IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 1, 2018, accepted November 25, 2018, date of publication November 28, 2018,
date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2883787

Critical Communications Over Mobile Operators' Networks: 5G Use Cases Enabled by Licensed Spectrum Sharing, Network Slicing and QoS Control

MARKO HÖYHTYÄ[1], (Senior Member, IEEE), KALLE LÄHETKANGAS[2], (Student Member, IEEE), JANI SUOMALAINEN[1], MIKA HOPPARI[1], KAISA KUJANPÄÄ[1], KIEN TRUNG NGO[1], TERO KIPPOLA[3], MARJO HEIKKILÄ[3], HARRI POSTI[2], JARI MÄKI[4], TAPIO SAVUNEN[5], ARI HULKKONEN[6], AND HEIKKI KOKKINEN[7]

[1]VTT Technical Research Centre of Finland Ltd., 90571 Oulu, Finland
[2]Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland
[3]Vierimaantie Campus, Centria University of Applied Sciences, 84100 Ylivieska, Finland
[4]Airbus Defence and Space Oy, 00380 Helsinki, Finland
[5]Department of Communications and Networking, Aalto University, 00076 Aalto, Finland
[6]Bittium Wireless Ltd., 90590 Oulu, Finland
[7]Fairspectrum Oy, 02150 Espoo, Finland

Corresponding author: Marko Höyhtyä (marko.hoyhtya@vtt.fi)

This work was supported by Business Finland through the CORNET Project.

ABSTRACT Commercial mobile operators' networks will be used for public safety communications due to demand for wireless broadband services, new applications, and smart devices. Existing dedicated professional mobile radio networks, such as terrestrial trunked radio, Tetrapol, and project 25, are based on narrowband technologies and hence their data bandwidth is limited. This paper studies how critical communications needed, e.g., by ambulance personnel, rescue squads, and law enforcement agencies can be implemented over a 5G network. The most important technology enablers are described and test network architectures used in our project given. We focus on two different use cases. First, how to enable priority communications over a commercial mobile network. Second, how to create rapidly deployable networks for emergency and tactical operations. Tests done with the implemented systems in real networks show that both approaches are very promising for future critical users. Techniques such as network slicing and licensed shared access provide means to support mission critical applications in any environment.

INDEX TERMS Public safety, priority communications, mission-critical communications.

I. INTRODUCTION

Traditionally public safety communications services have been provided with narrowband professional mobile radio (PMR) systems such as terrestrial trunked radio (TETRA) and Tetrapol in Europe and project 25 (P25) in North America [1]. The trend is going towards commercial mobile broadband networks e.g. long term evolution (LTE) and fifth generation (5G) networks in the future due to demands for broadband services, new applications and smart devices. For example, multimedia transmission is useful in many critical scenarios but current PMR systems support this kind of services poorly. The maximum data rate of the TETRA system is 28.8 kbps and for the P25 system it is 9.6 kbps. Enhanced TETRA may reach a few hundred kilobits per second which is not yet enough for many multimedia services. Thus, there is a need for higher transmission rates. There are already ongoing projects for nationwide next generation public safety services based on mobile operators networks, e.g. FirstNet in the US, Emergency Services Network (ESN) in the UK and SafeNet in Republic of Korea. Mission critical users such as police officers, border guards, ambulance personnel, and fire and rescue need reliable communications, high availability, and security that cannot be matched without numerous technological enablers. Key enabling technologies for critical communications in fourth generation (4G) networks standardized by 3rd generation partnership project (3GPP) are device-to-device (D2D) communications and proximity services (ProSe), group communications, mission-critical push-to-talk, video and data (MCPTT, MCVideo, MCData), quality of service (QoS) and prioritization mechanisms including preemption, and end-to-end security.

The situation will be further improved in 5G systems that will enable seamless integration of multiple radio and network technologies and even creation of logical public safety networks within the same infrastructure as is used for commercial users [2]. Development of 5G includes a diverse set of technologies such as software-defined networking (SDN), multi-access edge computing (MEC) and spectrum sharing to better support different application areas [3]–[5]. Especially licensed spectrum sharing approaches that guarantee QoS for sharing applications are promising also for rapid deployment of public safety networks.

There is a need for practical testing and trials to verify how the proposed technologies can be used e.g. in 3GPP evolution networks. 5G test network activities are going on globally, in Finland aim is to build an infrastructure where beyond state-of-the art technologies and flexible service configurations are developed and tested. Recently, we demonstrated citizen broadband radio service (CBRS) [6] technologies in live trials with commercial network devices. We have implemented and tested licensed shared access (LSA), QoS and policy control mechanisms and network slicing techniques [7]–[14] to run critical traffic such as MCPTT in our test network. Our trial environment is geographically diverse, distributed to several locations in Finland and it supports multiple domains. In addition, it enables a combination of techniques both on the core network and access network sides.

The main motivation for this paper is to show how critical communication use cases are implemented in a 5G network. Our work complements previous studies reported in [1]–[5] by 1) reviewing mission-critical services and latest enabling techniques and standards in 5G and by 2) implementing and studying use of commercial technologies for mission-critical services in two important use cases. In the priority communication use case we use the policy and charging rules function (PCRF) in the core network for dynamic QoS management to prioritize the MCPTT application. In the rapidly deployable network use case, we implement a distributed LTE network for the scenarios where the commercial network might be unavailable. We further use LSA and sensing to find the spectrum information for the available frequencies for our network.

This article is organized as follows. First we describe needed technological enablers and review the advances within 3GPP standardization. Then we present the trial environment for priority communications and discuss how we implemented MCPTT application in the network. Another trial environment focusing on a rapidly deployable network and a distributed LSA solution is given in the following part. Finally, we define promising future research ideas and conclude the paper.

II. ENABLERS FOR CRITICAL COMMUNICATIONS

Mission-critical communication services in mobile operators' networks require multiple technological enablers that are continuously advanced in standardization. Various QoS control methods can be used to guarantee required level of low latency, packet error loss, and high priority. We review the status of standardization and describe the main mechanisms under the 3GPP roadmap. Reliability and integrity of the communication are crucial for authorities and thus, security mechanisms are needed. In addition, softwarization of future networks and edge computing enables to tailor the network to specific needs of the critical users. For example, network slicing can be used to create a logical network inside the physical network to guarantee enough communication resources e.g. for ambulance communications. In some occasions spectrum sharing technologies are crucial in finding suitable radio resources for communications e.g. when the current infrastructure has been damaged or lost. Finally, multiple radio technologies are integrated in the 5G system and they can be seamlessly used to support different capacity and communication range needs of the users. More detailed description of each enabler can be found in the following subsections.

A. 3GPP ROADMAP AND QoS CONTROL

3GPP is the main standardization body for 5G technologies. Figure 1 shows how supporting technologies are included in different releases of 3GPP standardization to enable critical communications over commercial networks. The QoS concept [7] has been included since Rel. 8 and the following releases have advanced the QoS mechanisms. Device-to-device communications (D2D) [8] was included already in Rel. 12 to enable different proximity services and operation of critical users even without supporting infrastructure. Group communication enablers [9] were developed in the same release and improved in the following 13th release. Support for mission-critical push-to-talk is included in Rel. 13 and for data and video in the Rel. 14.

In the first phase of 5G system, i.e., in Rel. 15 all the mission-critical services are enhanced. In addition, interworking with other systems such as TETRA will be used so that in the future services could be seamlessly provided to mission critical users with different radio interfaces. The 5G system will include tailored support for different vertical such as railway and maritime operations.

QoS control in 3GPP networks ensures that users with higher priority classification are given access to appropriate operator resources and receive sufficient service quality even in congestion situations. Policy-based management i.e., applying operator-defined rules for resource allocation and resource use, plays a fundamental role in QoS control and traffic prioritization [7], [12]. QoS in 3GPP networks is based on the concept of bearers, which is a transmission path

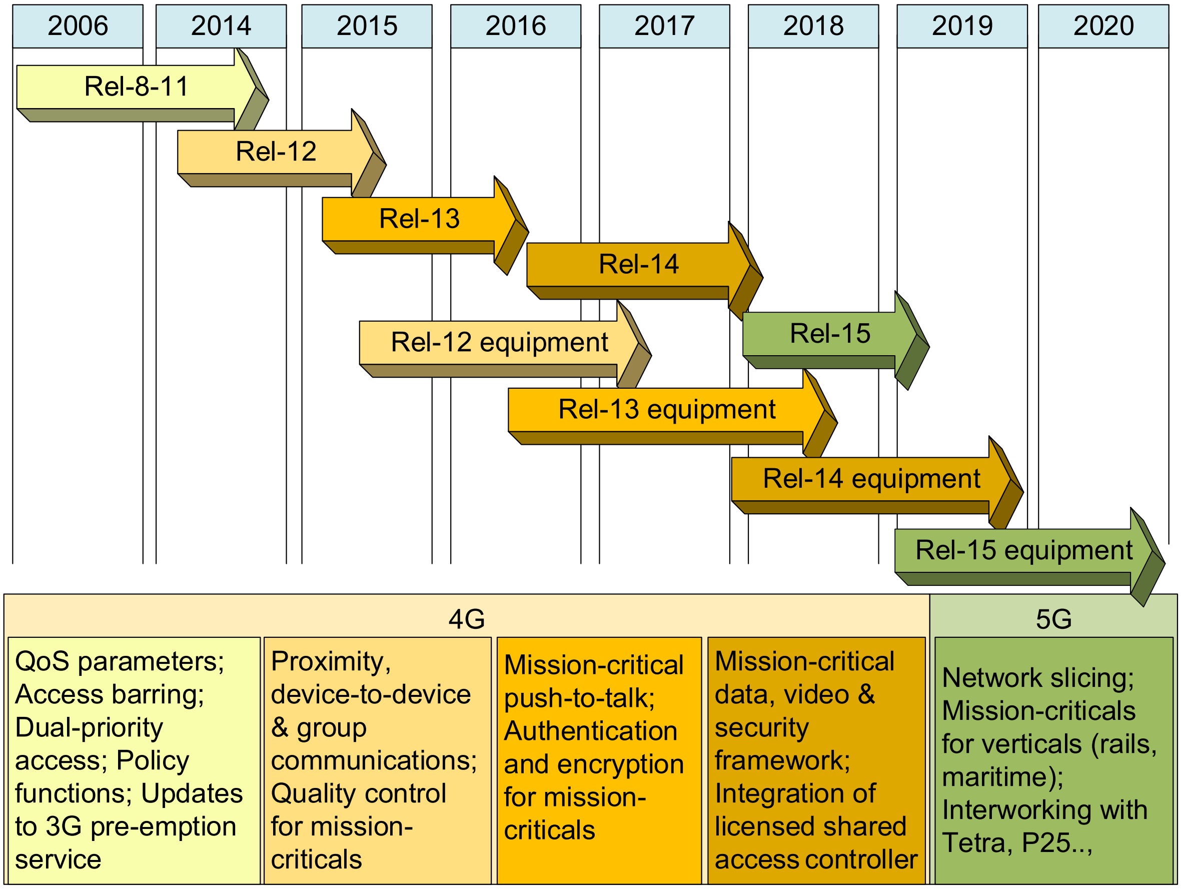

2006
2014
2015
2016
2017
2018
2019
2020
Rel-8-11
Rel-12
Rel-13
Rel-14
Rel-12 equipment
Rel-15
Rel-13 equipment
Rel-14 equipment
Rel-15 equipment
4G
5G
QoS parameters; Access barring; Dual-priority access; Policy functions; Updates to 3G pre-emption service
Proximity, device-to-device & group communications; Quality control for mission-criticals
Mission-critical push-to-talk; Authentication and encryption for mission-criticals
Mission-critical data, video & security framework; Integration of licensed shared access controller
Network slicing; Mission-criticals for verticals (rails, maritime); Interworking with Tetra, P25..,

FIGURE 1. Mission critical services and QoS in 3GPP standardization.

through the infrastructure and radio interface with a defined capacity, latency, and packet loss. Bearers are assigned for different applications according to applications' QoS class identifiers (QCI) as depicted in Table 1. For each QCI class a resource type that is either guaranteed bit rate (GBR) or non-guaranteed bit rate (NGBR) is given. Every QCI is associated with a priority level. Mission-critical services such as MCPTT have the highest priority in the defined QCI classes.

Priority level 5 is the highest priority level and it is assigned for MC-PTT signaling. Numerical requirements for delay and packet loss rate are shown in the table for each QCI.

Enforcement of QoS policies is based on several mechanisms. Creation of dedicated bearers and dynamic QoS control is enabled with the policy and charging rules function (PCRF) [15]. Access Class Barring (ACB) is mainly used for congestion control of a specific area or a specific base station or cell in two ways: 1) Access class control method enables mobile terminals to determine whether they should send the connection request to base station; 2) Connection reject method enables base station to accept or reject connection requests. Mobile network operators may use both methods depending on the network congestion and traffic conditions. Every data bearer must have QCI and allocation and retention priority (ARP) defined. ARP primarily allows network to decide whether a bearer establishment request can be accepted or rejected. As priority communication needs may arise dynamically, 3GPP has defined also preemption mechanisms that provide means to remove lowest priority users so that higher priority users can start immediately their transmission when accessing the network.

Priority services rely on 3GPP's security architecture [16] to authenticate users and to protect network assets against external threats. To support end-to-end confidentiality and integrity protection, 3GPP has also defined identity and key management mechanisms for mission critical applications [17]. Further, mobile network operators typically apply domain and vendor specific security firewalling and monitoring solutions to preact and react against disturbances and attacks affecting the availability of critical services.

B. SOFTWARIZATION AND NETWORK SLICING

Promising enablers in 5G networks, affecting a lot both to architectural choices and mechanisms, include multi-access edge computing (MEC), software-defined networks in (SDN), network function virtualization (NFV), cloud computing and cloud networking. They enable deployment and runtime of network functions as software only make networks dynamic programmable through centralized control

TABLE 1. QoS class identifiers for different applications [11].

Class	Resource Type	Priority	Delay Budget	Error Loss	Example Services
1	GBR	20	100 ms	10^{-2}	Conversational voice
2	GBR	40	150 ms	10^{-3}	Conversational (streaming) video
3	GBR	30	50 ms	10^{-3}	Real time gaming
4	GBR	50	300 ms	10^{-6}	Non-Conversational Video
65	GBR	7	75 ms	10^{-2}	Mission Critical user plane Push To Talk voice
66	GBR	20	100 ms	10^{-2}	Non-Mission-Critical user plane Push To Talk
75	GBR	25	50 ms	10^{-2}	Vehicle to everything
5	non-GBR	10	100 ms	10^{-6}	IMS signaling
6	non-GBR	60	300 ms	10^{-6}	Buffered video, TCP-based (www, email…)
7	non-GBR	70	100 ms	10^{-3}	Voice, streaming video, gaming
8	non-GBR	80	300 ms	10^{-6}	Buffered video, TCP-based (www, email…)
9	non-GBR	90	300 ms	10^{-6}	Buffered video, TCP-based (www, email…)
69	non-GBR	5	60 ms	10^{-6}	Mission Critical delay sensitive signalling
70	non-GBR	55	200 ms	10^{-6}	Mission Critical Data
79	non-GBR	65	50 ms	10^{-2}	Vehicle to everything
80	non-GBR	66	10 ms	10^{-6}	Low latency eMBB, augmented reality
81	Delay Critical GBR	11	5 ms	10^{-5}	Remote control
82	Delay Critical GBR	12	10 ms	10^{-6}	Intelligent transport systems
83	Delay Critical GBR	13	20 ms	10^{-5}	Intelligent transport systems
84	Delay Critical GBR	19	10 ms	10^{-4}	Discrete automation
85	Delay Critical GBR	22	10 ms	10^{-4}	Discrete automation

points [2], [15]. These technologies are the main drivers for enabling customized 5G network infrastructures for specific applications and services and for seamless integration of different heterogeneous networks. NFV and SDN can make network slicing (NS) a reality, allowing operators to customize networks according to various requirements of mobile services, thus leading to a more cost-effective way to build dedicated networks.

3GPP defines a network slice as a complete logical network, which provides telecommunication services and network capabilities [13]. Distinct Radio Access Network (RAN) network slices and core network slices will interwork with each other to provide mobile connectivity. A device may access multiple network slices simultaneously through a single RAN. The realization of NS faces significant challenges in cellular systems [14], [18]. There are great difficulties in organizing mobility and authentication management in the control plane as well as session and charging management in the user plane. Network slices are isolated from each other to prevent control plane congestion on one slice to affect the control plane of other slices, and to improve security.

The simplest way to implement NS would be to create static slices for certain purposes. However, in critical communications the demands are dynamic and thus, dynamic network slicing is a preferred way of operation.[1] The following phases describe the network slice lifecycle [13]: 1) Preparation phase, 2) Instantiation, Configuration and Activation phase, 3) Run-time phase, 4) Decommissioning phase. Run-time monitoring and controls enable dynamic management the functionality and resources of slice. Network slices can be dedicated or shared among multiple applications or users [18]. The slices may have dedicated or common network functions. Dedicated functions facilitate customization of slices and assure strong isolation between different applications. A fixed splitting of common functions and resources simplifies the network management and operation but may lead to inefficient network utilization.

C. SPECTRUM SHARING AND MULTI-RADIO ACCESS TECHNOLOGIES (RATs)

Spectrum sharing approaches support critical communications by enabling use of more spectrum resources [19]. Typically, critical communications are the primary user in the sharing arrangements. Allowing commercial and other

[1] However, an always available dedicated slice in commercial networks for critical communication purposes could be very useful. The drawback for this approach is resource consumption since the slice might be underused majority of time.

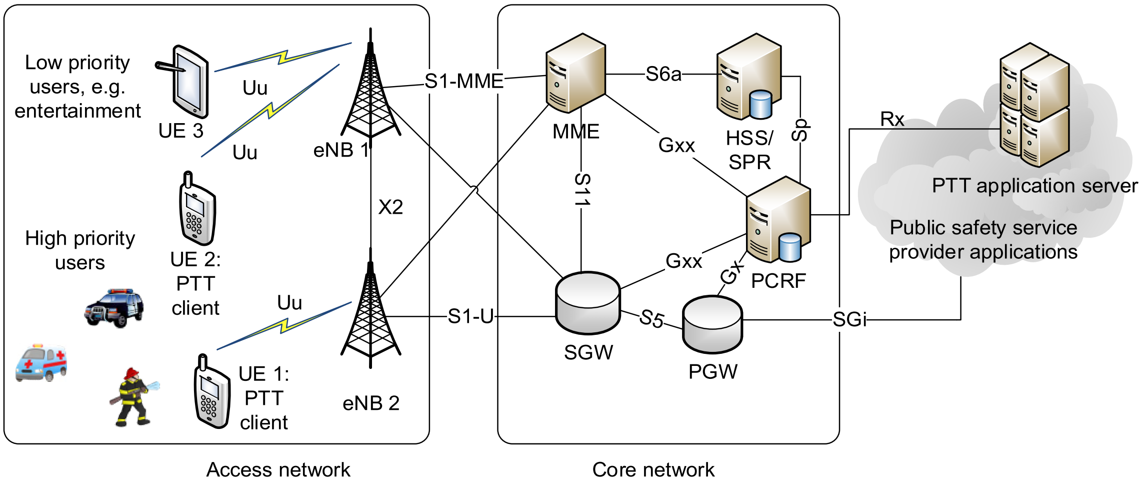


FIGURE 2. Test network architecture for priority communications.

spectrum users on the critical communications bands can reduce the risk of being migrated to another band, even if the use of the radio spectrum is rare. Organizations utilizing critical communications may also benefit from secondary access to commercial spectrum bands, for example for training purposes. Spectrum sharing with a primary status between different critical communications systems could also be a possible scenario in the Public Protection and Disaster Recovery (PPDR) missions. Distributed LSA is a promising approach for rapidly deployable networks. The basic principle of a spectrum database approach is that the database controls when the secondary user can access the spectrum and such helps to avoid harmful interference to protected spectrum users. Under the LSA approach, the incumbent operators are required to provide information about their spectrum use over the area of interest to the database. Based on that information, the spectrum database determines explicitly where, when, and which parts of the frequency bands are available for the secondary use. This approach enables interference free spectrum sharing for all and guaranteed QoS for the incumbent networks.

5G is a multi-radio system built upon both new high capacity and low-latency interfaces and convergence of existing radio technologies such as 5G new radio (NR), LTE and WiFi to a ubiquitous radio access network. The wireless access can be obtained with multi-operator 3G/4G/LTE router. The routers can be combined with a high gain directional narrow beam antenna high of the ground when long range communications are required. This setup provides connection in areas where the normal LTE mobile phones do not have coverage. Then, for even more remote environments, satellite broadband connections are available in integrated satellite-terrestrial 5G networks [20]. This multiradio network requires intelligent end-to-end network management where selection of the most appropriate RAT and route to the data is based on the QoS requirements and measurements.

III. CRITICAL COMMUNICATIONS TRIALS

Our practical work has focused on two use cases. First, how to implement critical communication services in the existing mobile operator network using described technological enablers? We focus on push-to-talk application in Trial 1, describing how we have implemented the system in our test network and what are the main components and communication interfaces between those components. Trial 2 focuses on creation of a network in an area where infrastructure is not currently available. The rapidly deployable network (RDN) requires that all the required functionalities such as core network, application servers, and the LSA server for spectrum needs are implemented and built in the area on interest. Finally, collaboration trials between the RDN and the commercial 5G are presented.

A. PRIORITY COMMUNICATIONS OVER MOBILE OPERATORS' NETWORKS

This use case focuses on enabling critical communication in commercial networks by use of QoS management and prioritization mechanisms. We are using dedicated bearers and mission-critical QCI classes for those bearers to prioritize PTT users in the commercial networks. This can be seen as "4G network slicing" that we were able to implement already with existing network components. In the future 5G networks the slicing will be based on software-defined network switches and network function virtualization mechanisms. The proposed "4G network slicing" with dedicated bearers could be implemented in the existing commercial networks already now. Figure 2 describes the implemented trial environment for priority communications. The key building blocks and interfaces of the trial environment are given in the following. The trial architecture is geographically distributed in several locations in Finland. The architecture connects the application server in Helsinki area to the core network in Oulu and can be used to support PTT clients over an access network both in Helsinki and in Oulu. The architecture

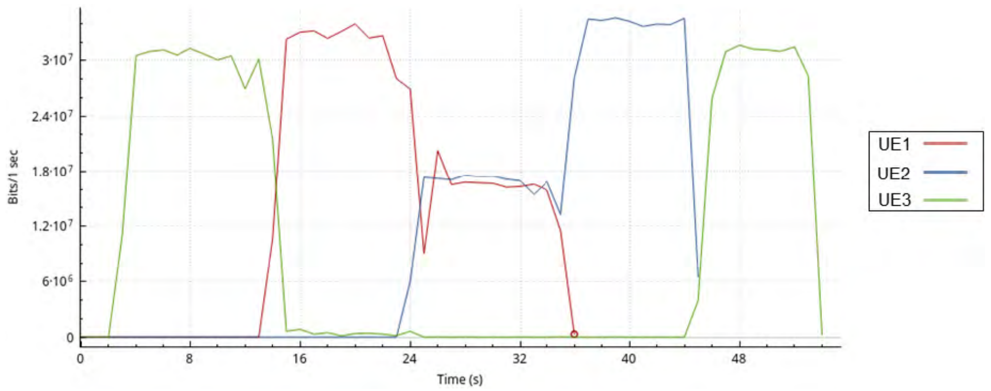


FIGURE 3. **Throughput of different priority users in the trial network.**

enables adding flexibly components and testing technologies in different locations and environments.

1) PTT APPLICATION

One or more PTT clients require priority connection in the commercial network for authority communications, i.e., using pull mode from the end -users' side to open the connection. The PTT client sends service request over the LTE-Advanced network to the PTT application server.

PTT application server provides the group communication and messaging service to the PTT clients. It also interfaces to the narrowband TETRA networks providing seamless interoperability between PTT clients and TETRA radios. The server uses Rx interface to communicate with the PCRF located in the core network and requests priority connection to the PTT clients based on a service request, PTT client user profile, and service profile provisioned in the server.

Core network is implemented with the OpenEPC [21]. The main components regarding the priority communication are given in the figure. A key component is the PCRF that provides QoS of different applications and subscribers. It can also apply security procedures before accepting information from the PTT application server that is under control of the public safety service provider. The PCRF is used in creating a dedicated bearer for the PTT application with a mission critical QCI 65 value. The PCRF allows dynamic creation and management of dedicated bearers, i.e. new bearers can be added on the fly to the network.

Other main component of the core network is the mobility management entity (MME) that is the main signaling node in the evolved packet core (EPC), taking care of e.g. authentication and handover signaling between different networks. MME connects to the base station, evolved node B (eNB), through the S1-MME interface and connects to the serving gateway (SGW) through the S11 interface. MME works with the home subscribing server (HSS) and the RAN to decide the appropriate radio resource management strategy that can be UE-specific. The HSS includes user identification and addressing data as well as subscriber profile repository (SPR) where user-subscribed QoS classes are stored. The PCRF is connected to the SGW, packet data network (PDN) gateway (PGW), HSS and MME using Diameter based connectors Gxx, Gx, and Sp. The PDN Gateway provides connectivity from the UE to external packet data networks and public safety applications over the SGi interface. The S5 reference point provides tunneling and management between the SGW and the PGW.

2) ACCESS NETWORK

The used RAN in our test network is located in office environment. It includes 3GPP base stations that are connected to each other using X2 interface. The base stations and UEs are commercially available 3GPP compliant equipment that are constantly updated with the latest software releases.

We have tested creation of dedicated bearers and use of them in a congested network, especially the mission-critical applications. The results shown in Figure 3 were achieved with our trial network using a pico base station and three UEs with different QCI class bearers. First, there is a 30 Mbits/s QCI9 default bearer data transmission to UE3 (green line) going on, this user being the only one over the air. The transmission stops after data transmission to the user UE1 (red line) with a high priority dedicated bearer QCI5 starts. The result shows that the priority user reserves the whole band for its use. After another critical user UE2 (blue line) with the same priority and dedicated bearers QCI5 starts transmission UE1 and UE2 divide the bandwidth equally while they are receiving data simultaneously. Traffic to UE3 default bearer continues after UE1 and UE2 have stopped. The way to use the bandwidth can be affected by policy management in the core network. For example, in our case the priority users may request total bandwidth for their use but there could be also a policy set to leave e.g. 20 % of the bandwidth available for commercial users. This could be still limited so that video transmission is not allowed but e.g. speech and text is fine.

This trial shows how critical communication users can receive a high quality service in a commercial network when needed. The trial scenario enabled us to evaluate the maturity levels of available commercial products. For instance, we noticed that the support for mission-critical quality classes was inadequate in the base station and consequently we utilized lower quality classes with identical behavior. We were also able to advance development of the EPC to support better GBR bearers.

B. RAPIDLY DEPLOYABLE NETWORKS

This use case focuses on building a rapidly deployable network (RDN) for public safety applications for scenarios where the commercial network is fully or partially unavailable. This could be caused by some catastrophic situation such as an earthquake or there might be a need to create a dedicated network in a remote location for search and rescue, as an example. The rapidly deployable network provides the basic services such as voice and data transfer for the users as well as multiple ways to access the network and its services including local LTE, WiFi and access via a commercial mobile network, if available. Here, drones, sensors, and cameras can be connected to the network wirelessly or wired. Figure 4 describes the rapidly deployable network concept including the LSA functionality that is used for spectrum management [4]. The RDN can utilize towable lifts or crane cars to allow the rapid deployment and sufficient radio coverage without fixed tower assemblies. The test environment is Finnish forest.

The lite-EPCs provide LTE access points to the tactical network and emulate the EPC functionalities of a commercial LTE network. The lite-EPC is a server program running inside a small and portable computer. Compared with the complete commercial EPCs, this is a distributed and a lighter solution to enable stand-alone LTE operation for the selected users.

The tactical network offers the backhaul for the public safety operator network and consists of SDR-routers [22], which support both wireless and wired connections. These routers are able to select and use the best possible connection/route available and will re-route the connection automatically, if needed. In addition to tactical connections, a connection to any public and mobile networks can be provided allowing the users connect to, for example, to the internet, or remote users connected to a mobile network to access the tactical network through a secure Mobile virtual private network (VPN) connection. Note, that while in Figure 4 we have two tactical routers, the network is scalable, i.e., the number of the access points and tactical routers can vary. As an example, Figure 5 shows a tactical network trial with four backhaul nodes. We also see a crane car that has all the necessary equipment. The trial included backbone links up to 12 km distances, which provided sufficient connectivity at each location and enabled group communication between LTE handhelds.

The LSA system offers spectrum information for the rapidly deployed LTE network. A secondary spectrum license is sufficient, because this network is a backup network for the commercial network. Here, the incumbent spectrum users reserve the spectrum an agreed time before their transmission. The LSA repository saves this information. The LSA server obtains the latest spectrum information from the repository, which is then valid for the agreed time after the LSA server has had a repository connection. The LSA server acts as a mediator between the LSA repository and the distributed LSA controllers.

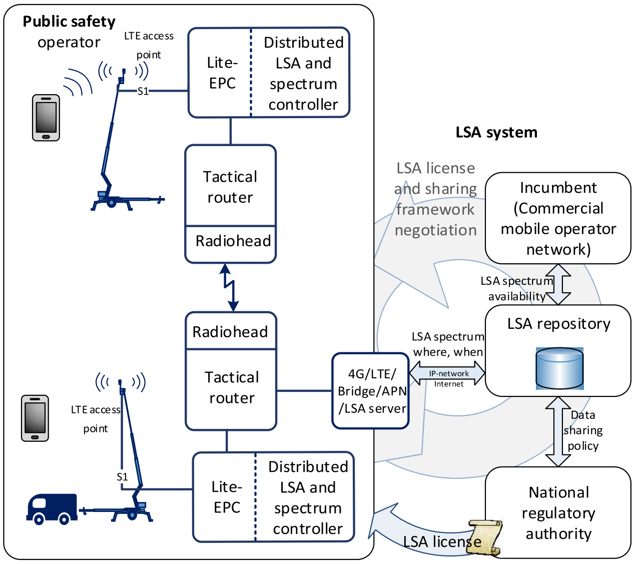

Public safety operator
LTE access point
S1
Lite-EPC
Distributed LSA and spectrum controller
Tactical router
Radiohead
Radiohead
Tactical router
LTE access point
S1
Lite-EPC
Distributed LSA and spectrum controller
4G/LTE/ Bridge/APN /LSA server
LSA system
LSA license and sharing framework negotiation
Incumbent (Commercial mobile operator network)
LSA spectrum availability
LSA repository
LSA spectrum where, when
IP-network
Internet
Data sharing policy
National regulatory authority
LSA license

FIGURE 4. A concept for rapidly deployable public safety network using LSA for spectrum needs.

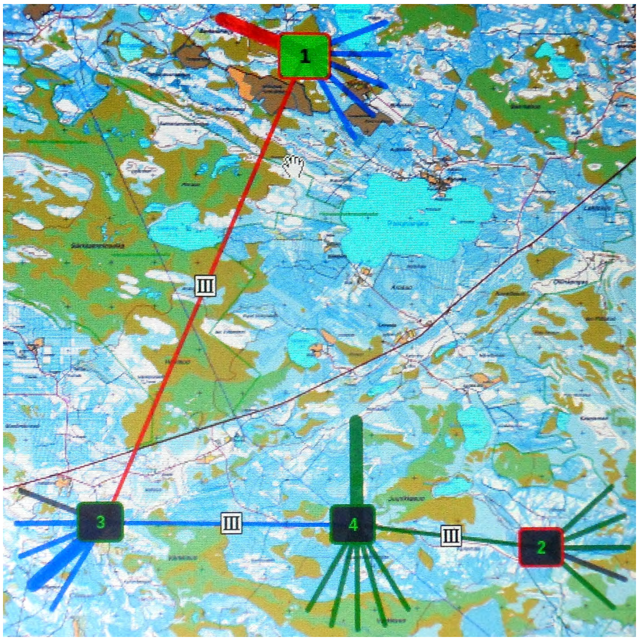


FIGURE 5. An example public safety backhaul network.

The distributed LSA controllers are running on the same computers as the lite-EPCs. The controllers control their own LTE access point spectrum use, but decide the spectrum sharing together. They synchronize with each other and obtain spectrum information from the LSA repository and from the sensing system. This information enables to control the

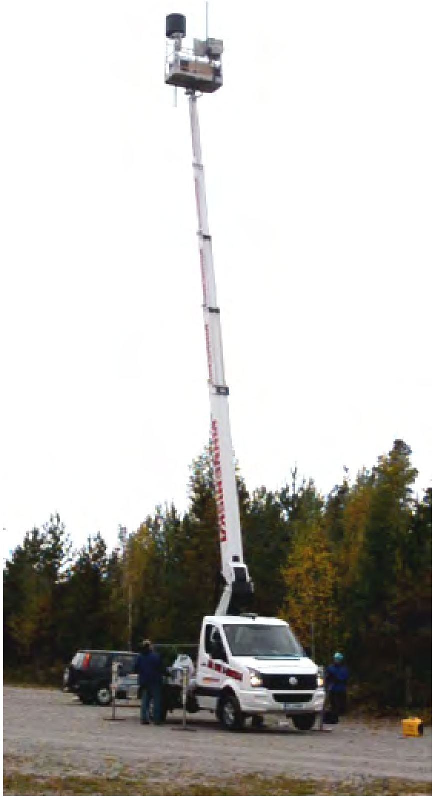


FIGURE 6. Rapid network deployment with crane cars.

access point for locking/unlocking cells, changing frequency, and/or changing transmission power. The controller is a small and lightweight software that provides rapid base station control. It is easy to port to any computer and thus easy to utilize in mobile scenarios. The performed trials verified the LSA functionality for this type of rapidly deployed network operation.

The sensing offers additional spectrum information for the rapidly deployed network. It is used if the LSA information is uncertain or invalid due to commercial network breakage; the sensing is used both to verify the spectrum information validity and to select the channel with the least interference when the LSA system fails. In our trials, a spectrum analyzer was used remotely to calculate the channel energy of downlink LTE Band 7. Initial tests suggest that sensing the LTE channel free with an energy detector and by using antenna gain 6 dBi and antenna height 30 meters can guarantee sufficient separation distance to the incumbent macro base station in remote areas. We plan to use the radioheads for sensing.

To understand the dynamic spectrum use capability of our trial system, we performed measurements with the distributed LSA setup while evacuating the frequency and starting the transmission in a new band. The evacuation process aims to protect the incumbent spectrum users' rights by evacuating LSA band when the band request from the incumbent is received. The restart frequency process on the other hand defines the necessary time for a base station to start their service in a new LSA band from the time the base station received a new frequency band information from the LSA repository. Thus, we measured time consumption in both processes in order to show the efficiency of own new LSA concept in this experiment.

The measurement begins at the moment the LTE base station received the information from the LSA repository that the current frequency is not available anymore. Following steps are then performed: 1) At the base station, LSA controller executes LOCK procedure to turn off the air interface at the current frequency. 2) After that, the LSA controller inquires new information about available spectrum from the LSA repository and synchronizes the newest update with other LSA controllers in the network. 3) Then, the controller uses new information to find available frequency and executes SET_FREQUENCY procedure to reconfigure the base station to operate in a new spectrum band. 4) Finally controller executes UNLOCK procedure to turn the air interface of the base station back on to continue transmission on the configured frequency.

TABLE 2. Reconfiguration times in the rapidly deployable network trial.

System Commands	Time duration	Standard Deviation
LOCK - Turn off air interface at base station	8.78 s	0.39 s
SET_FREQUENCY - Change LSA frequency from one to another	7.97 s	0.37 s
UNLOCK - Turn on air interface at base station	8.97 s	0.37 s

The results are shown in Table 2. Our previous measurements that have used large network management systems [6] instead of our self-developed controllers have shown reconfiguration times in the order of minutes. Now we achieved much better results for a rapidly deployable network where we are only controlling the small network with dedicated controller functionality. The achieved times show that current band can be evacuated in less than 10 seconds during LOCK command. The restart frequency process combining the SET FREQUENCY and UNLOCK times takes approximately 17 seconds.

C. COLLABORATION BETWEEN COMMERCIAL AND RAPIDLY DEPLOYABLE PUBLIC SAFETY NETWORKS

In addition to the conducted main trials and achieved results, we have tested the RDN concept collaboratively with commercial networks. The tests have been conducted during public safety operations so that the personnel has used more than 20 end user equipment that can access both RDN and commercial network. The solution has ensured operational safety and priority communications in commercial network. Based on the operational tests following requirements and recommendations can be given.

The collaboration between commercial and public safety networks can be enabled with a political decision.

Alternatively, the commercial operators can have monetary incentives to offer tailored and complete solutions for public safety together with the rapidly deployable network equipment providers. The public safety needs interconnection and requires a similar operation of the applications and services in every network. The public safety can utilize common applications in each type of network in the following fashion.

1) COMMON SERVICES AT THE INTERNET

The public safety offers and uses its application servers and data bases over the internet. The services can be hidden services in the tactical networks and alternatively offered in any other private or public networks. These applications are reachable from any network having an internet connection. The connection can be secured for example with a VPN. Normally, the public safety can gain wireless internet with single or multi-radio access technologies and in planned operations, public safety can use locally available commercial hardwired networks.

2) COMMON SERVICES AT THE COMMERCIAL NETWORK EPC

The commercial network configures the public safety base stations at the tactical networks to its EPC. Likewise, the public safety configures its base stations to use the commercial EPC. The main benefits of this scenario are the latest commercial application services and the interoperability with older mobile systems.

The public safety can connect to the EPC via a VPN using an internet connection or via commercial network slices. Then, when there is no connection, the public safety can utilize a local EPC solution, which can support the services that the public safety has noticed to be beneficial.

Note that the public safety can also act as a mobile virtual network operator inside the commercial networks. Furthermore, the public safety can operate a full commercial EPC service itself. Here, the public safety obtains more control over the network it uses. Then, it can have roaming agreements for the communication with the commercial networks. With roaming, the public safety can allow commercial users to use their base stations. This can be critical in some operational scenarios, where the commercial network is down and the commercial users do not have an outside world connection.

3) COMMON COMMERCIAL NETWORK SWITCHES AND ROUTERS

The commercial networks can enable the backbone of the commercial networks for public safety use. Here, any of the connected networks can offer the applications, which are accessible to critical users via routing. Rapidly deployed public safety networks are connected to commercial networks using interface devices, which are secure traffic relays. The public safety can have multiple interface devices in different parts of the commercial internet protocol (IP) networks. They can be connected to each other with methods like a virtual local area network (VLAN) or a virtual private local area network service (VPLS). Then, they can communicate together with their desired method. Note that these interface setups can be dynamically set up or pre-defined permanent installations.

The interface devices can also give tactical network access to the LTE users outside of the public safety operator network. Here, the interface device has been defined a known access point name (APN) for critical data. Moreover, the critical LTE user equipment request the same APN in their critical applications. Note that the LTE has support for multiple packet data networks [23]. Thus, the non-critical applications can route their data to elsewhere.

IV. FUTURE RESEARCH TOPICS

A. DYNAMIC NETWORK SLICING

Network slicing can improve many public safety services by decreasing delays. For example, QCIs are currently requested on per session basis potentially slowing down overall call control setup. Already a static network slice enables reserving the resources ahead of time in a coarse-grained manner instead of per session. Since static slicing consumes resources, dynamic slicing techniques will be needed in future networks to quickly create, adapt, and manage slices according to the needs of users and applications. Dynamic slicing provides also robustness against challenging network conditions, as application specific network slices can be more easily isolated from other applications and adapted e.g. in the case of emerging cyber security attacks or hardware failures. It is an open research challenge how to do these in practice.

Softwarization and virtualization of the network resources are key enablers for the dynamicity [24]. One of the core challenges currently is to identify or develop a set of technologies suitable to implement the infrastructure over which network slicing will be built, without requiring major rework of the 3GPP specifications. In the longer term, trials of dynamic network slices for priority communications between rapidly deployed networks is a potential topic to be tested in our trial environment. Traditional QoS and prioritization mechanisms will be used in network slices to prevent congestions and emerging possibility to dynamically adjust e.g., the size of the slice will further improve the situation. Open research challenges include how to apply machine learning based control strategies in dynamic adjustments.

B. REMOTE OPERATIONS

Majority of work conducted with prioritized public safety communications has been done in densely populated areas and due to congestion probabilities it will remain as the most important environment also in the future. However, prioritized PTT applications in commercial and in rapidly deployable networks in remote locations is a topic that requires more work to be done. How to create rapidly deployable networks with D2D connections and slices in those areas? How to efficiently use multi-RAT networks, combining satellite systems, long-range digital communications and broadband solutions in the remote and isolated environments to different services?

QoS-aware radio and network resource management schemes will be required. Partly this work is done by developing solutions for different mobile platforms such as cars [20], [25] ships [20], unmanned aerial vehicles [26] and trains [27].

V. CONCLUSIONS

This paper discusses how critical communications can be carried out in a mobile operators' network and how a dedicated rapidly deployable network can be implemented to support public safety needs. The most important enabling techniques such as prioritization, QoS management, SDN, network slicing, end-to-end security, and spectrum sharing are discussed and their use in practical trials described. Architectures of trial networks used for priority communications and rapidly deployable operations are given. The results shown in each trial indicate that the developed mechanisms in prioritization and spectrum sharing are good enablers for future public safety users. The paper defines promising future research questions, especially more trials are needed to validate technologies.

REFERENCES

[1] A. Kumbhar, F. Koohifar, I. Guvenic, and B. Mueller, "A survey on legacy and emerging technologies for public safety communications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 97–124, 1st Quart., 2017.

[2] C. Sexton, N. J. Kaminski, J. M. Marquez-Barja, N. Marchetti, and L. A. DaSilva, "5G: adaptable networks enabled by versatile radio access technologies," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 688–720, 2nd Quart., 2017.

[3] M. Höyhtyä *et al.*, "Spectrum occupancy measurements: A survey and use of interference maps," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2386–2414, 4th Quart., 2016.

[4] R. H. Tehrani, S. Vahid, D. Triantafyllopoulou, H. Lee, and K. Moessner, "Licensed spectrum sharing schemes for mobile operators: A survey and outlook," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2591–2623, 4th Quart., 2016.

[5] O. Ergul, G. A. Shah, B. Canberk, and O. B. Akan, "Adaptive and cognitive communication architecture for next-generation PPDR systems," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 92–100, Apr. 2016.

[6] M. Palola *et al.*, "Field trial of the 3.5 GHz citizens broadband radio ervice governed by a spectrum access system (SAS)," in *Proc. DySPAN*, Mar. 2017, pp. 1–9.

[7] *Quality of Service (QoS) Concept and Architecture*, document TS 23.107 V15.0, 3GPP, 2018

[8] *LTE Device to Device Proximity Services*, document TS 36.877 V12.0, 3GPP, 2015.

[9] *Group Communication System Enablers for LTE*, document TS 23.468 V15.0, 3GPP, 2017

[10] M. Alasti, B. Neekzad, J. Hui, and R. Vannithamby, "Quality of service in WiMAX and LTE networks [topics in wireless communications]," *IEEE Commun. Mag.*, vol. 48, no. 5, pp. 104–111, May 2010.

[11] *System Architecture for the 5G System*, document TS 23.501 V15.2, 3GPP, 2018.

[12] *Technical Specification Group Core Network and Terminals; Policy and Charging Control Over Rx Reference Point (Release 14)*, document TS 29.214 V14.3.0, 3GPP, Mar. 2017.

[13] *Study on Management and Orchestration of Network Slicing for Next Generation Network (Release 15)*, document TR 28.801 V1.2.0, 3GPP, May 2017.

[14] X. Zhou, R. Li, T. Chen, and H. Zhang, "Network slicing as a service: enabling enterprises' own software-defined cellular networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 146–153, Jul. 2016.

[15] H. Nam, D. Calin, and H. Schulzrinne, "Intelligent content delivery over wireless via SDN," in Proc. IEEE WCNC, Mar. 2015, pp. 2185–2190.

[16] *Security Architecture and Procedures for 5G System (Release 15)*, document TS 33.501, 3GPP, 2018.

[17] *Security of the Mission Critical Service*, document TS 33.180, 3GPP, 2018.

[18] R. Peter *et al.*, "Network slicing to enable scalability and flexibility in 5G mobile networks," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 72–79, May 2017.

[19] M. M. Sohul, M. Yao, X. Ma, E. Y. Imana, V. Marojevic, and, J. H. Reed, "Next generation public safety networks: A spectrum sharing approach," *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 30–36, Mar. 2016.

[20] M. Höyhtyä, T. Ojanperä, J. M¨akelä, S. Ruponen, and P. Järvensivu, "Integrated 5G satellite-terrestrial systems: Use cases for road safety and autonomous ships," in *Proc. KaConf*, Oct. 2017, pp. 1–9.

[21] M. Corici, F. Gouveia, T. Magedanz, and D. Vingarzan, "OpenEPC: A technical infrastructure for early prototyping of NGMN testbeds," in *Proc. TridentCom*, May 2010, pp. 166–175.

[22] Elektrobit, "Enhancing the link network performance with EB tactical wireless IP network (TAC WIN)," EB Defense Newsletter, Bittium, Oulu, Finland, Dec. 2014. [Online]. Available: https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/enhancing_the_link_network_performance_with_eb_tactical_wireless_ip_network_tac_win.html

[23] *LTE; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access*, document TS 123 401 V14.6.0, ETSI, Jan 2018.

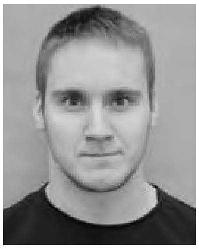
[24] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[25] W. Sun, D. Yuan, E. G. Ström, and F. Brännström, "Cluster-based radio resource management for D2D-supported safety-critical V2X communications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2756–2769, Apr. 2016.

[26] A. Merwaday and I. Guvenic, "UAV assisted heterogeneous networks for public safety communications," in *Proc. WCNCW*, Mar. 2015, pp. 329–334.

[27] A. Sniady, J. Soler, M. Kassab, and M. Berbineau, "Ensuring long-term data integrity: ETCS data integrity requirements can be fulfilled even under unfavorable conditions with the proper LTE mechanisms," *IEEE Veh. Technol. Mag.*, vol. 11, no. 2, pp. 60–70, Jun. 2016.

MARKO HÖYHTYÄ (S'07–M'11–SM'15) received the M.Sc. (Tech.) degree in information engineering and the D.Sc. (Tech.) degree in telecommunication engineering from the University of Oulu. Since 2005, he has been with the VTT Technical Research Centre of Finland, where he is currently a Team Leader with the Autonomous Systems Connectivity team. From 2007 to 2008, he was a Visiting Research Scientist with the Berkeley Wireless Research Center, CA, USA. He is also an Adjunct Professor with the University of Oulu. His research interests include critical communications, hybrid satellite-terrestrial connectivity, spectrum sharing, and autonomous systems. He is a Steering Group Member of Research Alliance for Autonomous Systems. He has received an Excellent Paper Award in the IEEE ICTC 2017 Conference for his work on autonomous ship connectivity.



KALLE LÄHETKANGAS (S'11) received the B.Sc. (Tech.) and M.Sc. (Tech.) degrees in electrical engineering from the University of Oulu, Finland, in 2010 and 2011, respectively, where he is currently pursuing the Dr.Sc. (Tech.) degree. In 2010, he joined the Centre for Wireless Communications, University of Oulu. His research interests include optimization, cross-layer design, critical communications, spectrum sharing, and system development in wireless communication networks.

JANI SUOMALAINEN received the M.Sc. (Tech.) degree in information technology from the Lappeenranta University of Technology and the Lic.Sc. (Tech.) degree in telecommunications software from Aalto University. Since 2000, he has been with the VTT Technical Research Centre of Finland Ltd., where he is currently a Senior Scientist. He is specialized on network and information security and has been involved in these topics in various international joint projects and customer projects. His research interests include adaptive security solutions for dynamic and heterogeneous network environments. Recently, he has been involved in both European and Finnish cooperation projects developing secure network slicing and monitoring solutions and testbeds for emerging mobile networks.

MIKA HOPPARI received the M.Sc. (Tech.) degree in information engineering in telecommunication engineering from the University of Oulu. Since 2006, he has been with the VTT Technical Research Centre of Finland Ltd., where he is currently a Research Scientist with the 5G and Beyond Network Team. He is especially interested in hands on research.

KAISA KUJANPÄÄ received the M.Sc. degree in information processing science from the University of Oulu in 2007. Since 2005, she has been working in various international research projects related to mobile services, network simulations, sensor networks, vehicular communication, and network resource management. She is currently a Research Scientist with the VTT Technical Research Centre of Finland Ltd. Her recent research work has focused on critical communications and QoS management.

KIEN TRUNG NGO received the B.Sc. degree in telecommunication engineering from the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam. He is currently pursuing the M.Sc. degree in wireless communication engineering with the University of Oulu, Finland. He is working at the VTT Technical Research Centre of Finland Ltd., under the Autonomous Systems Connectivity Team. His research interests include autonomous systems, spectrum sharing, critical communications, and energy harvesting.

TERO KIPPOLA received the B.Eng. degree in telecommunication from the Centria University of Applied Sciences. Since 2006, he has been with the Centria Research and Development Laboratory, Centria University of Applied Sciences, where he is currently a R&D Specialist with the Future Networks Research Group. His research focus has been in the areas of active antenna system and shared spectrum access development in particularly LTE base station, active antenna and core network functionalities and parameters, mobile communication network planning, and parametrization. His current research focus is in 5G and beyond 5G technologies.

MARJO HEIKKILÄ received the B.Sc. (Tech.) and M.Sc. degrees in information technology from the University of Jyväskylä in 1999 and 2013, respectively. She has 20 years of experience of various research and development projects developing wireless communication systems and applications. She has worked as RF and EMC Type Approval Engineer with Nokia Networks. Since 2004, she has been with the Centria University of Applied Sciences, where she is currently a Research and Development Manager. She is also working in 5G Test Network and Critical Operations Over 5G Networks Projects as Project Manager.

HARRI POSTI received the M.Sc. (Tech.) and D.Sc. (Tech.) degrees in telecommunication engineering from the University of Oulu. From 1990 to 2009, he worked in various positions in Nokia Corporation. From 2010 to 2012, he participated in the regional renewal process, when Nokia Mobile Phones discontinued its operations. Since 2012, he has been the Research Director with the Centre for Wireless Communication, University of Oulu.

JARI MÄKI received the M.Sc. (Tech.) degree in electrical engineering from the Tampere University Technology. From 1990 to 2005, he worked in various positions in Nokia Corporation. Since 2005, he has been a Senior Project Manager with Airbus Defence and Space Oy.

TAPIO SAVUNEN received the M.Sc. (Tech.) degree in communications engineering from the Helsinki University of Technology. He is currently pursuing the Ph.D. degree with Aalto University. He was the Director and Strategic Marketing with Airbus Defence and Space in the domain of critical communications. His research interests include critical communications, mobile operators, and information security. Many international patents have been granted to him in the domain of mobile communications. He is an Active Member of The Critical Communications Association.

ARI HULKKONEN received the M.Sc. degree in telecommunications with the University of Oulu, Finland. From 2002 to 2008, he was leading Elektrobit's Wireless Communications Research with the main focus in wireless broadband access with the software-defined-radio as the key implementation technology, until the research organization was integrated to business units. He is currently a Research and Technology Manager with Bittium Wireless Ltd., (former Elektrobit) with the main responsibility to coordinate the technology development related to tactical and special communications in close collaboration with the key customers and partners. His research interests comprise techniques aiming at higher data rates and link performance, improved combat sustainability, and security. The applications he has worked with cover a broad range of special cases from underground mines to satellite communications, tactical communications, public safety applications, and many others.

HEIKKI KOKKINEN received the master's degree in electronics and the Licentiate degree in telecommunications and industrial economics from the Helsinki University of Technology in 1993 and 1997, respectively, the Ph.D. degree in computer science from Aalto University in 2011, and an Academic Entrepreneur degree from the School of Business, Aalto University, Espoo, Finland, in 2013. He is currently the Founder and the Chief Executive Officer of Fairspectrum Oy, Espoo. His research interests include the marketing, research and development, financing, system integration, piloting, and deploying of wireless access networks.

• • •