3

LTE for Public Safety Networks

3.1 Why LTE for Public Safety Networks?

When the Federal Communications Commission (FCC) of the United States of America (USA) decided to use Long-Term Evolution (LTE) as the new radio technology for public safety communication, it was building on the assumption of a global widespread adoption of the LTE technology. At the time of writing this book, the Global Mobile Suppliers Association (GSA) had listed 300 deployed LTE networks in 107 countries and forecasts 350 networks by the end of 2014. Nearly 1900 LTE-capable devices are available on the market by now. For more information on market figures, see Ref. [1].

One important driver behind the desire to use LTE for Public Safety Communication was the economies of scale achievable with LTE compared to existing Public Safety Communication technologies. This is on cutting down not only infrastructure costs (CAPEX, Capital Expenditure) but also operational costs (OPEX, Operational Expenditure). Technology for legacy Public Safety networks such as the Project 25 (P.25) or Association of Public Safety Communications Officials (APCO-25), standardized under the Telecommunications Industry Association Engineering Committee TR-8 [2], and the Terrestrial Trunked Radio (TETRA), standardized under ETSI Technical Committee TETRA (TCCE) (TETRA and Critical Communications Evolution) [3], are addressing relatively small markets with few suppliers only and thus do not have the potential to cut down costs to build-out public safety networks and costs of devices (e.g., public safety devices can be very expensive, from $1000 onward, compared to well-known mobile smartphone prices). In contrast, LTE is a global standard, the equipment being able to be used everywhere in the globe with minor adaptations as necessary. This allows reducing production and deployment costs significantly.

On OPEX side, using widely adopted LTE technology allows building public–private partnerships, various studies estimate high savings on total cost of ownership over 10 years of operation. In this scenario, a Public Safety network operator teams up with commercial operators of 3rd Generation Partnership Program (3GPP) networks making use of their infrastructure where possible and potentially enhancing coverage when necessary.

Another driving force is the ability of LTE to provide efficient high speed, low latency, low setup time, and high-security data connectivity, which is the precondition to provide multimedia and especially mission critical multimedia communication. TETRA, for example, provides

LTE for Public Safety, First Edition. Rainer Liebhart, Devaki Chandramouli, Curt Wong and Jürgen Merkel.

only 7.2 kbit/s data transfer rate per time slot (P.25 offers even less). Four time slots can be combined, which results in a gross data rate of 28.8 kbit/s. New versions of the TETRA standard support data rates up to 691.2 kbit/s.

Another bonus in using LTE is the availability of radio equipment for the most diverse deployment scenarios. LTE base stations are available from macro down to micro, pico, and even femto cell size, that is, at the size of residential Wireless Local Area Network (WLAN) or cable router modems, making it simple to quickly adapt and dynamically set up Public Safety networks even in rural areas where there is no coverage of a macrocellular network.

3.2 What are Public Safety Networks?

In the role model of 3GPP, a Public Safety network is a network providing communication services to public safety entities such as police, firefighters, and civil defense or paramedic services. Depending on the situation in the country of deployment, such networks can also be used by commercially operated security firms, for example, providing security services at airports or at company campuses.

The very first public safety communication networks were based on direct communication between an officer and the dispatcher located in a command center close by. These networks were using specially developed and mostly proprietary technology and special frequency bands for communication. They were isolated solutions, in the worst case not even interoperable across city borders. Another major drawback of this technology was the tight linkage to a single supplier with all the downsides of pricing, unavailability of features, and delivery problems.

As these networks were dedicated to official use only and were strictly governed by a dispatcher located in a command center, they inherently offered priority and preemption like mechanisms by arbitrating communication requests (usually a request to talk) via the dispatcher. The dispatcher was in control of the floor, i.e., deciding who has the right to talk next. Since the mode of communication was mostly “direct communication” mode, these networks also offered intrinsic reliability against network failures, as only the command center and the officer’s “walkie-talkie” devices were involved in the communication. Even in case the command center failed, officers were still able to communicate directly to each other. One disadvantage of this direct communication mode was the limited coverage. Soon relay nodes and other network infrastructure equipment were rolled out to extend the communication range, but also adding additional points of failure.

With the upcoming cellular communication systems and the widespread deployment of these networks the interest of public safety authorities to use these technologies was raised, as these networks offer lower deployment costs, multivendor support and with, for example, Global System for Mobile Communications (GSM) growing global coverage.

In parallel to the upcoming second-generation cellular systems, also the development of digital Public Safety communication started in the United States with APCO P.25 and in Europe with TETRA. These systems reduced the fragmentation of the Public Safety communication market quite significantly. P.25 is deployed in more than 50 countries among these are United States, Canada, Australia, New Zealand, Brazil, India, and Russia, while TETRA is used in more than 100 countries, for example, in Europe, Middle East, Africa, Asia Pacific, and Latin America. On a global scale market fragmentation persisted as P.25 and TETRA are not interoperable.

In the mid-1990s of the 20th century a first attempt was made to use GSM for public safety communication. When starting work on TETRA in Europe it was investigated whether to reuse GSM, but it turned out that GSM was missing some important features at that time. Operation on certain frequency bands was not possible and priority/preemption mechanisms were still in their infancy at that time. As a consequence, in Europe, the dedicated cellular TETRA network for public safety communication was standardized, which is nowadays widely adopted. There is one noteworthy exception. Mid of the nineties the GSM technology was enhanced to provide communication services for railways (GSM-R), which have to some extent similar communication needs as public safety authorities. The main reason this succeeded and has been even a success outside of Europe, for example in China, was the radio spectrum dedicated for railways being adjacent to the European GSM 900 frequency band for commercial networks. Thus, no significant changes to the radio system were required and the frequency band was large enough to cope with the traffic demand, without implementation of elaborated priority and preemption mechanisms from the beginning.

With the evolution of GSM from a voice-only to a data-centric network and in parallel moving to a global standardization organization (the 3GPP), the initial problems to make use of 3GPP technology for public safety communication began to disappear. For example, Universal Mobile Telecommunications System (UMTS) and LTE are deployed in a large number of countries around the globe and operating in many different frequency bands. LTE even allows operation on fragmented frequency bands at the same time.

3.3 LTE meets Demands of Public Safety Networks

Besides cost aspects there are many features LTE can already provide for Public Safety use cases without any upgrade. LTE offers interoperability between network equipment of different device and infrastructure manufacturers and between different networks, either national or international (known as roaming), very important in regions such as Europe where networks will likely be operated on a per country basis. Provided roaming agreements between countries exist, users of a Public Safety network in one country will be able to use Public Safety network infrastructure in other countries too. LTE also offers “state-of-the-art” authorization, authentication, and encryption mechanisms ready to be used for Public Safety communication. LTE allows the user to be authenticated toward the network, but also the network to be authenticated toward the user, effectively protecting eavesdropping attacks on Public Safety users.

An intrinsic strength of LTE is the openness of used security standards (for details see 3GPP TS 33.401 [4]) and the large number of security experts monitoring for security breaches and backdoors, providing updates to the standards before these security gaps can be exploited. For example, long time before the first encryption algorithm A5/1 was hacked the new algorithm A5/3 was defined by 3GPP. Owing to the openness of the standards and the global participation from many countries, chances of backdoors implemented in the standards by “interested” parties are less likely to succeed. Even though the parts standardized by 3GPP, especially the communication between device and network, can be considered fairly safe 3GPP networks rely on backhaul and interdomain security where special care has to be taken to prevent attacks.

LTE allows for flexible network sharing mechanisms (see 3GPP TS 23.251 [5]) by which operators, either commercial or Public Safety ones, can share parts of their networks to a certain extent. Most common scenario is Radio Access Network (RAN) sharing where different operators use dedicated core network equipment but share radio equipment with other operators. This allows for reducing deployment costs, but also to overcome gaps in radio coverage.

Priority and pre-emption mechanisms initially designed for disaster scenarios such as tsunamis, earthquakes, and typhoons allow important communication to succeed in case of network overload. These are already in-built features specified for LTE thus they can be easily re-used for Public Safety networks.

LTE provides quality of service on different levels such as per subscriber, per service, or per application. This allows traffic with high requirements on throughput and latency, for example, video streaming, to receive preferential handling over ordinary data transfer.

This has led to the conclusion that only very few features were missing from LTE to allow Public Safety communication. These features were taken up by 3GPP into their work program from Release-12 onwards. The features are concretely: direct mode of communication (for details see Chapter 4 and 3GPP TS 23.303 [6]), group communication (for details see Chapter 5 and 3GPP TS 23.468 [7]), and the Mission Critical Push to Talk (MCPTT) (targeted for 3GPP Release 13, see 3GPP TS 22.179 [8]) service. These additional features can provide a resource efficient group communication mimicking the behavior of "push to talk (PTT)" speech communication of legacy public safety systems. Besides the MCPTT service, other applications can also make use of the enablers specified by 3GPP.

3.4 Wide Range of LTE Devices for Public Safety

As pointed out earlier with the adoption of LTE as radio technology for public safety networks and the implementation of functionalities required to support ProSe or GCSE in the chipsets, it is quite likely that prices for public safety LTE devices will decrease and it also allows various other players to enter the market for public safety devices.

This is especially the case for non- or semi-ruggedized devices where the market already offers semi-ruggedized versions of phones for some time.

Public safety devices are available based on smartphone technology, thus they are able to offer more than just voice, video, group communication, or device-to-device communication, but also applications that enable to streamline the work flow of police officers. Figure 3.1 shows an LTE-based Public Safety tablet from Harris.

LTE will not only change the technical ecosystem but also the economical conditions to bring up interesting new use cases and varieties of devices.

For less harsh operating environments it can be anticipated to use ordinary smartphones or tablets with a few in-built applications to support Public Safety communication. With the exception of mechanical resilience, the boundaries between the highly specialized Public Safety devices and ordinary phones will begin to disappear.

It is expected that Public Safety mobile devices will not only include LTE defined functionality to support Public Safety communication, but also, depending on the region the device is used, TETRA or P.25 functionality to provide service where no LTE coverage is available – a likely scenario during the rollout of LTE Public Safety systems. The interworking between these two applications is out of scope of the 3GPP work and is left to the individual device manufacturer and national/regional regulation.

Figure 3.1 Harris RF-3590 LTE Public Safety Tablet

3.5 Standalone versus Shared Deployments

In most of the cases, Public Safety networks have been designed as standalone networks, usually deployed by national authorities or parts of the government. By doing so it was rather simple to be in full control of the network assuring privacy and secrecy. Deploying a network this way comes with high costs for providing a high quality, high reliable, for being fully government controlled network in the end.

As expected, this is the most expensive way of providing Public Safety networks, not being able to fully assess the installation costs in the beginning. Thus, in many countries the initial cost assessments for the final deployment of legacy public safety systems with coverage in all relevant areas were exceeded significantly in the end.

To overcome such a situation, commercial mobile operators were also confronted with 3GPP developed RAN sharing mechanisms allowing operators to share radio base stations and implicitly also sites or part of sites where base stations are physically deployed. If a Public Safety network operator has a sharing agreement with national mobile operators he benefits from the combined coverage and capacity of these networks, not only in areas where one network may have fringe coverage but also in areas where peak traffic is to be expected such as densely populated city centers. With (national) roaming agreements in place the

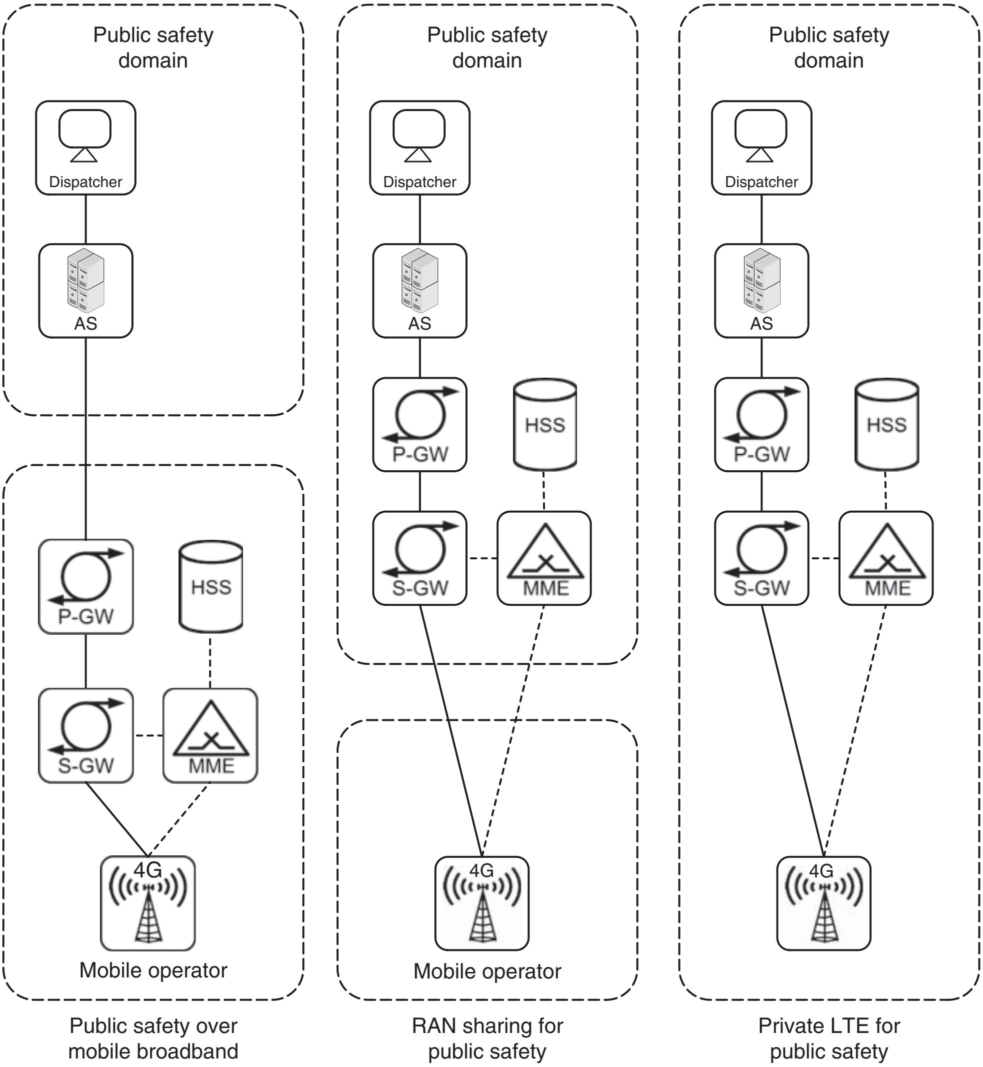

Figure 3.2 Examples of deployment options

Public Safety network operator could even make use of the infrastructure of commercial operators in certain areas without the need to deploy its own infrastructure. Figure 3.2 shows the examples of deployment options, ranging from a fully mobile network operator-hosted deployment scenario to a dedicated, standalone Public Safety deployment scenario.

Another benefit comes with the higher network/service availability and reliability when using more than one network. It reduces the probability of outages caused by technical problems by the number of operators involved, provided these operators all have an independent infrastructure in the area.

3.6 Interworking

3.6.1 Device Aspects

It is expected that an LTE-based public safety device (in terms of 3GPP the UE) will also provide legacy network support, for example, for TETRA or P.25. The working assumption is that the decision which of the two networks to use will be controlled by the application running on the UE. Even if 3GPP is going to specify the MCPTT application, it does not have a mandate to work on topics outside of its scope, that is, the 3GPP-standardized MCPTT application will not specify in detail the interworking to P.25 or TETRA systems.

But of course, the 3GPP standardized part will not be completely agnostic to the fact that there are other ways of communication for a public safety device. For example, to enable decisions when to switch over from network-based GCSE to ProSe-based communication necessary information from the lower 3GPP layers can be provided to the MCPTT application. Parts of this information in conjunction with information from the legacy part of the device can also be used to decide when to switch from LTE to P.25/TETRA and vice versa.

3.6.2 Network Aspects

The other interworking scenario is when a device currently connected via LTE and using MCPTT wants to communicate to one or several devices of which some might only be reachable via legacy public safety networks or vice versa. In this case the network has to ensure interworking on the different layers, for example, transport and application layer. For the application layer this might require protocol translation and transcoding capabilities in case devices are using different codecs.

References

[1] Global Mobile Suppliers Association (GSA): http://www.gsacom.com/.

[2] Telecommunications Industry Association (TIA) TR-8: http://www.tiaonline.org/all-standards/committees/tr-8.

[3] ETSI TCCE: http://www.etsi.org/technologies-clusters/technologies/tetra.

[4] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[5] 3GPP TS 23.251: "Network Sharing; Architecture and Functional Description".

[6] 3GPP TS 23.303: "Proximity-Based Services (ProSe)".

[7] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE_LTE)".

[8] 3GPP TS 22.179: "Mission Critical Push to Talk MCPTT (Release 13)".