostly on the non-line-of-sight (NLOS) operations (e.g., automatic path control) of a drone.

In the past, mounting a spoofing attack with a GPS signal simulator was not easy; first, because modern simulators were expensive (each one could cost about $400K US dollars); second, most GPS signal simulators were heavy and cumbersome [9]. However, in recent years, the cost of such equipment has dropped significantly, because of the availability of low-cost hardware, e.g., the universal software radio peripheral (USRP) [10], along with open-source codes for software defined radio such as GNU radio.

As shown in Fig. 5, we have implemented a GPS signal simulator to launch GPS spoofing attacks. We attach a power amplifier and an antenna to a GPS signal simulator (here a USRP B200 is used) and radiate the RF signal toward the target receiver. The USRP sends periodic signals, which are simultaneously repeated by the antenna.

There are anti-spoofing techniques to detect GPS signal simulators. On the other hand, more advanced spoofers are available, which are relatively hard to detect. For example, a receiver-based spoofer, comprised of a GPS receiver concatenated with a spoofing transmitter, is more sophisticated. Its generated signal is synchronized with the real GPS signals. Even receivers in tracking mode can be spoofed [11]. Unfortunately,

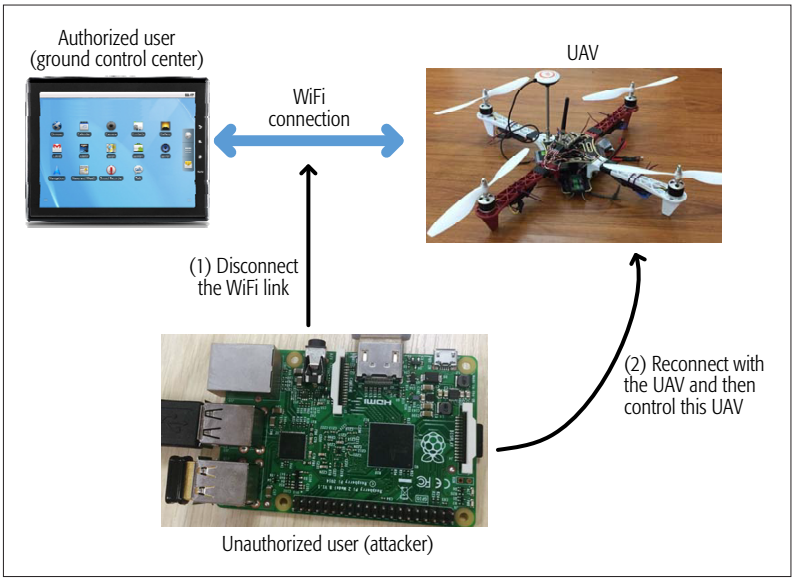


Figure 3. The Wi-Fi attack procedures.

```
CH  7 ][ Elapsed: 1 min ][ 2015-08-08 15:41

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

64:09:80:79:E0:26  -51      192       100    0  11  54e  WPA2 CCMP   PSK  908
24:05:0F:15:FB:CA  -61      183         7    0  11  54e. OPN              KYJJ-TEST
0C:D9:96:01:34:50  -61      187       173    0   1  54e. OPN              ECNU
6C:E8:73:1C:97:5E  -72      330         0    0   6  54e. OPN              TP-LINK_1C975E

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   64:A6:51:0D:BF:1A  -79    0 - 1      0         4
(not associated)   78:92:9C:85:60:82  -79    0 - 1      0         1
(not associated)   8C:29:37:EE:A3:14  -67    0 - 1      0         3  ECNU
64:09:80:79:E0:26  B0:9F:BA:4C:A7:A9  -44    0e- 0e     0        15
64:09:80:79:E0:26  64:5A:04:C5:5E:1A  -46    0e- 0e     1        21  908
64:09:80:79:E0:26  38:BC:1A:0D:E9:18  -47    0 - 0      0        15
64:09:80:79:E0:26  34:23:87:4B:FE:19  -57    0e- 1      0         7
64:09:80:79:E0:26  98:5A:EB:9F:34:78  -61    0e-24      0        22
24:05:0F:15:FB:CA  F4:8B:32:27:3D:37  -39    0 - 1e     0       184
0C:D9:96:01:34:50  00:26:C7:92:21:1C  -67    0 - 1      0        13  ECNU
```

(a) The results of the network scan

```
qyh@qyh-Vostro-3900:~/temp/wifi-test$ sudo aireplay-ng -0 3 -a 24:05:0F:15:FB:CA -c F4:
8B:32:27:3D:37 wlan0
15:55:57  Waiting for beacon frame (BSSID: 24:05:0F:15:FB:CA) on channel 11
15:55:58  Sending 64 directed DeAuth. STMAC: [F4:8B:32:27:3D:37] [ 0| 3 ACKs]
15:55:59  Sending 64 directed DeAuth. STMAC: [F4:8B:32:27:3D:37] [ 0| 8 ACKs]
```

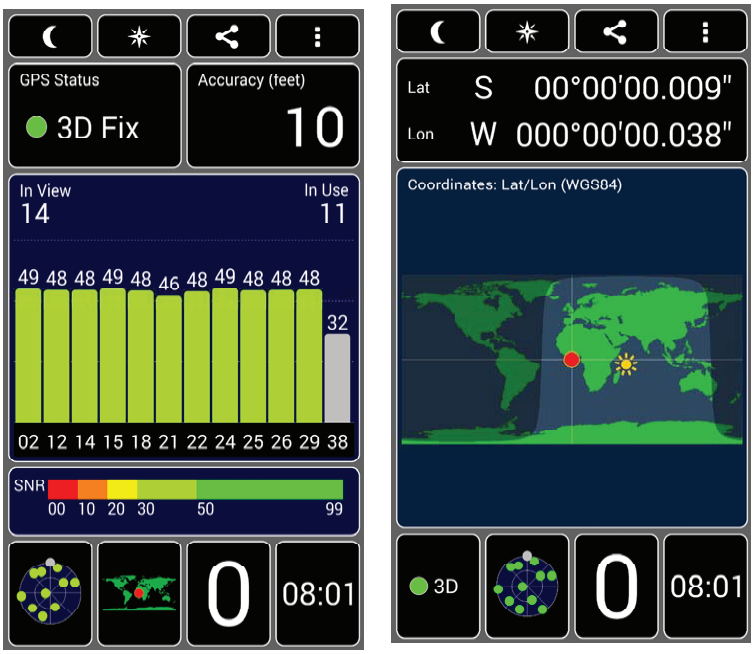
(b) The disconnection of the mobile terminal (its MAC address is F4:8B:32:27:3D:37)

Figure 4. Details of deauthentication attack.

the limited capabilities of the drone (e.g., battery power) limit some of the recently proposed techniques. On the other hand, the energy efficient mitigation techniques of correlating GPS data with measurements of the inertial measurement unit (IMU) on the drone are feasible, provided that the additional load on the drone due to the IMU is acceptable.

The biggest challenge is encrypting civilian GPS since it means a significant upgrade of the infrastructure and is very costly. There are ways to detect a counterfeit signal, but they are not guaranteed to ward off a very sophisticated spoofing attack. They mainly depend on the ratio of signal strength to noise; if it exceeds a certain threshold, an alarm is raised to indicate the signal is probably being spoofed. Alternatively, the existence of counterfeit positioning signals can be revealed by checking the consistency between the measurements at the position layer and those from other external sensors such as Wi-Fi access points. However, this approach incurs higher hardware and software complexity. Thus, novel and efficient approaches are needed to secure GPS. For example, some algorithms should be employed in civil GPS receiver chipsets to detect spoofing. Also, for civil GPS transmitters, it is feasible to add digital signatures into the extensible GPS civil navigation message.

(a) Hardware setup.



(b) The results of GPS spoofing attack (through phone's GPS API)

Figure 5. Details of a GPS spoofing attack: a) hardware set up; b) the results of GPS spoofing attack (through phone's GPS API).

Implementing Security Services in Drone-assisted Public Safety Networks

Key Establishment and Trust Setup

One of the key steps in setting up a drone-assisted public safety network is to establish cryptographic keys for subsequent use. There have been a variety of protocols to achieve that in WSNs and MANETs [12]. However, due to the inherent properties of public safety networks, those protocols are not suitable. In emergency situations, a public safety network should have the capability for fast network establishment without disabling security functions, making some public-key cryptographic primitives and their extended versions too expensive in terms of system overhead (e.g., communication overhead, key establishment and update time). Also, most of the existing key management protocols for public safety networks do not consider the existence of the UAVs.

For supporting fine-grained access control, the traditional public key based encryption schemes need to use different keys to encrypt multiple copies of a file. Such a scalability problem can be tackled by one-to-many encryption methods such as attribute-based encryption (ABE). With ABE, data is encrypted under a set of attributes such that only the users with the expected properties can decrypt and then obtain the data. As a result, encryption and key management become more efficient. For secure broadcast communication scenarios, ABE can be used to support efficient broadcast key distribution, and allow the user to achieve the authorization and delegation with some constraints. Terminal or user attributes and their relationship are maintained by the unified cryptosystem. When the data or communication keys are being distributed, they are bounded with the expected property by using the ABE algorithm.

Moreover, the trust relation patterns of drone-assisted public safety networks differ from other wireless networks. More specifically, most of the existing key management protocols assume either participating nodes already have established a trust relationship, or there exists a trusted third party such as a key distribution server. Unfortunately, this assumption would not hold during the rescue operation in major disasters because first responders most likely belong to different organizational units. This makes the problem of key management and distribution in public safety networks challenging. This issue may be addressed at a higher organizational level, independent of any particular communications technology.

Ultimately, drone-assisted public safety networks need a secure, efficient and scalable key-distribution mechanism that allows simple and quick key establishment by exploring the features of such networks.

Intrusion Detection

Similar to other networks, intrusions will bring attacks to public safety networks. Therefore, traffic from both inside and outside of a network needs to be monitored and analyzed for anomalies. This is usually carried out by an intrusion detection sys-

tem (IDS) that aims to identify cyber attacks by examining the audit data collected at different parts of a network. However, the approaches used in wired networks are computationally expensive. What public safety networks need are approaches that are computational- and energy-efficient. Very recently, Mitchell and Chen proposed a general framework called a *behavior rule-based unmanned air vehicle intrusion detection system* (BRUIDS) as an IDS for detection of malicious UAVs in an airborne system [13]. The run-time resources required by BRUIDS is minimal. In addition, by dynamically adjusting its detection strength to meet the requirement for a maximum false negative rate, it is adaptive to changing environments.

Secure Data Aggregation

One benefit of a drone-assisted public safety network is the fine-grain sensing that large sets of drones can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic sent to the base station. For example, the system may combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the public safety network, aggregation may take place in different parts of the network.

Although data aggregation can reduce consumption of communication bandwidth and energy, it introduces a new challenge of how to aggregate encrypted data, because data are encrypted before transmission by drones. In this regard, a method that can directly aggregate encrypted data is needed. Homomorphic encryption (HE) is such a method by which N ciphertexts can be aggregated into a single ciphertext without the need to decrypt the ciphertexts. Recently, a practical secure data aggregation scheme based on additive HE has been proposed [14]. With this scheme, the total length of ciphertexts can be reduced, and end-to-end confidentiality is achieved. On the other hand, by incorporating a pairing-free identity-based signature scheme, hop-by-hop authentication is supported. That is, not only the base station, but also the aggregators can verify the authenticity of all the transmitted encrypted data.

Secure Group Management

Although a drone may have limited computing capabilities, a group of drones can be deployed to perform in-network data aggregation and analysis, or other key services provided by public safety networks. This leads to the need for secure group communication protocols, which admit new group members securely and support secure communication among group members. One of the major requirements of such protocols is computational and energy efficiency. For example, group authentication is very important in secure group communications. It is able to authenticate all group users as a batch, instead of authenticating each group user individually.

Recently, Bian *et al.* presented a secure communication framework for UAV networks [15]. Using an information dispersal algorithm, high fault-tolerance is provided by their framework. Moreover, based on security-enhancing mechanisms, the risk of exposing information to adversaries is reduced. Before each data packet is sent to a nearby UAV, it is signed digitally with the drone's private key to ensure integrity and authenticity. Their framework is particularly suitable for situations in which a large number of drones are simultaneously involved in carrying out a mission in hostile environments.

Conclusion and Future Work

The use of UAVs with broadband wireless technologies will serve as the pillar of next generation networks for public safety. To reap the benefits of such an architecture, security is one of the technical challenges that need to be addressed, especially attack vulnerabilities due to the involvement of UAVs. More research is needed to ensure that cyber security of public safety networks would not be compromised due to the introduction of UAVs. For example, although existing proprietary drone-assisted public safety networks have cyber security measures, they can only provide weak protection. As a result, security risks such as unauthorized access, malicious control, illegal connection or other malicious attacks still exist. One possible future direction is to develop a unified security access specification for these networks.

The use of UAVs with broadband wireless technologies will serve as the pillar of next generation networks for public safety. To reap the benefits of such an architecture, security is one of the technical challenges that need to be addressed, especially attack vulnerabilities due to the involvement of UAVs.

Acknowledgment

This research is supported by the National Science Foundation of China (Grants 51477056 and U1636216), a strategic research grant from City University of Hong Kong (Project No. 7004615), the Pearl River Nova Program of Guangzhou (No. 2014J2200051), the Shanghai Rising-Star Program (No. 15QA1401700), the CCF-Venustech Hongyan Research Initiative, and the State Grid Corporation Science and Technology Project "The pilot application on network access security for patrol data captured by unmanned planes and robots and intelligent recognition based on big data platform" (Grant No. SGSDDK000KJJS1600065).

References

[1] X. Li *et al.*, "The Public Safety Wireless Broadband Network with Airdropped Sensors," *Proc. 2015 IEEE China Summit and Int'l. Conf. Signal and Information Processing (ChinaSIP)*, July 201, pp. 443–475.
[2] R. Ferrus *et al.*, "LTE: The Technology Driver for Future Public Safety Communications," *IEEE Commun. Mag.*, vol. 51, no. 10, Oct. 2013, pp. 154–61.
[3] Z. Fadlullah *et al.*, "A Dynamic Trajectory Control Algorithm for Improving the Communication Throughput and Delay in UAV-Aided Networks," *IEEE Network*, vol. 30, no. 1, Jan–Feb. 2016, pp. 100–05.
[4] X. Li *et al.*, "Drone-Assisted Public Safety Wireless Broadband Network," *Proc. 2015 IEEE Wireless Commun. and Networking Conf. Wksp. (WCNCW)*, Mar. 2015, pp. 323–28.
[5] A. Merwaday and I. Guvenc, "UAV Assisted Heterogeneous Networks for Public Safety Communications," *Proc. 2015 IEEE Wireless Commun. and Networking Conf. Wksp. (WCNCW)*, Mar. 2015, pp. 329–34.
[6] G. Baldini *et al.*, "Survey of Wireless Communication Technologies for Public Safety," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 2, May 2014, pp. 619–41.
[7] SkyJet, https://samy.pl/skyjack/.
[8] T. Humphreys, "Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systemes to Civil GPS Spoofing," University of Texas at Austin, July 18, 2012.
[9] T. E. Humphreys *et al.*, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," *Proc. ION GNSS Int'l. Technical Meeting of the Satellite Division*, 2008.
[10] N. Tippenhauer *et al.*, "On the Requirements for Successful GPS Spoofing Attacks," *Proc. ACM Conf. Computer and Communications Security*, 2011, pp. 75–86.
[11] K. Hartmann and C. Steup, "The Vulnerability of UAVs to Cyber Attacks—An Approach to the Risk Assessment," *Proc. 2013 5th Int'l. Conf. Cyber Conflict (CyCon)*, June 2013, pp. 1–23.

[12] C. Chen *et al.*, "A Bilinear Pairing-Based Dynamic Key Management and Authentication for Wireless Sensor Networks," *J. Sensors*, vol. 2015, 2015, pp. 1–14.
[13] R. Mitchell and R. Chen, "Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications," *IEEE Trans. Systems, Man, and Cybernetics: Systems*, vol. 44, no. 5, May. 2014, pp. 593–604.
[14] K.-A. Shin and C.-M Park, "A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Systems*, vol. 26, no. 8, Aug. 2015, pp. 593–604.
[15] J. Bian, R. Seker, and M. Xie, "A Secure Communication Framework for Large-Scale Unmanned Aircraft Systems," *Proc. 2013 Integrated Communications Navigation and Surveillance Conference (ICNS)*, Apr. 2013, pp. 1–12.

Biographies

Daojing He [S'07, M'13] (djhe@sei.ecnu.edu.cn) received the B.Eng. (2007) and M. Eng. (2009) degrees from Harbin Institute of Technology (China) and the Ph.D. degree (2012) from Zhejiang University (China), all in computer science. He is a professor with the School of Computer Science and Software Engineering, East China Normal University, P.R. China. His research interests include network and systems security. He is an associate editor or on the editorial board of international journals such as *IEEE Communications Magazine* and *IEEE/KICS Journal of Communications and Networks*.

Sammy Chan [S'87, M'89] (eeschan@cityu.edu.hk) received B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. From 1989 to 1994 he was with Telecom Australia Research Laboratories, first as a research engineer, and between 1992 and 1994 as a senior research engineer and project leader. Since December 1994 he has been with the Department of Electronic Engineering, City University of Hong Kong, where he is currently an associate professor.

Mohsen Guizani [S'85, M'89, SM'99, F'09] (mguizani@ieee.org) received the B.S. (with distinction) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and Chair of the Electrical and Computer Engineering Department at the University of Idaho, USA. He was a professor and the Associate Vice President for Graduate Studies at Qatar University, Doha, Qatar. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial boards of six technical journals, and he is the Founder and EIC of the journal *Wireless Communications and Mobile Computing*, published by John Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is a Senior member of ACM.

4 tracks. 3 days. 1 global conference.

Fog computing & networking – the necessary architecture for IoT, 5G and embedded AI.

Fog World Congress™

October 30 - November 1, 2017 | Santa Clara, California

Jointly produced by IEEE ComSoc™ IEEE Communications Society | OpenFog™

Learn what it's all about – why it matters and how to adapt fog in your environment – at Fog World Congress.

Trend-setting keynotes. Technical sessions. Industry use cases. Advanced research. Plus a hackathon, exhibition area and demos for hands on learning.

Early bird registration now open.

www.fogworldcongress.com