Cellular-enabled Wearables in Public Safety Networks: State of the Art and Performance Evaluation

Salwa Saafi[1,2], Jiri Hosek[1], and Aneta Kolackova[1]
[1]Department of Telecommunications, Brno University of Technology, Brno, Czech Republic
[2]Unit of Electrical Engineering, Tampere University, Tampere, Finland
Email: saafi@feec.vutbr.cz

***Abstract*—With the aim of offering services and products that ensure the safety of people and properties, public safety organizations are responsible for providing the first responders, i.e., police officers, firefighters, and emergency medical service workers, with devices and communication systems that help them exchange time-sensitive and critical information. To address the mission-critical requirements and to target new broadband public safety applications, these organizations started migrating from traditional land mobile radio towards cellular communication systems with the consideration of a new set of deployed devices, such as wearables. In this paper, we first provide a state of the art overview of the features that are introduced by the 3rd Generation Partnership Project (3GPP) and that can be used for public safety services. Second, we discuss the role of wearable devices, more precisely cellular-enabled wearables, in creating several new use cases as part of the concept of the Internet of Life Saving Things. Finally, we conduct a performance evaluation of a mission-critical service using cellular-enabled wearables, specifically a mission-critical push-to-talk (MCPTT) application using LTE Cat-M2-enabled smartwatches. In this evaluation, we examine the impact of different parameters related to the wearable device capabilities and the MCPTT call scenarios on the key performance indicator defined by 3GPP for this type of applications, which is the MCPTT access time.**

***Index Terms*—Public safety, Cellular connectivity, Wearables, Internet of Life Saving Things**

I. Cellular Public Safety Networks

A. Public Safety from LMR to LTE Networks

To offer delay-sensitive, reliable, and secure services, public safety networks utilize dedicated communication systems based on land mobile radio (LMR) technologies including terrestrial trunked radio (TETRA), TETRA for police (TETRAPOL), and project 25 (P25) of the association of public safety communications officials [1]. The main services provided by these networks to the public safety users are narrow-band voice-centric services, such as group and priority calls with push-to-talk (PTT) functionalities. However, to further improve the safety of both first responders and citizens, public safety operations are expected to leap to the next levels of efficiency by applying new applications utilizing broadband data communications [2].

As a result, the inability of the traditionally used LMR systems to support modern data applications makes the migration towards standards that support the requirements of broadband services evident [3]. Having mature, multi-vendor, and multi-service infrastructures, commercial cellular networks are considered to be an alternative for LMR systems [4]. Deployment cost optimization and public safety service expansion are the main reasons that are considered by the critical communications association (TCCA) to select the long-term evolution (LTE) technology to be the basis for future public safety implementations [4].

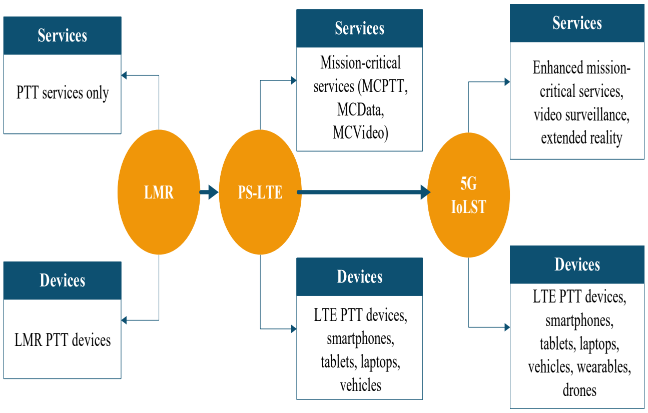
Services
PTT services only
Devices
LMR PTT devices
LMR
PS-LTE
Services
Mission-critical services (MCPTT, MCData, MCVideo)
Devices
LTE PTT devices, smartphones, tablets, laptops, vehicles
5G IoLST
Services
Enhanced mission-critical services, video surveillance, extended reality
Devices
LTE PTT devices, smartphones, tablets, laptops, vehicles, wearables, drones

Fig. 1. Evolution of public safety-related services and devices

The evolution of public safety technologies was also aligned with certain modifications that mainly affected the used devices and offered services in public safety networks as illustrated in Fig. 1. While only voice-based communications are exchanged in LMR networks (i.e., providing PTT services only), public safety LTE (PS-LTE) networks offer a set of mission-critical services that were introduced by the 3rd Generation Partnership Project (3GPP) among its public safety-related standardization items, more precisely in Rel-13. Based on the market demands, mission-critical PTT (MCPTT) was the first major step in the series of mission-critical services. Then, in Rel-14, 3GPP added certain enhancements to the MCPTT standard and enriched its repertoire of standardized public safety applications by introducing mission-critical data (MCData) and mission-critical video (MCVideo) [5].

A general framework for mission-critical services was also provided in the 3GPP Rel-14 to facilitate the standardization of additional services in the upcoming releases. This framework included a common architecture for the support of these services with the definition of two different planes and two functional modes [6]. Concerning the defined planes, the introduced architecture enables an application plane and signalling control plane split for the provisioning of the offered services. Based on the existence of a mission-critical server in the network, two functional modes were fixed in the related 3GPP technical specifications; on-network and off-network modes. In on-network mode, the communications are based on a client/server setup, where the client/server communication is established via the LTE core-network. However, in off-network mode, the communications are only supported by user equipment (UE) devices in a peer-to-peer setup [6]. Fig. 2 shows the difference between the two modes.

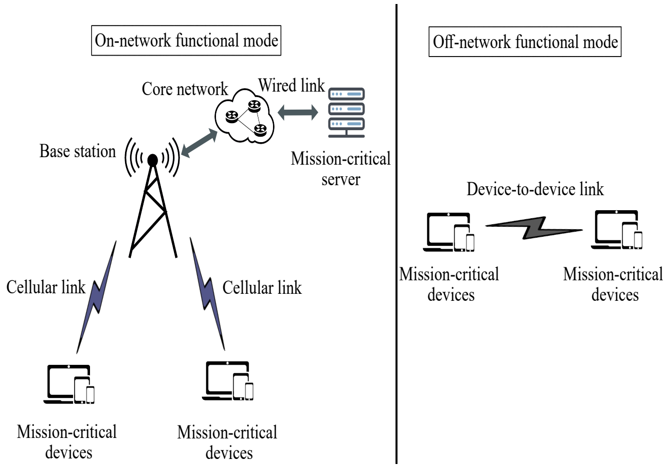

Fig. 2. On-network and off-network functional modes in mission-critical service architecture

B. 5G for Public Safety

The adoption of cellular connectivity solutions in public safety networks implies adapting these networks with the new technologies and features introduced in each of the 3GPP releases. Addressing new verticals and markets including industrial solutions and mission-critical communications, 5G technology is introducing several features that target different requirements and use cases. Among the introduced features, certain functionalities can be deployed in public safety networks to further extend the offered services and deployed devices [4].

With the support of very large number of devices that can communicate with each other, exchange data, and be involved in automated processes, 5G networks are helping address the evolution of the Internet of Things (IoT). Hence, in 5G networks, IoT devices are expected to form significant sources of information for the public safety community [7]. By processing this information and integrating it into the public safety operations, first responders can be more proactive and their tasks can be moved from the investigation to the prevention of accidents and crimes [4].

On top of the mission-critical service enhancements in 3GPP Rel-15 and beyond, 5G networks are expected to support network-based localization with an accuracy of less than 1 m [8]. This boost in the localization accuracy, in comparison with the LMR and LTE technologies, helps provide a reliable and fast emergency response in public safety networks [7]. Therefore, the 3GPP 5G-related content is outlined to include various features and functionalities that can improve the services offered by public safety networks. However, these benefits are dependant on the implementation choices made by the equipment providers [4]. More precisely, public safety bodies have the options to deploy LTE/LMR, LTE-only, or 5G networks based on the user needs and the business strategies.

C. Summary of Cellular Public Safety-related Features

From the implementation point of view, the migration from LMR to PS-LTE solutions for public safety requires the introduction of certain features on top of the LTE standard to match the public safety requirements. Thus, 3GPP started performing additional standardization efforts from its release Rel-12 [4]. However, the new functionalities are constantly evolving through the 3GPP releases to further enhance the public safety services. Fig. 3 depicts the set of features that are considered by 3GPP and that can be deployed in cellular public safety networks.

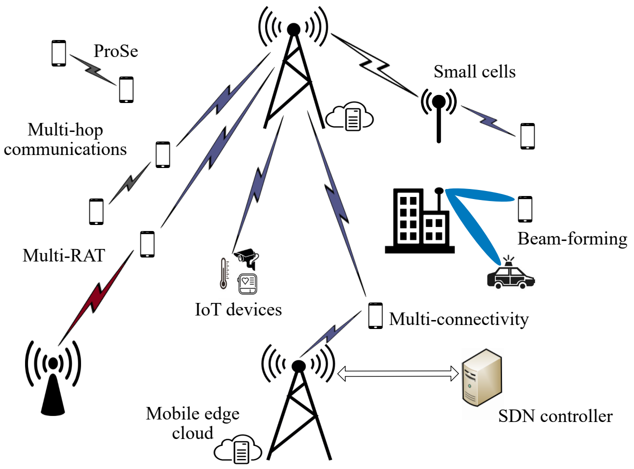

Fig. 3. Examples of public safety-related features in cellular networks

The proximity services (ProSe) were among the standardization items defined in 3GPP Rel-12 to present the architecture and radio interface for direct device-to-device (D2D) communications in LTE networks [4]. The new D2D interface is known as sidelink and it was introduced as part of the support of public safety ProSe by LTE networks. As proved by several research works dealing with this feature, deploying D2D communications in cellular networks, including for public safety applications, takes advantage of three gains (i.e., proximity, hop, and reuse) [9]. Each type of these gains holds the promises of improving certain network performance indicators. In summary, D2D communications may allow for high bit rates, low delays, high reliability, and low power consumption. On top of these gains, establishing direct links between devices in out-of-coverage scenarios helps provide the first responders with the needed communications especially in dangerous situations [10].

Public safety service reliability can be achieved not only using multi-hop communications but also through the flexible use of radio resources provided by the multi-connectivity and multi-radio access technologies (multi-RAT). Mobile-edge computing and software-defined networks (SDN) are among the features that can be deployed in cellular networks for improving the latency and security of the public safety services [10]. Furthermore, cellular networks, more precisely 5G networks, offer novel capabilities for managing a portfolio of various use cases with varying priorities such as network function virtualization and network slicing [4]. For instance, in the case of big events or major accidents, the traffic prioritization mechanisms can allow, in the first place, the necessary network capacity and performance for first responders and for other people around them who want to communicate in the second place [10]. As mentioned in Section I-B, IoT device adoption among the public safety community will enable various use cases like communication center alerting, accident video investigation, connected and automated cars. Among these new examples, certain applications are requiring very high data rates that can be achieved by the exploitation of techniques like beam-forming and small cells in 5G-enabled public safety networks [4].

II. Wearables in Cellular Public Safety Networks

With the evolution of public safety technologies and services, there is an increasing number of devices that are being deployed in these networks. Such a variety is shown in Fig. 1, where after having only PTT dedicated devices in LMR networks, safety, security, and health-care professionals are using cellular-connected mission-critical devices, smartphones, laptops, tablets, as well as vehicles in PS-LTE networks. However, the main capability of the PS-LTE networks is enabling the connection of the above-cited devices to the Internet [11]. With the aim of extending this capability, new devices are being deployed in a new ecosystem of public safety communications, known as Internet of Life Saving Things (IoLST).

Similar to the general definition of the IoT, the IoLST is a network of devices that collect data and use various communication technologies to share it in real time. However, its purpose is specific and consists in improving public safety responses to emergencies [11]. The IoLST represents an extension of the LMR and PS-LTE capabilities, which are mostly targeting the connection of computing devices to the Internet. In detail, IoLST solutions extend the public safety use cases into new types of applications including, but not limited to, real-time video using body-worn cameras, traffic system control with sensor-equipped vehicles, temperature and gas exposure measurement based on smart helmets, health-care and vital sign monitoring of first responders, and drone surveillance systems [12]. These IoLST use cases involve a variety of devices among which wearables are gaining the attention of the public safety community.

A. Wearables in the IoLST Ecosystem

One characteristic of public safety workforce is the mobility. Public safety personnel across law enforcement, fire, and emergency medical services (EMS) primarily operate in the field and deal with dangerous situations outside of their response vehicles. Therefore, relying on laptop computers is no longer an alternative for the first responders to stay connected. Hands-free operation is another peculiarity of public safety services, where the personnel is generally equipped with protective gloves that make it difficult for them to hold the smartphones or the tablets. Regarding these challenges, the IoLST ecosystem deploys wearable devices to make use of their form factor and their capability to encompass advanced sensors with the final aim of offering unique capabilities for the highly mobile, and in many cases autonomous, workforce and marking an important shift in the daily operation of the public safety personnel [11].

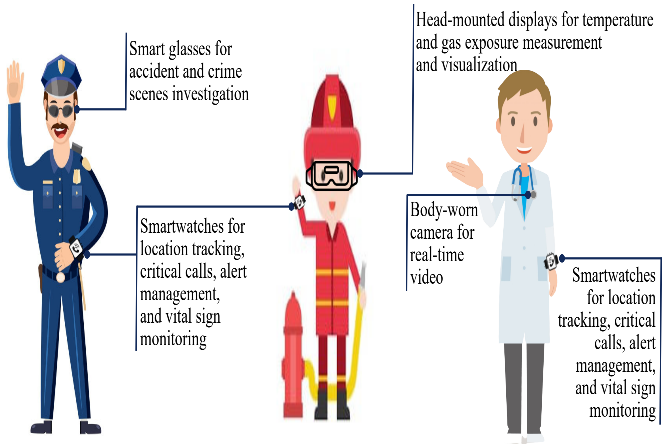
Smart glasses for accident and crime scenes investigation
Head-mounted displays for temperature and gas exposure measurement and visualization
Smartwatches for location tracking, critical calls, alert management, and vital sign monitoring
Body-worn camera for real-time video
Smartwatches for location tracking, critical calls, alert management, and vital sign monitoring

Fig. 4. Examples of wearable device-enabled services in the IoLST

Admittedly, wearable technology can deliver reliable in-field communications, enhanced situational awareness, and improved first responder safety by complementing the other cellular-connected devices and ensuring that the users stay closely connected to the data they need [13]. In Fig. 4, we illustrate examples of wearable devices and applications deployed within the framework of the IoLST for public safety. For instance, EMS workers can use body-worn cameras to send real-time videos about patients from ambulances and outdoor locations to indoor experts and professional doctors. Furthermore, outfitting the first responders with smartwatches enables the instant transmission of potentially lifesaving communications in a large-scale emergency response. These wearables can send real-time location, monitor alerts, and check the availability of required resources [13]. On top of these benefits, the introduction of low power wide area (LPWA) technologies in recent mobile networks (i.e., LTE-M and NB-IoT) can be considered as a motivation to provide wearable-based services, including public safety-related applications, at a lower cost, a better coverage, and lower power consumption [11].

B. Cellular-enabled Wearables

LPWA-enabled wearables are not the only standalone wearable devices that can use the cellular connectivity. Wearable devices and applications are among the verticals targeted by the 5G technology. With cloud native technologies being central parts of the 5G core architecture, the network will provide wearable devices with the needed storage capacity and processing power [14]. Hence, 5G-enabled wearables will be able to host more sensors, collect more data, and be involved in new sets of applications including public safety. Another fact that can motivate the public safety agencies and bodies to integrate 5G-enabled wearables in their networks is that 5G can be an all-inclusive communication platform for the delivery of low-end, mid-end, and high-end requirements of wearable applications [15]. More precisely, we identify three main facts that support this consideration, namely (i) the confirmation that NB-IoT and LTE-M fulfill, in the 3GPP study on "self-evaluation towards IMT-2020 submission", the IMT-2020 requirements for mMTC and can be certified as 5G technologies [16], (ii) the introduction of the NR RedCap technology for reduced-capability new radio devices and mid-end application requirements [16], and (iii) the dedication of several study items related to the 3GPP Rel-17 for the support of extended reality over 5G [17].

As depicted in Fig. 4, smart helmets, body-worn cameras, and vital sign (i.e., glucose, blood pressure, and heart rate) monitors are examples of wearable devices that can be involved in public safety applications. Other examples can include smart gloves and exoskeletons for supporting manual tasks. However, watch-type wearable devices are expected to be a game changer for public safety communications [18]. The ability to acknowledge the reception of messages, such as alerts and localization information, while keeping the hands free allows the first responders to perform their tasks with the addition of being safer and more responsive [18]. Several cellular LPWA-enabled smartwatches are currently available in the wearable market which make it possible for the public safety community to make use of both wearable technology and cellular connectivity.

III. Performance Evaluation of an MCPTT Service using Cellular-enabled Wearables

In this section, we investigate the performance of a wearable-based mission-critical application, more precisely an off-network MCPTT service using cellular-enabled smartwatches. The deployed smartwatches belong to one of the LTE-M device categories (LTE Cat-M1 and LTE Cat-M2), specifically LTE Cat-M2. In the following subsections, we refer to the LTE Cat-M2-enabled smartwatch as UE. Furthermore, we use network simulator 3 (ns-3) for the performance evaluation of the MCPTT scenarios. Specifically, this evaluation is performed based on the LTE/EPC network simulator (LENA) module updated with the scenarios and models that are specific to public safety communications. Such updates are supported by the research community and were first published in [19].

On top of the D2D communication support in ns-3, we extended LENA module by the features needed for the simulation of public safety scenarios and wearable devices. In detail, we consider scenarios in which the cellular network is deployed in the 700 MHz frequency band. In terms of wearable device modeling, an empirical off-body propagation loss model is implemented to better capture the signal propagation between wearable devices [20]. We also updated the ns-3 adaptive modulation and coding model with the reduced base-band capabilities that are provided by the 3GPP physical layer specifications [21].

A. Scenarios and Parameters

In general, MCPTT services support three categories of calls, namely private calls, general group calls, and broadcast group calls [22]. A private call is established between two MCPTT applications for two users to communicate. A general, or basic, group call is a call where a group of users that are associated with a particular group ID contend to talk. The third type of MCPTT calls is the broadcast group call which has the particularity of having one call initiator that is allowed to speak. In this paper, our main scenario is off-network basic group call with out-of-coverage UEs.

TABLE I
Performance evaluation parameters

Wearable device-related parameters	**Value**
UE type	Bandwidth-reduced low-complexity UE
Max. bandwidth	5 MHz
Max. modulation order	16-QAM
Max. transport block size	4008 bytes
UE transmission mode	1 (1 TX/RX antenna)
UE TX power	20 dBm
UE noise figure	9 dB
UE antenna height	1.5 m
D2D-related parameters	**Value**
Sidelink transmission mode	Mode-2 (Autonomous)
PSCCH period	40 ms
PSCCH length	8
MCS	10
Number of PRBs	5
kTRP	1
MCPTT application-related parameters	**Value**
Message size	60 Bytes
Packet interval	20 ms

In 3GPP specifications, the term bandwidth-reduced low-complexity (BL) is used to indicate the implementation of LTE-M device categories [21]. More precisely, the 3GPP TS 36.213 provides the recommendations for complexity reduction and base-band configuration of these devices. As part of these recommendations and as illustrated in Table I, the BL

TABLE II
ACCESS TIME CALCULATION IN MCPTT BASIC GROUP CALL SCENARIOS

The group call n exists?	The UE A is already in group call n?	The floor arbitrator of group call n exists?	Access time (AT) formula
No	No	No	$AT1 = TFG1$ (1)
Yes	No	No	$\boldsymbol{AT2 = T_{tx}(``CallProbe'') + T_{tx}(``CallAnnouncement'') + TFG2 + C201 * T201}$ (2)
Yes	Yes	No	$AT3 = C201 * T201$ (3)

UEs have a maximum bandwidth of 5 MHz, a maximum modulation order of 16-QAM, and one TX/RX antenna. Hence, the choice of these reduced-capability parameters allows us to better model the LTE Cat-M2-enabled smartwatches.

In connection with D2D communications and ProSe support, the main parameter is the sidelink transmission mode that defines the entity responsible for sidelink resource configuration. Two main modes have been defined for NR sidelink in 3GPP Rel-16; (i) network-controlled mode, also called transmission mode-1, in which the sidelink configuration is monitored and provided to the UEs by the BS, and (ii) autonomous mode, known as transmission mode-2, where UEs rely on sidelink pre-configurations stored in the devices [23]. While in-coverage UEs can operate in mode-1 or mode-2 as decided by the network, out-of-coverage UEs are restricted to using mode-2. As a result, we use the sidelink autonomous mode in our off-network basic group call scenario with out-of-coverage UEs.

In transmission mode-2 and before a D2D communication takes place on the Physical Sidelink Shared Channel (PSSCH), a sidelink grant needs to be pre-configured. The Physical Sidelink Control Channel (PSCCH) period parameter defines the periodicity of this grant configuration performed by each UE. Within a PSCCH period, there are separate sub-frames and physical resource blocks for control (PSCCH) and for data (PSSCH). Therefore, the number of sub-frames dedicated to the control, i.e., PSCCH length, needs to be fixed as mentioned in Table I. At the application level, the MCPTT model we use in the evaluation assumes that 60 byte voice packets are generated every 20 ms. This means that the data rate demand for the voice communication is 24 kbits/s.

B. Evaluation Results

As part of the performance assessment, we provide the numerical results of the MCPTT access time. According to the 3GPP specifications, the "MCPTT access time is defined as the time between when an MCPTT user requests to speak and when this user gets a signal to start speaking" [22]. The determination of this key performance indicator depends on the different processes of initiating or joining the basic group calls. Table II illustrates three possible situations with the correspondent access time formulas. In these situations, we assume that UE A is affiliated to a group call with an identifier n and wants to communicate with the other members.

Several concepts and notions that are included in the access time calculation are related to the MCPTT control protocols. More precisely, two families of control protocols are defined by the 3GPP specifications for the MCPTT calls, namely the call control protocols [24] that are responsible for the initial setup of the calls and the floor control protocols [25] that provide the "floor" to a single member of the group to be allowed to talk at a time. This current speaker is called floor arbitrator since it handles the requests of the other floor participants and gives them permissions to talk. As part of these control protocols, certain timers and counters are included in the MCPTT calls, such as:

- $TFG1$: "wait for call announcement" timer: is the time that a user should wait after sending a "Call Probe" message. By the expiry of this timer, the user decides about initiating or joining an existing group call.
- $TFG2$: "call announcement" timer: is restarted every time a "Call Announcement" message is sent.
- $C201$: "floor request retransmission" counter: defines the maximum number of "Floor Request" messages that a user can send.
- $T201$: "floor request retransmission" timer: is the time between sending two "Floor Request" messages.

The used timers and counters have default values that are defined by the 3GPP specifications. Therefore, the access time results, based on the Equations 1 and 3, have predictive values that do not allow the evaluation of the impact of several parameters on the access time values. Consequently, we focus on the second scenario depicted in Table II, more precisely on the access time values produced using Equation 2. In this formula, $T_{tx}(X)$ represents the one-way transmission time of message X, which is defined as the duration from when the message X becomes available at the source UE to when it is successfully received by the destination UE.

The first parameters that we consider are related to the wearable device capabilities. As shown in Table III, we provide the average access time to an MCPTT application established between two LTE Cat-1 smartphones versus two LTE Cat-M2 smartwatches. On top of the significant impact that can be resulted from the difference in the supported bandwidth, thus in the number of physical resource blocks (PRBs) that can be allocated for sidelink, the propagation model is another essential and challenging parameter especially when considering body communications and the peculiarities of signal propagation in wearable applications. However, the resulted gap in the access time performance can be compensated by the consideration of other MCPTT-related parameters.

TABLE III
AVERAGE ACCESS TIME RESULTS IN TERMS OF DEVICE CAPABILITIES: LTE CAT-1 SMARTPHONES VS. LTE CAT-M2 SMARTWATCHES

Main device capabilities	**Average access time**
Device category: LTE Cat-1 Bandwidth: 10 MHz TX power: 23 dBm Free space path loss propagation model	205 ms
Device category: LTE Cat-M2 Bandwidth: 5 MHz TX power: 20 dBm Off-body propagation model	230 ms

In terms of D2D-related parameters, we start with the impact of the PSCCH period and PSCCH length on the access time results. As illustrated in Fig. 5, longer PSCCH periods result in longer access time values. This can be justified by the fact that one important component of the access time formula provided in Equation 2 is the "floor request retransmission" timer which is equal to the PSCCH period according to the 3GPP default setting. The impact of the number of sub-frames dedicated to the control (PSCCH) is also depicted in Fig. 5. Preferring PSSCH over PSCCH transmissions (i.e., shorter PSCCH length) can provide shorter access time values, which is important in public safety services where even few milliseconds can make a difference in critical situations. In summary, to guarantee a short access time for critical MCPTT communications, short PSCCH periods with low PSCCH to PSSCH ratios are recommended. However, this recommendation can increase the probability of collisions due to the frequent scheduling messages exchange and the limited number of sub-frames dedicated to the control. Therefore, latency and reliability trade-off mechanisms should be considered for critical and reliable MCPTT group calls.

The second part of D2D-related parameters that we focus on is the sidelink grant scheduling method. In transmission mode-2, that we are using in this evaluation since the UEs are out-of-coverage, the MCPTT group call members are responsible for determining the modulation and coding scheme (MCS), the number of PRBs, and the number of transmission opportunities in each time resource pattern defined by the kTRP parameter. As depicted in Table I, we used a default scheduling in the previous access time results, where sidelink grant parameters are pre-fixed (i.e., fixed scheduling). Nevertheless, and as demonstrated in Fig. 6, the sidelink grant scheduling can be performed following certain optimization goals, such as selecting a grant configuration that utilizes the minimum number of PRBs per transmission (i.e., Min. PRB scheduling) or that maximizes the communication range (i.e., Max. coverage scheduling). These optimized methods show a better performance in terms of access time values, which is necessary especially in the case of MCPTT group calls with an increasing number of members.

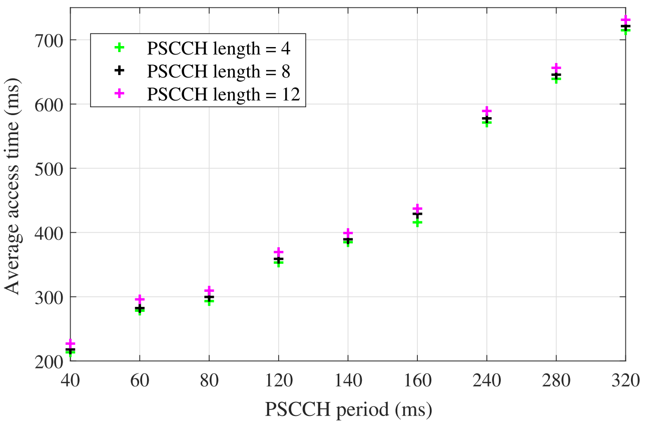

Fig. 5. Average access time for joining an MCPTT group call in function of the PSCCH period and PSCCH length

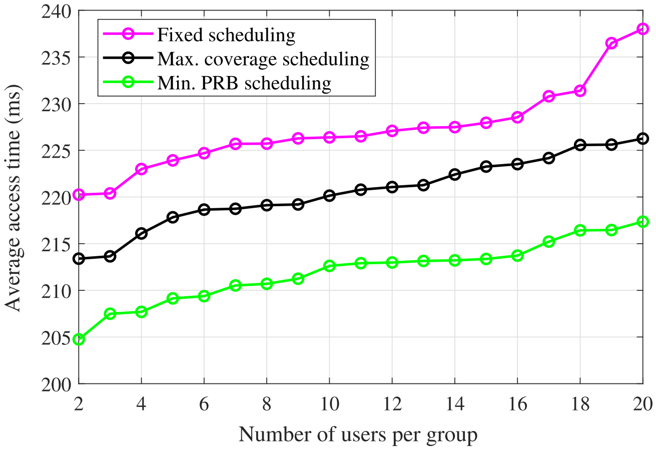

Fig. 6. Impact of sidelink resource scheduling methods on the average access time with an increasing number of MCPTT clients in a basic group call

IV. CONCLUSION

Enhancing current office-bound applications and enabling new services are the reasons behind the migration from traditional LMR to cellular systems for public safety. In this paper, we presented the main features that are introduced in the 3GPP specifications and that can motivate the public safety organizations to select the cellular connectivity as an alternative in their communication platforms. As part of the new applications that can be enabled in the cellular-based IoLST ecosystem, we focused on wearable services and we provided examples of use cases that show how wearable technology can deliver improved safety and situational awareness for first responders.

This state of the art overview of cellular-enabled wearables in public safety networks was followed by a performance evaluation of a mission-critical service using LTE Cat-M2-enabled smartwatches. More precisely, we analyzed the MCPTT access time performance for different combinations of device capability and D2D-related parameters. The aim of this evaluation is to show that with an appropriate sidelink tuning cellular-enabled wearables can compensate the latency performance degradation due to the device complexity reduction. This tuning has to take into consideration several parameters like the PSCCH period, the number of PSCCH sub-frames, and the grant scheduling method. Additionally, dealing with other open issues, such as the latency and reliability trade-off, can help further enhance the performance of wearable-based MCPTT applications in future public safety use cases.

Acknowledgment

The authors gratefully acknowledge funding from the European Union's Horizon 2020 Research under the Marie Sklodowska Curie grant agreement No. 813278 (A-WEAR: A network for dynamic wearable applications with privacy constraints, http://www.a-wear.eu/).

References

[1] A. U. Chaudhry and R. H. Hafez, "LMR and LTE for public safety in 700 mhz spectrum," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[2] M. Stojkovic, "Public safety networks towards mission critical mobile broadband networks," Master's thesis, Norwegian University of Science and Technology, June 2016.

[3] A. Yarali, *Public safety networks from TETRA to commercial cellular networks*. Wiley Telecom, 2020, pp. 1–13.

[4] TCCA, "4G and 5G for public safety," White Paper, March 2017. [Online]. Available: https://tcca.info/documents/2017-march_tcca_4g_and_5g_for_-public_safety.pdf

[5] "Mission-critical services in 3GPP," June 2017, [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/1875-mc_services. [Accessed: 2020-07-09].

[6] 3GPP, "Technical specification group services and system aspects; common functional architecture to support mission critical services; stage 2 (release 14)," TS 23.280, November 2016.

[7] A. Yarali, *Higher generation of mobile communications and public safety*. Wiley Telecom, 2020, pp. 81–95.

[8] P. Zhang, J. Lu, Y. Wang, and Q. Wang, "Cooperative localization in 5G networks: A survey," *Ict Express*, vol. 3, no. 1, pp. 27–32, 2017.

[9] G. Fodor *et al.*, "Design aspects of network assisted device-to-device communications," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 170–177, 2012.

[10] A. Yarali, *Public safety communication evolution*. Wiley Telecom, 2020, pp. 37–65.

[11] "What is the Internet of Life Saving Things (IoLST)?" December 2018, [Online]. Available: https://www.sierrawireless.com/iot-blog/iot-blog/2018/12/internet-of-life-saving-things/. [Accessed: 2020-07-09].

[12] "The Internet of Lifesaving Things: Smarter cities, smarter response," January 2018, [Online]. Available: https://about.att.com/newsroom/internet_of_lifesaving_things.html. [Accessed: 2020-07-29].

[13] The Public Safety Network, "Enhancing response capabilities with smartwatches in public safety," White Paper, 2019. [Online]. Available: http://publicsafety.network/SmartWatch-White_Paper.pdf

[14] 5G Americas, "5G and the cloud," White Paper, December 2019. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/12/5G-Americas_5G-and-the-Cloud..pdf

[15] Research and Markets, "Opportunities, challenges and forecasts in the global public safety LTE & 5G market 2020-2030," Report 5067345, May 2020.

[16] 3GPP, "New SID on support of reduced capability NR devices," TDoc RP-193238, December 2019.

[17] ——, "Technical specification group services and system aspects; extended reality (XR) in 5G; (release 16)," TR 26.928, September 2019.

[18] "CAD on smartwatches is a game changer for police communications," May 2019, [Online]. Available: https://www.publicsafety.network/blog-5.29.19.html. [Accessed: 2020-07-29].

[19] R. Rouil, F. J. Cintron, A. Ben Mosbah, and S. Gamboa, "Implementation and validation of an LTE D2D model for ns-3," in *Proceedings of the Workshop on ns-3*, 2017, pp. 55–62.

[20] R. G. Garcia-Serna, C. Garcia-Pardo, and J. M. Molina-Garcia-Pardo, "Effect of the receiver attachment position on ultrawideband off-body channels," *IEEE Antennas and Wireless Propagation Letters*, vol. 14, pp. 1101–1104, 2015.

[21] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); physical layer procedures (release 8)," TS 36.213, March 2007.

[22] ——, "Technical specification group services and system aspects; mission critical push to talk (MCPTT); stage1 (release 13)," TS 22.179, September 2014.

[23] S. A. Ashraf, R. Blasco, H. Do, G. Fodor, C. Zhang, and W. Sun, "Supporting vehicle-to-everything services by 5G New Radio Release-16 systems," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 26–32, 2020.

[24] 3GPP, "Mission critical push to talk (MCPTT) call control; protocol specification (release 13)," TS 24.379, December 2015.

[25] ——, "Mission critical push to talk (MCPTT) media plane control; protocol specification (release 13)," TS 24.380, December 2015.