ofinno

Mission Critical Services

Pushing the LTE Limits to Save Lives

Table of Contents

Abstract

In mission critical situations, communications among responders must maintain a high level of reliability, availability, quality of service and security in scenarios that go beyond the limits that are stipulated in a commercial wireless network. The 3rd Generation Partnership Project (3GPP) Technical Specification Group on Service and System Aspects (TSG-SA) has developed a series of technical specifications in its SA6 working group to define an architecture for various mission critical services including mission critical push to talk (MCPTT), mission critical data (MCData), and mission critical video (MCVideo). This paper provides an overview of 3GPP standardization of mission critical services in LTE and its evolution in the 5th generation (5G) wireless networks.

2. Introduction

Mission critical services are essential for survival in extra ordinary situations, when any decision may be a matter of life or death.

If a public safety service is ranked as "mission critical," the service will automatically be given a goal to minimize the likelihood of the service failing to avoid any risk of injury or worse. Mission critical services for public safety rely heavily on communications among first responders such as police, firefighters, and medical emergency personnel. First responders have a primary goal to reduce the devastating outcomes of disasters. Therefore, it is imperative for the first responders to mission critical situations to successfully communicate with each other and with responders who arrive later to the mission critical situations.

Maintaining communications during a mission critical situation, where public safety is at risk, is challenging if the responders find themselves in an environment with no network connectivity due to pre-existing conditions or geographical obstructions. Locations where mission critical communications can break down include tunnels, rural areas where there is no network access, and service areas where network access nodes are nonfunctional. In these locations, first responders may establish mission critical communications directly and exclude network involvement.

Mission critical communications must be very reliable with minimal to no loss of connectivity. The mission critical communications must also have high data rates, high quality, and very low end-to-end latency for media transmission among the mission critical responders and robotics.

Mission critical communications must not cause any confusion among responders. The responders must be able to communicate about the public safety situation without being interrupted by less important conversations. At the same time, responders with important news must be able to interrupt other responders to describe their current conditions. Mission critical communications should also allow group leaders to interrupt other responders to call for actions which need immediate attention.

Mission critical communications are not limited to communications among the responders. Mission critical communications may also involve communications with robotics such as unmanned aerial vehicles (UAV) and autonomous vehicles. These robotics can gain visual, proximity, and transportation advantages in situations where it is not otherwise possible to take necessary actions. These advantages may be crucial to facilitate, improve, or even make possible mission critical responses. Mission critical communications must be very reliable with minimal to no loss of connectivity. The mission critical communications must also have high data rates, high quality, and very low end-to-end latency for media transmission among the mission critical responders and robotics.

3. 3GPP Standards

Third Generation Partnership Project (3GPP) standardization has taken a lead role to standardize a global system of mission critical services for public safety. To perform this task, the 3GPP Technical Specification Group on Service and System Aspects (TSG-SA) has created a new Working Group, SA WG6. SA WG6 is responsible for defining, evaluating, and maintaining the technical studies and technical specifications for application elements and interfaces supporting mission critical communications.

Although SA WG6 is the main group responsible for mission critical services, other working group in TSG-SA, TSG Core Network and Terminals (TSG-CT), and TSG Radio Access Network (TSG-RAN) are also involved in developing standards for these services. The main duties of SA-WG6 include:

- Defining services within critical communications,
- Defining an architecture for critical communications services,
- Defining reference points and interfaces between mission critical architectural network nodes,
- Defining and specifying flows between reference points with appropriate bit rates, delays, security,
- Identifying application protocols, and
- Maintaining interoperability with other existing critical communication services such as mission critical voice services and Land Mobile Radio (LMR) services.

Figure 1 shows the structure of the TSG-SA working groups and their responsibilities.

3GPP SA WG6 limited release 13 of mission critical services for the public safety to voice only (i.e. Mission Critical Push-to-Talk (MCPTT)), which was an extension and evolution of Open Mobile Alliance (OMA) Push-to-Talk over Cellular (PoC) for emergency scenarios. The work for mission critical services was expanded to accommodate new services such as video and data in Release 14 of mission critical services. Mission critical services in release 14 added capabilities to provide direct view and aid to critical situations using robotics, remote data access, and location based critical assistance. The mission critical services work items of release 14 are directed to:

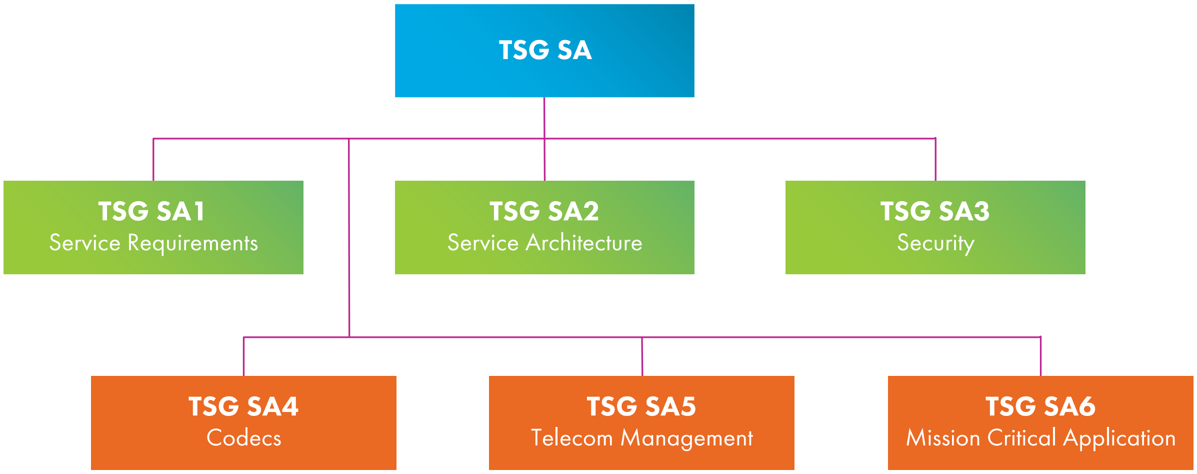

Figure 1: Structures of TSG-SA working groups

- Mission critical core (MCCoRe) for common features of all mission critical services,
- Mission critical Push-to-Talk (MCPTT) for mission critical voice conversations,
- Mission critical video (MCVideo) for transmission of mission critical video, and
- Mission critical data (MCData) for the transfer of mission critical data (e.g. file transfer, text transfer, and robotics).

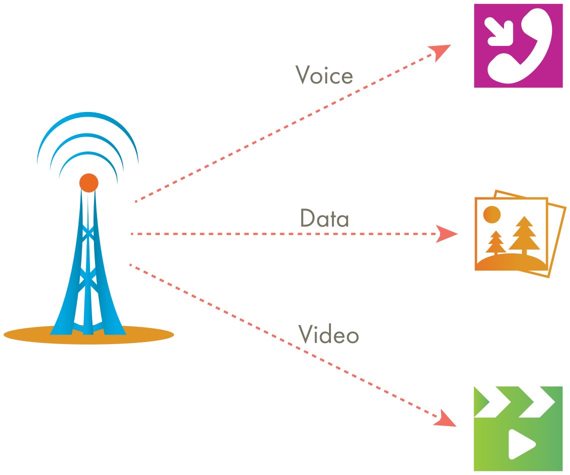

Figure 2: 3GPP release 14 mission critical services includes voice, video, and data

4. Proximity Services

Mission critical services employ proximity services (ProSe) that facilitate the discovery and communication of devices that are physically close to each other. Specifically, ProSe defines discovery mechanisms, Model A and Model B. The Model A discovery mechanism is based on a mission critical device making repeated announcements "I am here!" The Model B discovery mechanism is based on a request and response protocol where a mission critical device makes repeated announcements (i.e. a request) :"Who is there?" to find all mission critical group members, or "Are you there?" to specific mission critical group members. Subsequently, the called mission critical group members respond to the announcement.

Figure 3 shows a ProSe discovery message which is employed for Model A and Model B discovery procedures. When the mission critical services are employing Model A as the discovery mechanism, the "announced Temp ID" is the "MCS specific data" comprising information of a mission critical group member's identity and mission critical application. Depending on the discovery type for Model A, the MCS specific data may be either "restricted" or "open."

In the Model B discovery mechanism, the mission critical device is either a "discoverer" or a "discoveree." The discoverer mission critical device announces query codes. The discoveree mission critical device responds to the query codes with response codes. The query codes and response codes are obtained from a mission critical function and are related to the mission critical group member identities and mission critical applications. The discovery type is always set to "restricted" for Model B.

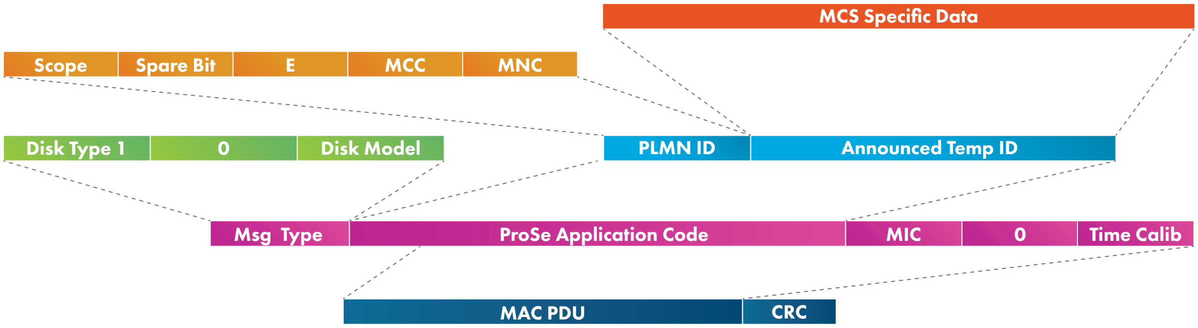

Figure 3: ProSe Discovery Message

Mission critical services may rely on either a Long-Term Evolution (LTE) network (i.e. “on-network” mission critical services), or direct communications (i.e. “off-network” mission critical services).

Since the security measurements for mission critical services are of great importance, the Model B discovery mechanism is employed by these services. The ProSe specification 3GPP TS 23.303 defines security measurements commensurate with the threat for Model A and Model B.

5. On-Network and Off-Network Mission Critical

Mission critical services may rely on either a Long-Term Evolution (LTE) network (i.e. “on-network” mission critical services), or direct communications (i.e. “off-network” mission critical services).

On-network mission critical services may use the LTE network for high efficiency real time communications, high quality video, and data transmission with low end-to-end latency. The on-network mission critical services employ an Internet Protocol Multimedia Subsystem (IMS) architectural framework for media control functions to access internet protocol (IP) multimedia services to provide a rich voice and rich media experience. Mission critical devices may also be compatible with other IMS services which are not mission critical services, such as Voice over LTE (VoLTE).

Off-network mission critical services rely on device-to-device (D2D) communications (i.e. direct communications between nearby devices). The D2D communications employ newly specified radio “sidelink” connectivity using the LTE radio and related radio channels to allow proximate devices to discover, synchronize, and communicate. Therefore, proximate mission critical devices in regions lacking commercial LTE spectrum may use

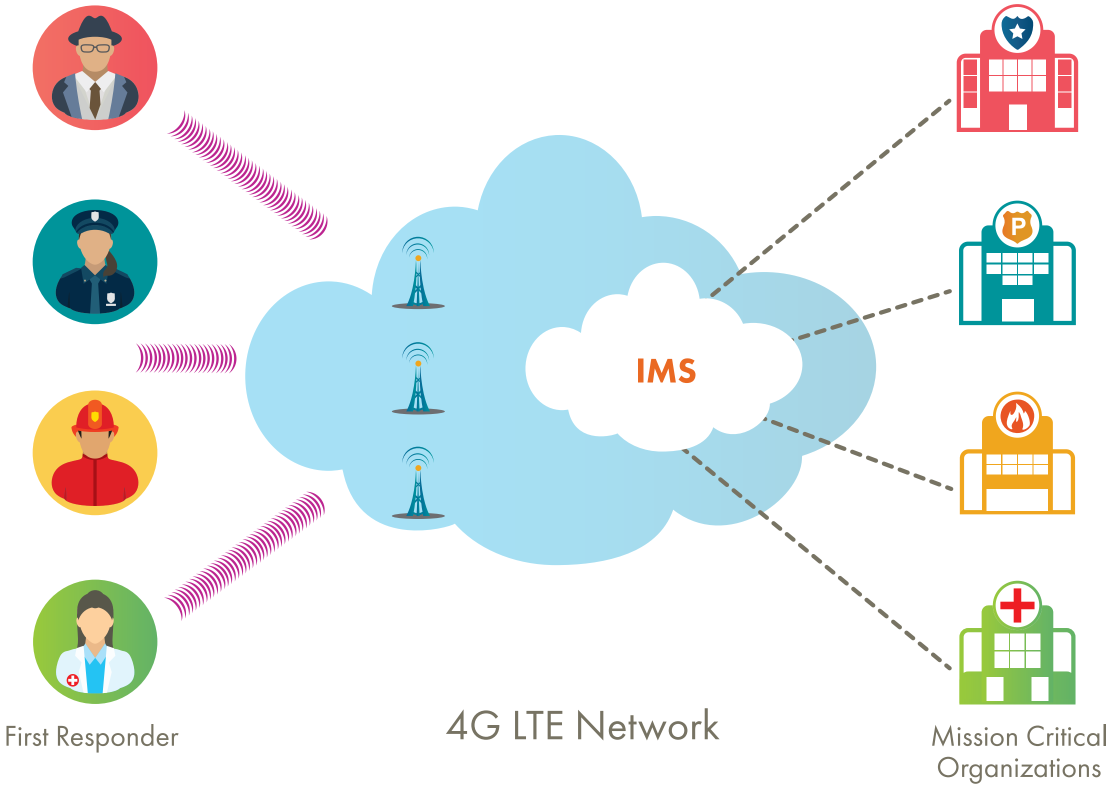

Figure 4: LTE and IMS for mission critical services

Both on-network and off-network mission critical services are proximity services which assume the devices are in the vicinity of each other.

sidelink connectivity to setup and maintain off-network mission critical services. Although absence of an LTE network leaves no other option than to operate mission critical services off-network, the 3GPP standards still provides the choice of operating mission critical services off-network using sidelink connectivity, even when there is an accessible LTE network available.

Both on-network and off-network mission critical services are proximity services which assume the devices are in the vicinity of each other. Prior to establishing an on-network and off-network mission critical service, the devices are configured with discovery codes and operating frequencies by the network. Figure 5 illustrates off-network MCS devices under indirect control of an LTE network that configures the MCS devices for synchronization and communication. On-network and off-network features of mission critical services allow mission critical devices to handle various scenarios and use cases defined by the 3GPP standards.

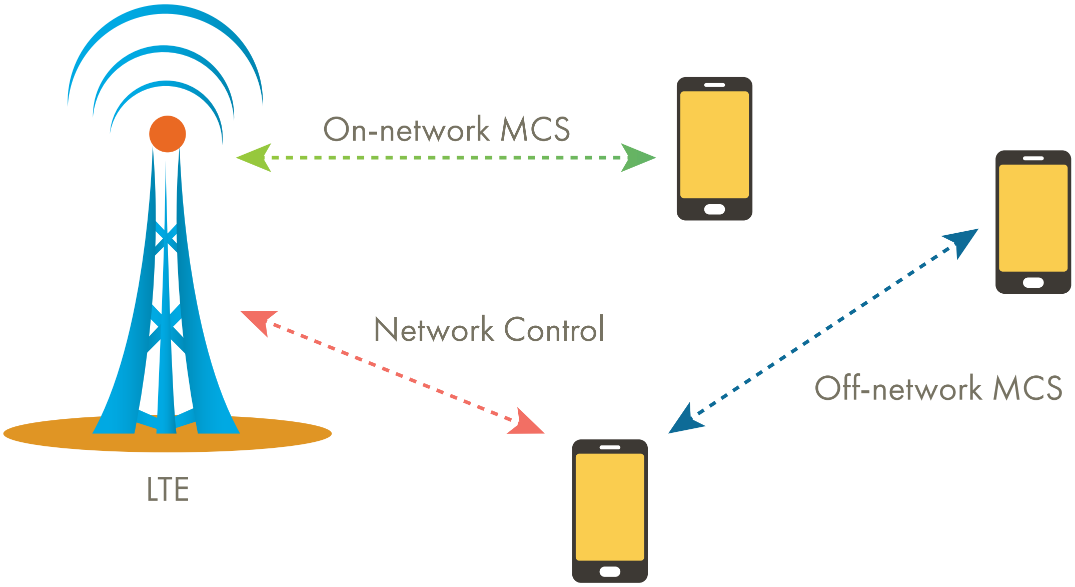

Figure 5: On-network and off-network mission critical services

6. Sidelink Radio Channels

Mission critical D2D communication is based on sidelink connectivity. Sidelink connectivity requires discovery, time synchronization, and frequency synchronization of the devices. In order to discover each other, mission critical devices first synchronize in time and frequency and then perform a discovery procedure. The mission critical devices may then communicate with each other using sidelink connectivity. LTE systems provide a system information block (SIB 19) that includes configuration parameters related to sidelink discovery, and another system information block (SIB 18) that includes configuration parameters related to sidelink communications.

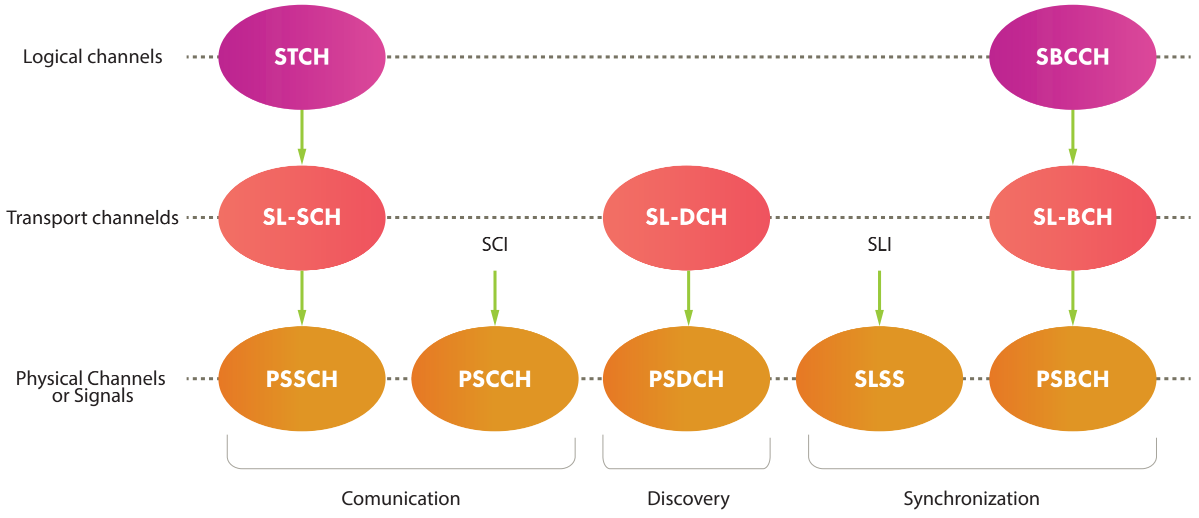

Figure 6: Channel structure for sidelink connectivity

Figure 6 illustrates LTE radio channels used for sidelink connectivity. Sidelink Traffic Channel (STCH) is a logical channel for exchanging sidelink communications user data and is mapped to a Sidelink Shared Channel (SL-SCH) transport channel. SL-SCH is then mapped to a Physical Sidelink Shared Channel (PSSCH). For a receiving device to detect and decode information in the PSSCH, the Sidelink Control Information (SCI) is mapped to a Physical Sidelink Control Channel (PSCCH) that is transmitted in parallel to the PSSCH.

A Sidelink Discovery Channel (SL-DCH) is a transport channel employed by a discovery procedure. The SL-DCH is mapped to a Physical Sidelink Discovery Channel (PSDCH). The sidelink discovery does not have any logical channel. Therefore, there is not a Radio Link Control (RLC) to support error detection and recovery, segmentation, reassembly, duplicate detection, and flexibility of data transmission with or without acknowledgment; nor is there a Packet Data Convergence Protocol (PDCP) to support header compression, ciphering, integrity protection, and transfer of user data and control data.

A Sidelink Synchronization Signal (SLSS) comprises a Primary Sidelink Synchronization Signal (PSSS) and a Secondary Sidelink Synchronization Signal (SSSS) associated by a Sidelink Identifier (SLI). The SLI indicates whether the broadcasted SLSS is synchronized in-coverage by a network or out of coverage by another reference mission critical device. Sidelink synchronization comprises a logical channel Sidelink Broadcast Control Channel (S-BCCH) corresponding to a Sidelink Broadcast Channel (SL-BCH) and a Physical Sidelink Broadcast Channel (PSBCH). The PSBCH may be employed by the mission critical devices to broadcast basic system information referred to as a Sidelink Master Information Block (SL-MIB) to convey the following information:

D2D communication is based on sidelink connectivity which requires discovery, time synchronization, and frequency synchronization by the devices. Mission critical devices must first synchronize in time and frequency in order to discover each other and thereafter communicate to each other.

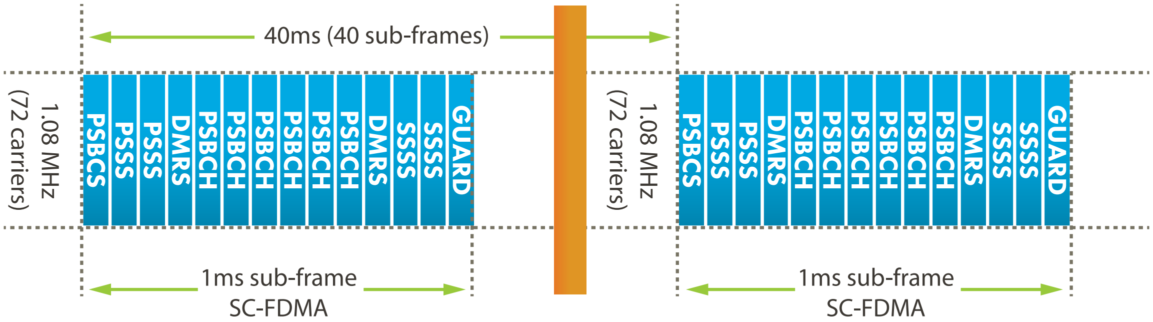

Figure 7: Structure for sidelink synchronization signal

- carrier bandwidth,
- time division duplex (TDD) configuration,
- actual transmitted subframe/frame number to facilitate the subframe/frame level synchronization, and
- an indicator for being in-coverage or being out of coverage.

Both the PSBCH and the SLSS are transmitted in the same subframe and the same resource blocks.

Figure 7 illustrates a structure for the SLSS (PSSS and SSSS) and the PSBCH. A Demodulation Reference Signal (DMRS) is a reference signal that enables the received subframe to be decodable. Regularity rules may inform what a mission critical device is transmitting to avoid interference within a radio cell. Thus, sidelink channels comprising the PSBCH and the SLSS (PSSS and SSSS) maximize commonalities with LTE uplink channels, even though the SLSS (PSSS and SSSS) employs principles of the LTE downlink PSS and SSS.

MCS devices which are in partial coverage or out of coverage may transmit the SLSS when the signal power from selected MCS devices fall under a certain threshold. The recipient MCS devices can then synchronize, discover and communicate with each other.

Figure 8 illustrates an in-coverage MCS device synchronizing to an LTE network and transmitting an SLSS when the MCS device is configured to transmit the SLSS. The MCS device may also transmit the SLSS when a signal power received from the LTE network is below a certain threshold. MCS devices which are in partial coverage or out of coverage may transmit the SLSS when the signal power from selected MCS devices falls under a certain threshold. The recipient MCS devices can then synchronize, discover and communicate with each other.

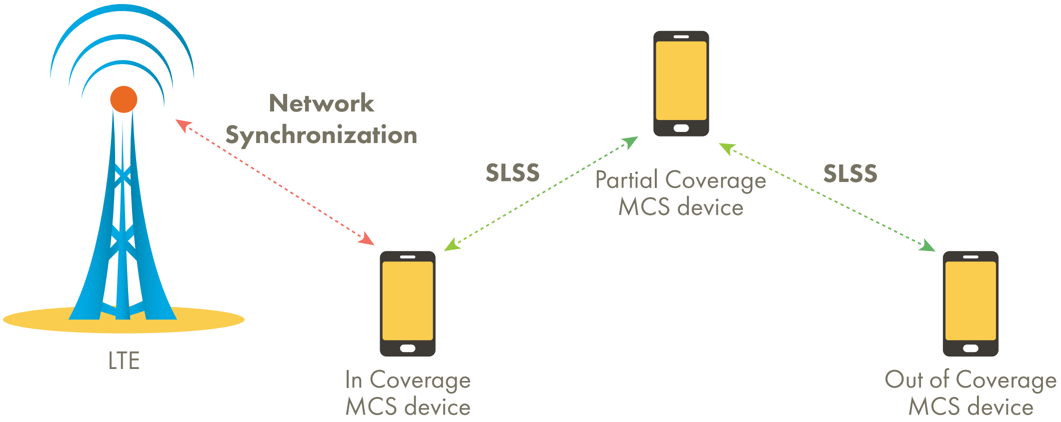

Figure 8: In coverage, partial coverage, and out of coverage synchronization

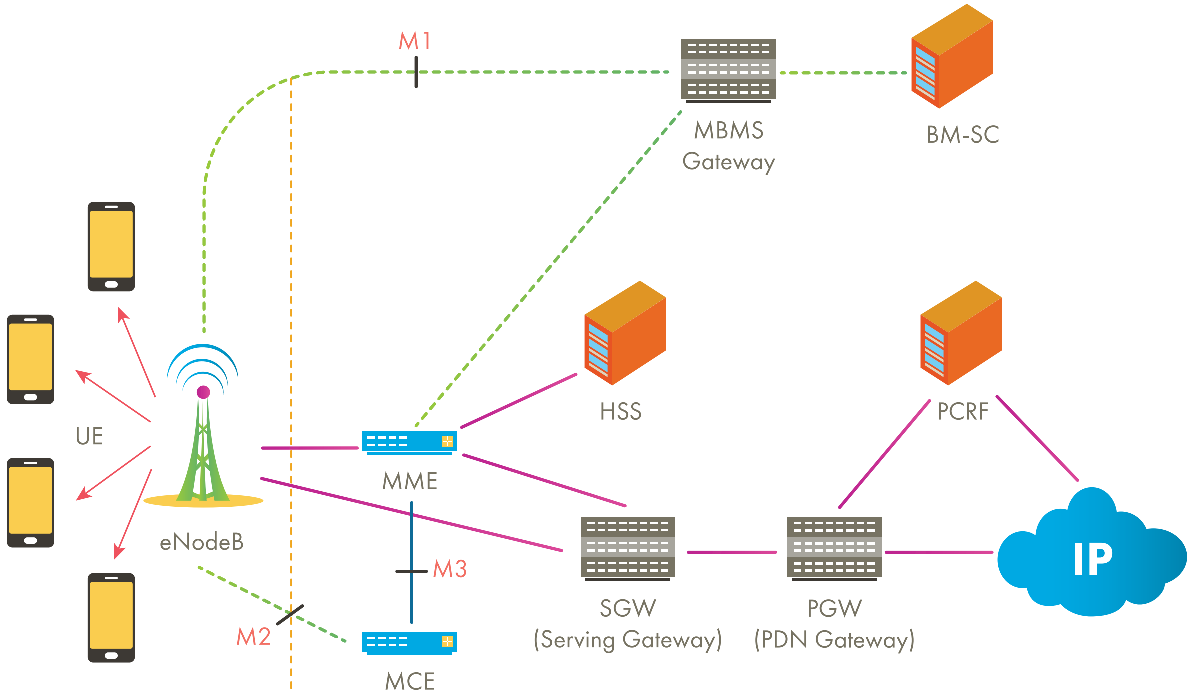

Figure 9: Architecture for GCSE

7. MBMS for Mission Critical Service

On-network mission critical services are a Group Communication Service Enabler (GCSE) of LTE technology. The concept of Group Communication Services (GCS) was introduced in 3GPP TS 23.468 release 12, with an architecture for both Evolved Packet System (EPS) and Multicast Broadcast, Multicast Services (MBMS) bearer services. A Group Communication Service application server (GCS AS) employs EPS and MBMS bearer services for transmitting downlink signaling and data from a GCS AS to wireless devices. In the uplink, the wireless devices employ EPS bearer services for signaling and transferring data to the GCS AS. (See 3GPP TS 23.468). There is no requirement for IMS in GCSE.

Figure 9 illustrates an architecture of the GCSE for LTE technology. EPS bearer services are implemented by a connection between the GCS AS (not shown in the figure) and a Packet Data Network (PDN) gateway, and a connection between the “function” of the GCS AS and Policy Charging Rules Function (PCRF). A Quality of Service (QoS) of the EPS bearer services are adjusted by PCRF with respect to the provided services and the subscription profile of the wireless device. The MBMS bearer services are implemented by a connection between the GCS-AS and a Broadcast Multicast Service Center (BM-SC). The BM-SC has a set of functionalities for authorization, authentication, security, scheduling, QoS, and many more for the MBMS bearer services. (See 3GPP TS 23.246).

Subject to network choice, use case, and availability of multicast bearer in a radio cell, mission critical services may operate employing MBMS bearer services.

Subject to network choice, use case, and availability of multicast bearer in a radio cell, mission critical services may operate employing MBMS bearer services. If both

MBMS and EPS bearer services are needed for an on-network mission critical service such as MCPTT, where floor control signaling needs to be transmitted one-to-one but the voice media can be distributed one-to-many, the mission critical services may operate by accessing both unicast and multicast bearer resources.

8. 5G and Mission Critical Services

Fifth Generation (5G) wireless mobile communication promises increased data rates, significantly reducing end-to-end latency, and enabling ultra-reliability for services such as mission critical services through new possibilities for rich media, automation, and robotics. Reduced end-to-end latency is achieved through network slicing and bringing content closer to users. 5G achieves ultra-reliability by introducing redundancy links and multiple connectivity. D2D communications also play a major role in 5G technology. D2D communications can be employed for off-network mission critical services to deliver faster and more reliable services by bypassing network processing for control and user planes. In addition, the D2D communications alleviate radio cell congestion via traffic offloading and thereby increases network capacity and reliability.

D2D communications can be employed for off-network mission critical services to deliver faster and more reliable services by bypassing network processing for control and user planes.

3GPP has already started a study to consider new use cases for high priority mission critical services as described in the technical report 3GPP TR 22.862. 3GPP 5G delivers significant improvements for mission critical services in terms of end-to-end latency, ubiquity, security, robustness, availability, and reliability.

Glossary

3GPP	3rd Generation Partnership Project
5G	5th Generation
BM-SC	Broadcast Multicast Service Center
D2D	Device-to-Device
DMRS	Demodulation Reference Signal
EPS	Evolved Packet System
GCS	Group Communication Services
GCS-AS	Group Communication Service application server
GCSE	Group Communication Service Enabler
IMS	Internet Protocol Multimedia Subsystem
IP	Internet Protocol
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MBMS	Multicast Broadcast, Multicast Services
MCCoRe	Mission Critical Core
MCData	Mission Critical Data
MCPTT	Mission Critical Push-to-Talk
MCS	Mission Critical Services
MCVideo	Mission Critical Video
OMA	Open Mobile Alliance
PCRF	Policy Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PoC	Push-to-Talk over Cellular
ProSe	Proximity Services
PSBCH	Physical Sidelink Broadcast Channel
PSCCH	Physical Sidelink Control Channel
PSDCH	Physical Sidelink Discovery Channel
PSSCH	Physical Sidelink Shared Channel

PSSS	Primary Sidelink Synchronization Signal
QoS	Quality of Service
RLC	Radio Link Control
S-BCCH	Sidelink Broadcast Control Channel
SCI	Sidelink Control Information
SIB	System Information Block
SL-BCH	Sidelink Broadcast Channel
SL-DCH	Sidelink Discovery Channel
SLI	Sidelink Identifier
SL-MIB	Sidelink Master Information Block
SL-SCH	Sidelink Shared Channel
SLSS	Sidelink Synchronization Signal
STCH	Sidelink Traffic Channel
SSSS	Secondary Sidelink Synchronization Signal
TDD	Time Division Duplex
TSG-CT	TSG Core Network and Terminals
TSG-SA	Technical Specification Group on Service and System Aspects
TSG-RAN	TSG Radio Access Network
UAV	Unmanned Aerial Vehicle
Voice over LTE	VoLTE

References

3GPP TS 23.303:
Proximity-based services (ProSe); Stage 2

3GPP TS 23.468:
Group communication System Enablers for LTE (GCSE_LTE; Stage 2

3GPP TS 23.246:
Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description

3GPP TR 22.862:
Feasibility study on new services and markets technology enables for critical communications; Stage 1

About Ofinno

Ofinno develops wireless technologies that address some of the most important technological issues in today's modern life. Our wireless technology innovators create new technologies that have an astounding 67% utilization rate, producing tangible results for both wireless device users and carriers alike. At Ofinno, the people inventing the technologies are also the people in charge of the entire process, from the idea, through design, right up until the technology is sold. Ofinno's research focuses on fundamental issues such as improving LTE-Advanced performance, Mission Critical Services, Inter-Band Carrier Aggregation, New Radio for 5G, V2X, IoT, and Power Management. Our team of scientists and engineers seek to empower mobile device users, and the carriers that serve them, through cutting edge network performance innovations.