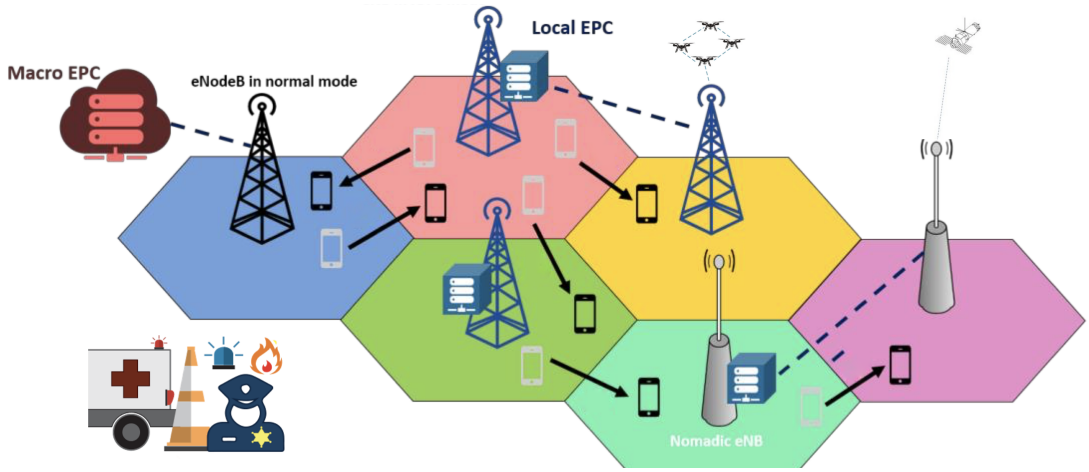
TÉCNICO LISBOA



Software-based Networking in Public Safety Networks

Daniela Santos Tinoco

Thesis to obtain the Master of Science Degree in

Telecommunications and Informatics Engineering

Supervisor: Prof. Rui António dos Santos Cruz

Examination Committee

Chairperson: Prof. Ricardo Jorge Fernandes Chaves
Supervisor: Prof. Rui António dos Santos Cruz
Member of the Committee: Prof. Fernando Henrique Côrte-Real Mira da Silva

September 2020

Acknowledgments

First of all, I have to thank to my parents and my brother for all the support and encouragement not only in the last few years but since ever I can remember. Without my family's support was not possible to complete this mark in my journey, so I have to thank you all.

Then, a huge part of my journey in Instituto Superior Tecnico (IST) were the colleagues that have done this journey with me. I'm lucky enough to assure that some of them became friends and that they are coming with me for life. And to them, an even special thank you for all the good times that we lived until now that, for sure, helped this journey becoming easier and funnier.

I would also like to acknowledge my dissertation supervisor Prof. Rui Santos Cruz for his insight, support, sharing of knowledge and big patience that has made this Thesis possible.

To each and every one of you – Thank you for being part of my journey.

Abstract

Public Safety Systems (PSSs) are an important part of each country's population protection and correspond to systems with which each country government worries about, but that does not always work in the best way. In times where technologies run our lives and changes the world, it seems that some of those vital systems for the society protection are being left behind and outdated. The Master Thesis described in this document intends to study the technologies, standards and solutions applicable to PSSs, with a focus on Software Defined Networking (SDN) and Network Function Virtualization (NFV) for the Public Safety Networks (PSNs), in order to present a viability study for the integration of those technologies in PSNs, and propose possible solutions for the "softwarization" of Public Protection and Disaster Relief (PPDR) communications systems.

Keywords

Public Safety Network (PSN); Emergency Networks; Public Protection and Disaster Relief (PPDR); Software Defined Networking (SDN); Network Function Virtualization (NFV); Network Slicing.

Resumo

Os sistemas de Proteção Pública são uma parte muito importante da proteção da população de cada país e correspondem a sistemas com os quais cada governo se preocupa, mas que nem sempre funcionam da melhor maneira. Em tempos em que a tecnologia domina as nossas vidas e muda o mundo, parece que alguns sistemas considerados vitais para a proteção da sociedade estão a ser deixados para trás e desatualizados. A Tese de Mestrado apresentada neste documento pretende estudar as tecnologias, standards e soluções aplicáveis aos Sistemas de Proteção Pública, com foco em redes definidas por software e virtualização de funções de rede para as Redes de Segurança Pública e apresentar um estudo de viabilidade para a integração destas tecnologias neste tipo de sistemas e propor possíveis soluções de "softwarização" de Sistemas de Comunicação para Proteção Pública e Assistência em Catástrofes.

Palavras Chave

Rede de Segurança Pública; Redes de Emergência; Proteção Pública e Assistência em Catástrofes; Redes Definidas por Software; Virtualização de Funções de Rede; Network Slicing.

Contents

1 Introduction **1**

1.1 Motivation . . . 3

1.2 Design Science Research Methodology (DSRM) . . . 4

1.3 Organization of the Document . . . 5

2 Theoretical Background and Literature Review **7**

2.1 Public Safety Networks . . . 9

2.1.1 Public Safety Networks Basic Requirements . . . 10

2.1.2 Today's Public Safety Networks . . . 11

2.1.2.A Land Mobile Radio System (LMRS) Networks . . . 12

2.1.2.B Long Term Evolution (LTE) Broadband . . . 16

2.1.2.C Public Safety System (PSS) Frequency Band . . . 18

2.1.3 Public Safety Networks Topology . . . 19

2.1.3.A Pre-Disaster Solutions . . . 19

2.1.3.B Post-Disaster Solutions . . . 19

2.2 Mobile Communication Technologies . . . 23

2.2.1 Commercial Networks Requirements . . . 23

2.2.2 Mobile Communications Technologies . . . 24

2.2.2.A LTE Proximity Services (ProSe) . . . 28

2.2.2.B Group Communication over LTE . . . 28

2.2.2.C Voice over LTE (VoLTE) . . . 29

2.2.3 Public Safety Technologies Vs. Cellular Communications Technologies . . . 32

2.3 Software Defined Networking . . . 33

2.3.1 SDN Controllers . . . 35

2.3.2 Southbound Protocols . . . 36

2.3.3 Network Functions Virtualization . . . 38

2.4 SDN, NFV and Network Slicing . . . 38

2.5 Public Safety Networks and Software Defined Networking . . . 41

2.6 Public Safety Networks and Network Slicing 43

3 Proposed Architecture **45**

3.1 LTE Networks and Operation for Public Safety 47

3.1.1 LTE Network Infrastructure and Spectrum Sharing 48

3.1.2 Isolated E-UTRAN Operation for Public Safety 50

3.2 Public Safety Networks and Network Slicing 51

3.3 Possible Architecture 52

4 Demonstration **55**

4.1 OpenAirInterface Emulator 57

4.2 CORE Emulator 58

4.3 Case studies 59

4.3.1 Earthquake Disaster Scenario 59

4.3.2 Mass Transportation Accident Disaster Scenario 61

5 Conclusion **63**

5.1 Conclusions 65

5.2 Limitations and Future Work 65

List of Figures

1.1 DSRM Process. . . . 4

2.1 PPDR system scheme. . . . 9
2.2 TETRA possible architecture . . . 14
2.3 FirstNet LTE network. . . . 18
2.4 Data transmission from sensors to data center. . . . 20
2.5 Emergency Network using walkie-talkies. . . . 20
2.6 Emergency Network using an LDRU. . . . 21
2.7 LDRU for Emergency . . . 21
2.8 Emergency Network using Satellite communications. . . . 22
2.9 Emergency Network using an Ad-hoc Network. . . . 23
2.10 GSM architecture . . . 25
2.11 UMTS architecture . . . 26
2.12 LTE architecture . . . 27
2.13 LTE ProSe architecture . . . 29
2.14 LTE Group Communication architecture . . . 30
2.15 LTE IMS . . . 30
2.16 SDN Network view. . . . 34
2.17 SDN Switch views . . . 35
2.18 SDN Controller architecture. . . . 36
2.19 OpenFlow vs. NETCONF. . . . 37
2.20 ONF SDN-based Slicing Architecture . . . 40
2.21 A Software-defined UAVNet. . . . 42

3.1 MOCN vs GWCN . . . 49
3.2 IOPS network formation. . . . 50
3.3 Possible solution architecture. . . . 53

4.1 Simulation architecture. 58
4.2 CORE Test Network. 59

List of Tables

2.1 PSN Standards comparison 16
2.2 Commercial Networks Comparison 32

Acronyms

1G	First Generation
2G	Second Generation
3GPP	Third Generation Partnership Project
3G	Third Generation
4G	Fourth Generation
5GPPP	5G Infrastructure Public Private Partnership
5G	Fifth Generation
API	Application Programming Interface
BMSC	Broadcast Multicast Service Center
BSC	Base Station Controller
BSS	Base Station System
BS	Base Station
BTS	Base Transceiver Statiobn
CAPEX	Capital Expenditures
CNMI	Central Network Management Interface
COW	Cell On Wheels
D-SDN	Decentralize-SDN
D2D	Device-to-Device Communication
DMO	Direct Mode Operation

DQPSK Differential Quaternary Phase Shift Keying

DSRM Design Science Research Methodology

E-UTRAN Evolved Universal Terrestrial Radio Access

EDGE Enhanced Datarates for GSM Evolution

EIR Equipment Identity Register

EPC Evolved Packet Core

EPS Evolved Packet System

ETSI European Telecommunications Standards Institute

FDD Frequency Division Duplex

FDMA Frequency Division Multiple Access

GCSE Group Communication System Enabler for LTE

GCS Group Communication System

GMSK Gaussian Minimum Shift Keying

GPRS General Packet Radio Service

GSM Global System for Mobile Communications

GUI Graphical User Interface

GWCN Gateway Core Network

HLR Home Location Register

HSS Home Subscriber Server

HeNB Home-eNBs

IMS MMTel IMS Multimedia Telephony Service

IMS IP Multimedia Subsystem

IOPS Isolated E-UTRAN Operation for Public Safety

IP Internet Protocol

ISDN Integrated Services Digital Network

ISI Inter-System Interface

IST Instituto Superior Tecnico

ITU-T ITU - Telecommunication

ITU International Telecommunication Union

LDRU Locally Deployed Resource Unit

LMRS Land Mobile Radio System

LTE-A LTE Advanced

LTE Long Term Evolution

MBMS GW MBMS Gateway

MBMS Multimedia Broadcast Multicast Service

MCE Multicast Coordination Entity

MCPTT Mission-Critical PTT

MIMO Multiple-input Multiple-Output

MME Mobility Management Entity

MMI Man Machine Interface

MOCN Multi-Operator Core Network

MRU Mobile Resource Unit

MS Mobile Station

MTA Mass Transportation Accident

NEOD Network Embedded On-line Disaster

NETCONF Network Configuration Protocol

NFV Network Function Virtualization

NGMN Next Generation Mobile Network Alliance

NSS Network Switching System

OAI OpenAirInterface

ODL OpenDayLight

OFDMA Orthogonal Frequency Division Multiple Access

OFDM Orthogonal Frequency Division Multiplexing

ONF Open Network Foundation

ONOS Open Network Operating System

OPEX Operational Expenditures

OSA OpenAirInterface Software Alliance

P-GW Packet Data Network Gateway

PDO Packet Data Optimized

PEI Peripheral Equipment Interface

PPDR Public Protection and Disaster Relief

PSN Public Safety Network

PSS Public Safety System

PSTN Public Switched Telephone Network

PTT Push To Talk

ProSe AS ProSe Application Server

ProSe LTE Proximity Services

QAM Quadrature Amplitude Modulation

QoS Quality Of Service

RAN Radio Access Network

RNC Radio Network Controller

RNS Radio Network System

RPC Remote Procedure Call

S-GW Service Gateway

SC-FDMA Single Carrier-FDMA

SD-RAN Software Defined RAN

SDN Software Defined Networking

SFC Service Function Chaining

SIRESP Sistema Integrado Redes de Emergência e Segurança de Portugal

SLA Service Level Agreement

SMS Short Message Service

SNMP Simple Network Management Protocol

SwMI Switching and Management Infrastructure

TD-CDMA Time Division-CDMA

TDD Time Division Duplex

TDMA Time Division Multiple Access

TEDS TETRA Enhanced Data Service

TETRA Terrestrial Trunked Radio

TE Terminal Equipment

TMO Trunk Mode Operation

UAVNet Unmanned Aerial Vehicle Network

UAV Unmanned Aerial Vehicle

UE User Equipment

UMTS Universal Mobile Telecommunication System

UTRAN UMTS Terrestrial Radio Access Network

UTRA Universal Terrestrial Radio Access

VLR Visitor Location Register

VM Virtual Machine

VoIP Voice over IP

VoLTE Voice over LTE

WCDMA Wideband Code Division Multiple Access

eMBMS evolved Multimedia Broadcast Multicast Service

eNB Evolve NodeBs

mmWave Milimetre-Wave

1

Introduction

Contents

1.1 Motivation 3

1.2 Design Science Research Methodology (DSRM) 4

1.3 Organization of the Document 5

Every day, somewhere in the world, some catastrophe of every kind happens, fires, road accidents, earthquakes, tsunamis, events that put populations and infrastructures in risk. These populations and infrastructures need to be protected and rescued/evacuated every time that it is necessary. To do this, citizens must be able to call for help and rescue teams must be able to communicate with citizens and with each other. To this end, each country must have its own Public Safety System (PSS), in order to protect its citizens in every accident and in every catastrophe that may occur.

The Public Protection and Disaster Relief (PPDR) System of each country is composed by law enforcement, emergency medical services, firefighting corporations, among other important services and by a Public Safety Network (PSN) that enables the emergency communications to allow to all of these forces just be able to communicate between them and with the population that they aim to protect. PPDR Systems are responsible for helping responding to emergency situations and, therefore, they are a major part in Public Safety.

Communication technologies and the Internet have evolved significantly in recent years and have reshaped the way we live and see the world. So, taking that into account, why are many PSNs still working with outdated technologies? With the evolution of technology, there are more and more solutions that can be applied in these types of systems, but due to the research and financial limitations of each country, the PSNs are not updated as often as desired.

1.1 Motivation

In Portugal, few people really knew what PSS was used to protect the population, until a huge tragedy occurred in 2017. On June 17, 2017 in Pedrogão Grande began what would become the biggest tragedy that would happen in Portugal in the last decades. A major forest fire consumed 53 thousand hectares of Portuguese land, affected more than 11 districts and took 66 lives, more than 1000 animals died, more than 250 citizens were injured and more than 500 houses were destroyed [1]. Since then, it seems that almost everyone already knows Sistema Integrado Redes de Emergência e Segurança de Portugal (SIRESP), not for the best reasons, but because the only thing the population hears is that SIRESP failed, then that year it failed again and in 2018 again ... and huge amounts of money (tens of millions of euros) are needed to " correct " the " flaws " (namely, lack of redundancy and resilience) of the current SIRESP PSS the infrastructure.

Therefore, it is necessary to understand how these emergency systems work, how important they are for the security of each country and what technologies can be added or used in these systems so that they can be improved and so that in the future it is possible to avoid or minimize tragedies in emergency scenarios. catastrophe and/or disaster, such as those that still happen around the world.

[1] https://www.jn.pt/nacional/interior/sintese-pedrogao-grande-sessenta-e-seis-mortos-mais-de-250-feridos-e-500-casas-destruidas-8991727.html

As such, the main objective of the Master's Thesis described in this document is to study all technologies, standards and solutions related and/or applicable to PSSs and to study recent/emerging technologies such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), in order to understand and evaluate if and how the integration of these technologies in the PSSs is viable and if they really bring advantages to these very important systems, and to propose possible solutions for the " softwarization " of PPDR communications systems.

1.2 Design Science Research Methodology (DSRM)

In order for the research process to be methodical and rigorous, we proposed to follow a DSRM. This problem solving methodology, proposed in [1], is based on an iterative process composed of six phases, and requires the development and evaluation of an "artifact" designed to solve a problem in a given area. This artifact can be represented in several forms, but in this case it will be the viability study that we carry out. Figure 1.1 illustrates the correspondence between DSRM phases and the steps of this work.

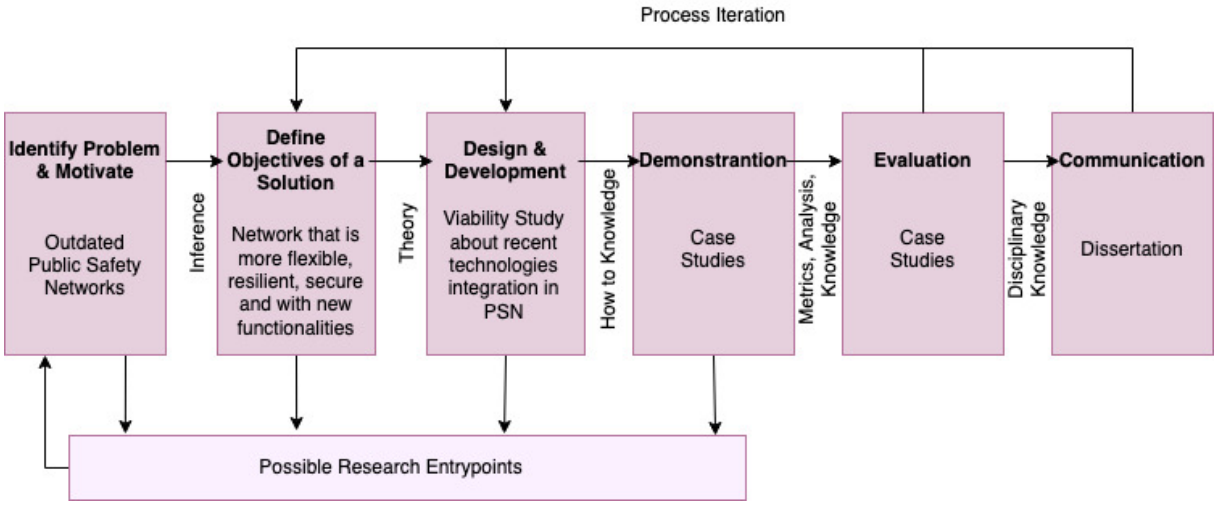


Figure 1.1: DSRM Process (adpated from [1])

.

The first phase of DSRM is Phase 1: problem identification and motivation. This phase was accomplished in the first chapter of this document. The problem of outdated Public Safety Networks is described and explained, justifying the importance that future solutions will have in preserving public safety.

The second DSRM phase is Phase 2: Define the goals for the solution. As stated further, the goals for a possible solution are the modernization of Public Safety Networks using recent cellular/mobile technologies combined with recent techniques such as Software Defined Networking (SDN) and Network

Function Virtualization (NFV).

The third phase of DSRM is Phase 3: Design and development. In this phase the solution/artifact will be design and defined.

The fourth phase of DSRM is Phase 4: Demonstration. Demonstration can be considered the first step for evaluating the artifact. In Demonstration phase will be described two case studies that will illustrate how the solution can be used in different emergency scenarios.

The fifth DSRM phase is Phase 5: Evaluation. The solution's evaluation will be made by seeing and justifying how the proposed architecture is able (or not) to respond to the scenarios different requirements.

The sixth phase of DSRM is Phase 6: Communication. This phase corresponds to the elaboration of this thesis and the document production, what is the problem, how is it relevant, the artifact and its importance, relevance and effectiveness are described.

1.3 Organization of the Document

This thesis is is organized as follows: Chapter 1 Introduction and motivation. In Chapter 2 is it possible to find the theoretical background and literature review that was made to gain theoretical bases to this thesis. In Chapter 3 will be described the theoretical architecture proposed. In Chapter 4 will be described the solution evaluation and in Chapter 5 will be described the conclusions obtain, system limitations and future work.

2

Theoretical Background and Literature Review

Contents

2.1 Public Safety Networks 9
2.2 Mobile Communication Technologies 23
2.3 Software Defined Networking 33
2.4 SDN, NFV and Network Slicing 38
2.5 Public Safety Networks and Software Defined Networking 41
2.6 Public Safety Networks and Network Slicing 43

In this chapter will be addressed the relevant background teams to this thesis. Here, it is possible to find information about Public Safety Network (PSN), about the cellular communication technologies available in the market, content about Software Defined Networking (SDN), Network Function Virtualization (NFV) and related techniques. Also, some projects related to this technologies and, in particular, with connection with PSN will be referred.

2.1 Public Safety Networks

As described in [2], "A Public Safety Network is a communication network used by emergency services, such as police, fire brigades and medical emergency services, to prevent or respond to incidents that endanger people and/or property".

PSNs are not "mass networks" but are indeed dedicated networks and have a mission, usually critical, where human lives and/or important infrastructures depend on the successful transmission of information.

PSSs can be divided in two major areas: 1. Prevention/Pre-disaster communication, and, 2. Post-disaster communication. Figure 2.1 illustrates the scheme of how a PPDR system should work.

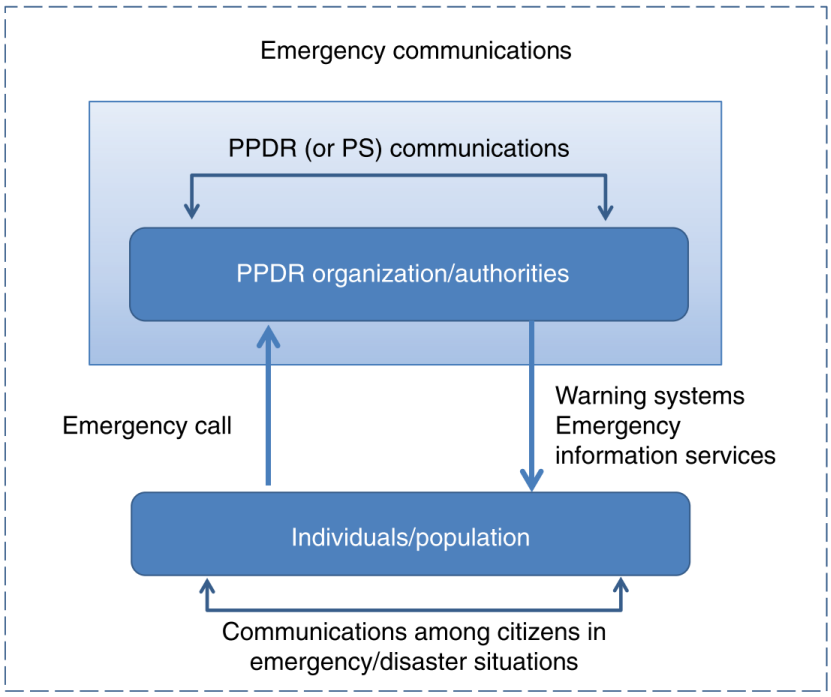


Figure 2.1: PPDR system scheme. Source: [3]

Pre-disaster communication is based on prior planning and reorganization of the communication network for planned/scheduled events, such as festivals or marathons, events that are likely to have a

large influx of people and the main tasks of this type of communication is to send notices/alerts to the population of certain areas, as soon as some type of potential natural disaster is detected affecting the areas where the events occur and network planning.

Post-disaster communication attempts to respond to unexpected situations, such as fires, earthquakes, tsunamis, etc., where it is necessary to guarantee and restore the proper functioning of the communication network. After an unexpected disaster, network infrastructure can be severely damaged or even completely destroyed. In these cases, quick action is needed to ensure that survivors can make contact and ask for help [4].

2.1.1 Public Safety Networks Basic Requirements

The first requirement of a PSN is that this type of network never fails in a crisis, being always available and reliable. With systems in use, this is not always the case.

Today's emergency communications rely primarily on voice communication and mission-critical voice transfer, which means that time-related aspects of voice transmission are crucial features for emergency communications. PSSs must have the minimum delay that the technology used allows. But with the evolution of communication technologies, there are other resources that are becoming very useful, such as photography, videos and geolocation [5], but these are not yet fully integrated into today's networks.

Situations where PSN is needed, usually have a great diversity of people involved: citizens, rescue teams, medical teams, control center, among others. Teams with different objectives have different needs in terms of communication, so when planning and organizing a network like this, it is important to take into account all types of communication needed. The most important types of communication on a ac PSN are:

- Multicast (and Group communications), that will allow rescue teams to communicate between them and to communicate with the control center;
- Unicast, to make possible report events up in the hierarchy, being that these communications should have high priority in the network.

In order to make all these different types of communication possible, the main requirements of a PSN are geographic coverage, which must be very close to 100% in the affected area, robustness and reliability of the network, as well as network resilience. In cases where it is not possible to guarantee full geographical coverage, it is necessary to have the Device-to-Device Communication (D2D) mode, a type of communication where the devices communicate directly with each other (not through the network infrastructure). The resilience of the network can be affected by many external factors, such as the lack of energy and, therefore, another main requirement PSN is the source of electrical energy.

PSS cannot operate without electrical power, so it is extremely necessary to ensure that the PSS power source is stable and as much as possible independent of the power distribution network, so that the power supply is not affected by the catastrophe/disaster. It is also important to ensure the efficient use of energy, as in some disasters, the power supply can become a scarce resource with no expected return. To ensure the robustness, reliability and resilience of the network, it may be necessary to have more than enough devices on the network, so that fault tolerance is secure and there are some methods of redundancy (for example, having more sensors or more switches than necessary) [6–8].

Due to the enormity of possible scenarios in which a PSN can be used, this type of network must be able to adapt itself to all scenarios, and it must be a very flexible and scalable network, due to the fact that the number of users (more rescue team members and/or more devices) can increase exponentially from one moment to the next. And networks must be scalable at more than one level. PSNs must be able to transfer different amounts of traffic, which can increase or decrease at any time, must be able to handle different amounts of active network equipment and must be able to support different network protocols due to different equipment may use different protocols [9, 10].

2.1.2 Today's Public Safety Networks

As explained earlier, the pre-disaster and post-disaster communications must be considered in the PSNs, and today there are different solutions for each case, with regard to the PSN architecture. PSNs can be classified into two categories:

- **Traditional/legacy Land Mobile Radio System (LMRS) Networks:** they are based on wireless communication (specialized) systems and target terrestrial users (pedestrians or vehicles) who carry special mobile devices, such as digital radios or walkie-talkies. These types of systems use dedicated private networks that have been deployed for a specific purpose and also use a dedicated frequency spectrum, which provides more network control and high availability. These systems allow voice communication and small amounts of data transfer (but not broadband data) and have as their main objective the response to emergencies and critical communications, with the consequence of their main characteristics being: robustness, reliability and attempt at interoperability.

- **Evolved/future Long Term Evolution (LTE)-based Broadband Networks:** these systems have recently become the next technology to be used in PSSs. In addition to being more recent and with space to evolve technologically, nLTE-based networks allow very high data rates (which are not supported by any of the networks LMRS). They have as main benefits, comparing with LMRS networks, lower costs, lower latency, easy integration with other services, a fast evolution of the communication capacities and a better Quality Of Service (QoS). The main standardization project

with LTE technologies is being developed by Third Generation Partnership Project (3GPP) and is described later in this document [8].

Although D2D communication is not a PSN category, it is a technology that has been evolving and taking its place in emergency communications in the last few years. Thus, it is an important requirement as to whether it is a PSN based on LMRS or LTE. As explained before, the communication D2D is a great help in cases where the mobile network infrastructure does not work, either because there is no mobile coverage or because the infrastructure was damaged by the catastrophe. What this D2D technology does is to maintain wireless connectivity (with limited range, but sufficient in most scenarios) where there is no mobile service infrastructure available. The D2D technology also works when two devices want to establish a communication channel only between them, which allows high-speed communications and reduces the load on the mobile network infrastructure, if it exists. In PSS, communications D2D can be extremely useful because it allows discovery of devices when people are considered lost/missing, for example [11].

The following sections describe in more detail some of the LMRS networks, some of the LTE -based networks and some of the existing solutions for configuring and recovering PSNs.

2.1.2.A Land Mobile Radio System (LMRS) Networks

The current legacy LMRS networks are Terrestrial Trunked Radio (TETRA), TETRAPOL and APCO-25.

TETRA: The Second Generation (2G) TETRA system was born in 1995 and is a set of standards for LMRS networks published by European Telecommunications Standards Institute (ETSI) and is mostly used in European countries, including Portugal, where SIRESP is based on TETRA. TETRA allows the use of some different services, such as voice calls (individual or group calls) using the Push To Talk (PTT) mode that provides short call establishment times (less than 300 ms) without the need for dial destination addresses for data and voice transmission, although data transmission works at low data rates (typically 4.6 kbps per slot). TETRA also has some security features and some advanced radio features.

The services provided by TETRA are designed to meet the needs of three specific user groups: 1) Mobile Station (MS) radio users, who are mobile and travel within a certain zone, 2) dispatchers who use fixed terminals to access some features of the system and 3) network managers, responsible for the proper functioning and maintenance of the system.

TETRA uses the air interface in Time Division Multiple Access (TDMA) mode to achieve maximum spectral efficiency and also uses $\pi/4$-Differential Quaternary Phase Shift Keying (DQPSK) as a modulation scheme. The radio frequency carriers used by TETRA have bandwidth of25 kHz and each is divided into four time slots, providing four communication channels for each 25 kHz of bandwidth,

achieving the best spectral efficiency possible. The frequency bands used are 230-400 MHz, 410-430 MHz and 800 MHz, which allows for very large coverage ranges (tens of kilometers).
With TETRA, communications can work in three different ways: Direct Mode Operation (DMO), when users communicate directly with each other, if it is not possible to connect to a specific network infrastructure, at Trunk Mode Operation (TMO), when communications depend on a specific infrastructure, with communications in TMO mode having a coverage area greater than the previous mode and in Packet Data Optimized (PDO), a mode created to transfer data exclusively in packet switching mode.

TETRAPOL: TETRAPOL is a set of standards for LMRS networks, developed by French police forces in the late 1980s of the 20th century, but has not been recognized by any international standardization organization. Similar to TETRA, TETRAPOL offers some services such as voice calls (individual or group) that can be PTT or within a group, and within a group, one participant speaks and the others just listen, and these groups can be configured either statically or dynamically. TETRAPOL also provides wireless data transmission (albeit at low data rates), some security features, among others. Communication can be done by retransmission by one or more base stations or at DMO. According with the standards, TETRAPOL should operate at frequencies between 70 MHz and 520 MHz, but nowadays it only uses frequency bands between 380 MHz and 450 MHz. In order to obtain the best possible spectral efficiency, TETRAPOL uses the Frequency Division Multiple Access (FDMA) scheme and Gaussian Minimum Shift Keying (GMSK) modulation. Each TETRAPOL channel is divided into radio channels with a bandwidth of 12.5 kHz or 10 kHz and each radio channel of 25 kHz can host up to 2 voice channels. The propagation of the communication has two defined air interfaces: one air interface to operate below 150 MHz (VHF) and another air interface for operations above 150 MHz (UHF). As the TETRAPOL data service is limited, it can only be compared to TETRA Release 1 [2, 3].

APCO-25: APCO-25, also known as Project 25 (P-25) is the most widely used set of standards PSS in North America, which allows interconnection between all American Public Safety agencies and allows communication between teams of rescue in each emergency scenario. APCO-25 is applied in a LMRS network and as such, the devices used within the network are APCO-25 radios and legacy radios, and between APCO-25 radios the communication can be done in analog mode and digital mode, and between APCO-25 radios and legacy radios, communication must be done in analog mode. Analog communication mode has many limitations, which is why it is increasingly being replaced by digital communication mode, but not all devices support this transmission mode, so analog transmission mode is still being used until all devices on the network are capable of digital transmission. The APCO-25 offers services such as calls (group or individual calls), wireless data transfer, integrated voice and data, communication encryption and dynamic calls. Project-25 also maintains compatibility with analog systems, allowing direct operation with analog radios that operate

on the same frequency (without using network infrastructure). APCO-25 devices use 136 MHz–174 MHz (VHF), 403 MHz–512 MHz and 800 MHz spectrum bands and currently have two phases. In Phase 1, the air interface used the FDMA channel scheme and the channels have 12.5 kHz bandwidth. In Phase 2, the air interface uses the TDMA scheme and therefore Phase 2 dedicated equipment is not able to operate in Phase 1, but Phase 1 equipment can still operate in Phase 2 because FDMA is still compatible with provide a smooth transition and interoperability between phases [2, 12].

There are two possible types of TETRA network architecture. An architecture with a centralized infrastructure, where the management and control of the network are based on a central database and a distributed architecture where there is no central infrastructure, but copies of the database (used to manage and control the network) are distributed and stored in the different TETRA Base Station (BS). The first architecture is widely used, particularly on large TETRA networks because a centralized core infrastructure shows better performance, especially on large networks.

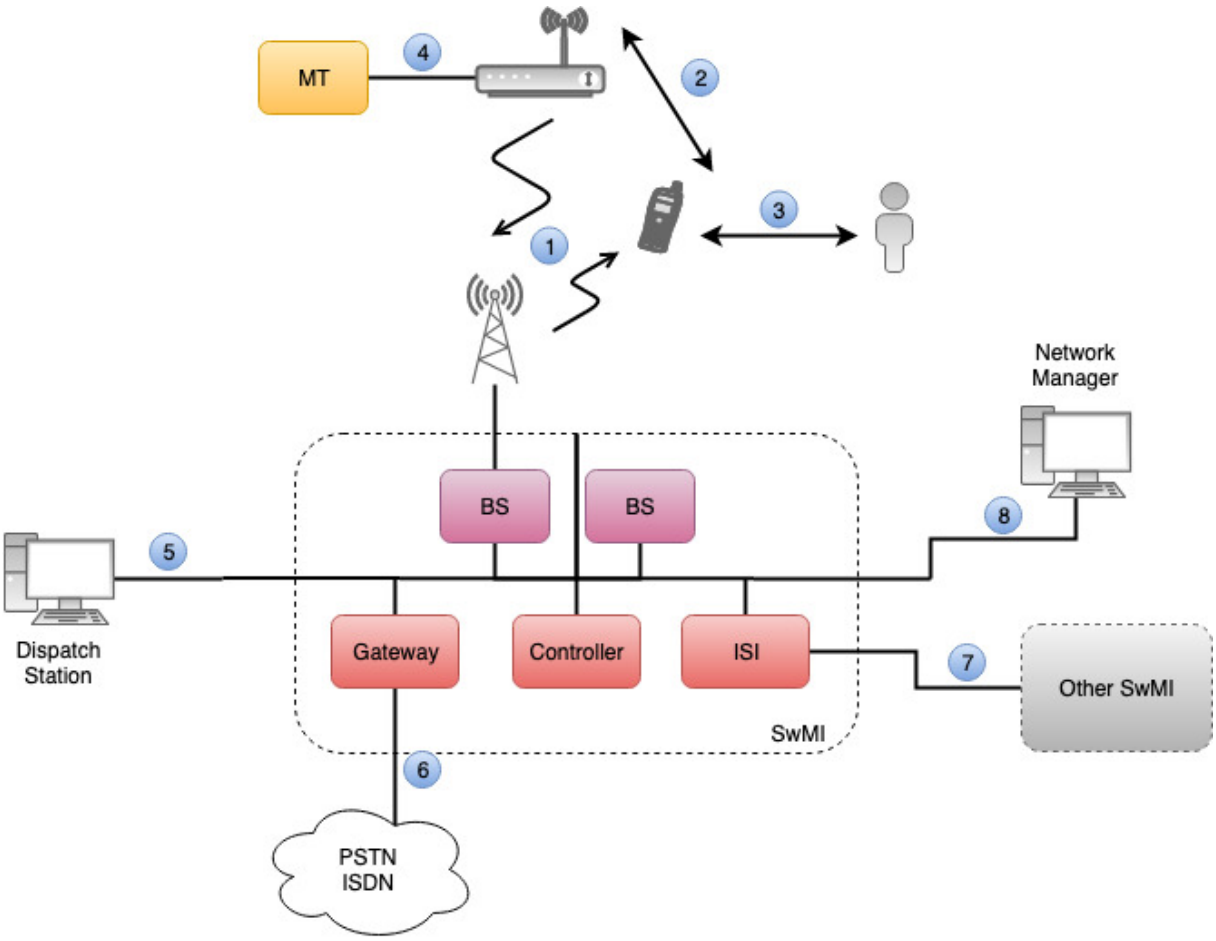


Figure 2.2: TETRA possible architecture.

In Figure 2.2 it is possible to observe an example of a TETRA network with a centralized core infrastructure. A system like this one presents a Switching and Management Infrastructure (SwMI), that harbor all the required components to network management as well as control and some relevant interfaces, being that not all of the interfaces are standardized by ETSI.

The most relevant interfaces are (see Fig. 2.2):

1. Air interface, that ensures communication between TETRA BS and Terminal Equipment (TE).
2. DMO air interface, that allows direct communication between TEs.
3. Man Machine Interface (MMI), interface targeted at TETRA terminals users. This interface is barely defined by ETSI.
4. Peripheral Equipment Interface (PEI), that allows connection between terminal radios and external equipment, supporting data transmission between them.
5. Remote Dispatcher Interface, interface that connects the network core to dispatch terminals.
6. External network Interface (such as Public Switched Telephone Network (PSTN), Integrated Services Digital Network (ISDN) and Internet Protocol (IP)).
7. Inter-System Interface (ISI), that enables interoperability between different TETRA networks, including different manufacturers networks.
8. Central Network Management Interface (CNMI), used to maintain the communication necessary to TETRA network correct operation. [13–16]

Due to technological innovation, TETRA had to continue to evolve over time (albeit slowly) and currently has two releases.

TETRA Release 1, supports three operation modes, 1. the Voice+Data (V+D) mode, that is the most used mode because it allows to transmit voice and data in the same channel (through the use of different slots), although the transmission at the same time is not possible. V+D mode uses the modulation scheme and the access control scheme explained above; 2. the DMO mode, previously mentioned, which also supports data and voice, but in different conditions; and, 3. the PDO mode, that is used to, occasionally, transmit high data volumes, such as location services data, when the users have that need.

TETRA Release 2, launched in 2005, kept the previously existing functions of Release 1 and added, among other things, a huge improvement, TETRA Enhanced Data Service (TEDS), which allows a higher flexibility and higher data rates. This is possible because TEDS, besides the previous modulation schemes, also uses higher order modulation, such as 4-Quadrature Amplitude Modulation (QAM), 16-QAM and 64-QAM and also uses channels with larger bandwidth, such as 25, 50, 100 and 150 kHz.

Theoretically, these features could improve the data rates up to 540 kbps, but in real life, channel bandwidth is limited typically at 50 kHz and the data rate is therefore limited to less then 100 kbps. TEDS is totally compatible with TETRA Release 1.

TMO also appears in TETRA Release 2 [2, 3, 12, 13, 16]. Table 2.1 provides a comparison of the four standards described in terms of their radio characteristics.

Table 2.1: PSN Standards comparison

	Medium Access	Carrier Bandwidth [kHz]	Channels/ Carrier	Frequencies [MHz]	Max. Data Rate [kbps]
TETRA	TDMA	25	4	380-400, 410-430, 800	28.8
TETRA - TEDS	TDMA	25, 50, 100, 150	4	380-400, 410-430, 800	100.0
TETRAPOL	FDMA	25	2	380-450	4.8
APCO-25	FDMA	25	2	136-174, 403-512	9.6

Even with all the progress of the PSN, there are still limitations to be overcome. Unfortunately, there is still no common " system " for all public safety organizations, and so, in each scenario, the big challenge is to link communication between different agencies in the field (not only at national level, but also at joint-international level, as a catastrophe scenario may involve different neighboring nations/states). Even with all the huge technological advances seen in communication systems for general public use (for example, a user can roam the world using voice and data), most PSN still use data communications 2G, or older technologies, even though Fourth Generation (4G) LTE systems are now common in most countries when it comes to commercial networks [9, 12].

2.1.2.B Long Term Evolution (LTE) Broadband

As stated before, the majority of PSS today still use old and outdated technologies, but now the first efforts are being made to integrate new mobile/cellular technologies into PSS. Typically, systems like TETRA use a dedicated private network to ensure the high availability and reliability of the network and the stagnation of PSS is due to the high cost of implementing an entirely new private and dedicated network for newer technologies like LTE, costs that cannot be borne by most national budgets.

The standards defined by 3GPP relate to the utilization of 4G LTE technology in Public Safety communications and in PSN. The 4G-LTE network uses a flexible air interface with low-latency and uses Frequency Division Duplex (FDD) and Time Division Duplex (TDD) as allocation methods in order to be able to support flexible channel bandwidth, which can vary between 1.4 MHz and 20 MHz (in both uplink and downlink communications). The difference between commercial LTE solutions and Public Safety LTE solutions is that LTE-based PSS should have greater availability and reliability, lower latency, different types of calls available, emergency calls, good quality communications, among other features

and must meet the PSN requirements described above.

These standards advise the utilization of Orthogonal Frequency Division Multiplexing (OFDM) scheme, and control of multiple access technologies to turn the transmissions more efficient, and also advises the use of Multiple-input Multiple-Output (MIMO) techniques in a way to improve the spectral efficiency.

Besides the LTE traditional features, 3GPP suggests some improvements specific for PSS, such as:

- Proximity Services (ProSe): LTE allows users to establish direct communication between two users using the D2D communication. The proximity services feature allows devices to discover who their neighbors are and allows them to establish optimized direct communication between them in three different ways: 1. Direct discovery, which allows the device to gather information about the surrounding devices and communicate directly with them; 2. Evolved Packet Core (EPC)-level discovery, where the device depends on the LTE network to discover it neighbours; and, 3. ProSe Relaying, service that allows to an User Equipment (UE) act as a relay between the E-UTRAN and one or more UE outside of the network coverage area, which will extend the coverage of the network.

- Group communication: allows an efficient exchange of voice and data between users of a certain group, in a controlled manner (similar to the normal PTT mode). For this, it was necessary to add a new resource to 4G LTE, Group Communication System Enabler for LTE (GCSE) LTE. This improvement includes a dedicated server in the architecture that decides which mode of data or voice transfer (unicast or broadcast) is indicated for a given situation;

- Mission critical PTT: a system that allows users to selectively and sequentially transmit messages between them, but when one of them is speaking, the only thing the others can do is listen, with permission to speak it is granted using priorities [17, 18].

The International Telecommunication Union (ITU) defined a standard spectrum allocation for PSS-LTE. The PSN-LTE should use frequencies in the 700 MHz range.

In 2018 there were already 19 countries working on the deployment of LTE-based PSNs, but Portugal was not one of them [2, 19], nor there is a perspective for that type of deployment in the medium term in this country.

The United States of America is one of the most developed countries in terms of Public Safety and the use of LTE-based PSS. Today they have the FirstNet system, a LTE-based broadband PSN that follows 3GPP standards. FirstNet's main functions are DMO, PTT, full duplex voice system, group calls, speaker identification, emergency alerts and good audio quality. FirstNet's components are the core network (EPC), Universal Mobile Telecommunication System (UMTS), mobile satellite system and many implantable systems.

FirstNet separates the LTE network into four different layers, as shown in Fig. 2.3. These layers are the Access devices, the Radio Access Network (RAN), that is, the layer that implements access radio technologies and allows the Access devices to connect to the Core Network, the Transport Backhaul that handles the connection between the Core Network and other subnetworks and the Core Network, which is the central part of this network and allows networked devices to use some of the available services [12].

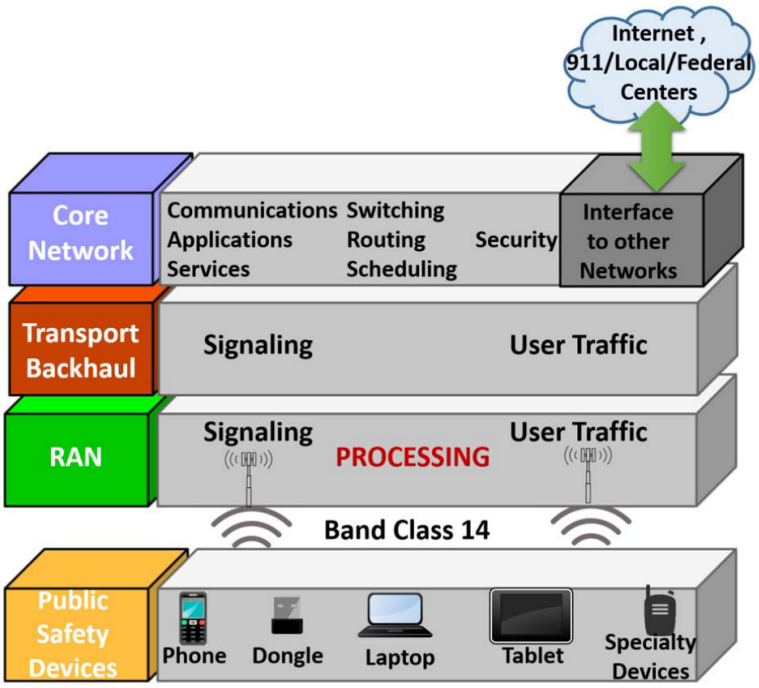


Figure 2.3: FirstNet LTE network. Source: [12]

2.1.2.C Public Safety System (PSS) Frequency Band

Each country has an entity responsible for allocating and defining the frequency band to be used by its PSS, although there are some guidelines from standardization entities such as ETSI and 3GPP. As previously noted, the frequency bands dedicated to PSS are allocated around the 400 MHz band in TETRA, TETRAPOL and APCO-25 and the 700 MHz band in LTE Broadband. It is possible to verify that, in general, the frequencies dedicated to emergency services are the lowest in which the technology in question can operate. This is because lower frequencies can propagate over greater distances and present better penetration through objects and obstacles, due to the greater wavelength that this type of waves presents. This allows for a larger coverage area with less infrastructure deployed in place when compared to higher frequency bands.

2.1.3 Public Safety Networks Topology

Nowadays, there are some different solutions that work in circumstances where it is necessary to complement and recover Public Safety Networks. In this section, some of the possible and most used topologies for this subject for pre-disaster communications and also for post-disaster communications will be described.

2.1.3.A Pre-Disaster Solutions

Pre-disaster communications have, as an important part, sending warnings to the population before any catastrophe happens. The possibility of a catastrophe occurring nowadays can be detected by sensors in the field that send periodic environmental information to a processing data center, where the sensor data is analyzed and analysts decide whether it is valuable information or not. If the information is relevant, warnings are sent to the people in the area who may be affected by the catastrophe. Today, communication between sensors and data centers takes place via wireline, wireless or via satellite, as represented in **??** and the warnings reach the population via wireline or wireless. Whether the warnings are sent via wireline or wireless, they are usually sent through a commercial network and there are service agreements between mobile phone operators and Governments that provide and guarantee the sending of these warnings if necessary. Some of the most used and relevant sensors today are seismic sensors, which detect possible earthquakes or tsunamis [4].

The major factor affecting pre-disaster communications is time. The warning must be issued and transmitted early enough to allow the population to take actions to help prevent or minimize possible damage from the catastrophe that is approaching [7].

2.1.3.B Post-Disaster Solutions

There are a few different strategies that can be used to ensure communication after a disaster, depending on the situation in question.

The use of walkie-talkies is considered the most reliable and appropriate form of communication, considering that majority of rescue teams are equipped with this type of technology. Walkie-talkies are portable radios that work wirelessly (without infrastructure). The frequency band of the radio spectrum is divided into channels and walkie-talkies tuned to the same channel are able to communicate between them.

Eventually, if the number of these devices increases, a data network capable of supporting the allocation of the necessary resources will be necessary for the use of walkie-talkies to be made available to everyone.

Walkie-talkies have some disadvantages such as the fact that they have limited battery capacity,

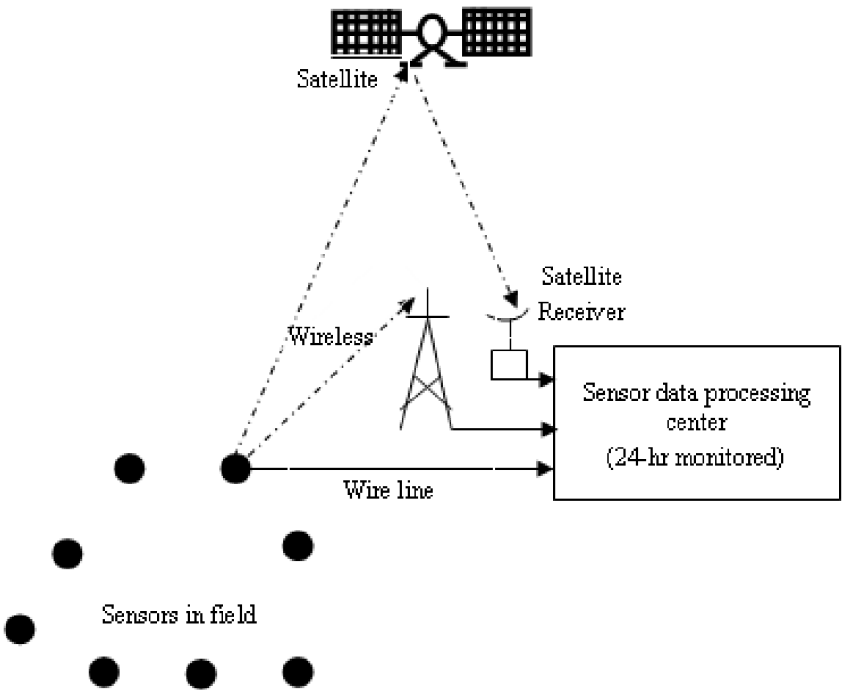


Figure 2.4: Data transmission from sensors to data center. Source: [4]

communication is not secure as everyone on the channel can hear the transmissions, each device must be manually tuned to the correct channel and is susceptible to interference as illustrated in Fig. 2.5.

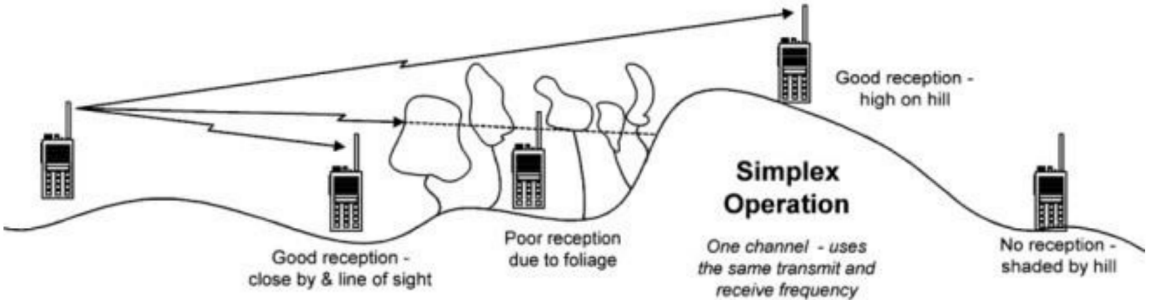


Figure 2.5: Emergency Network using walkie-talkies. Source: [7]

Another possible strategy is to use a Locally Deployed Resource Unit (LDRU). This strategy is only possible when most of the base stations are intact and only a few base stations have been destroyed in the entire affected area. In this way, the remaining functional base stations are used in conjunction with an added Mobile Resource Unit (MRU) that replaces the damaged base stations and configures the emergency network. It may also be necessary to change the transmission scheme (for example, change the frequency band in use or increase the power supply) in order to increase the signal strength and coverage in the affected area.

It is necessary to keep in mind that, for the population to be able to communicate with the emergency services, the emergency mode of regular mobile phones must be able to operate within the new transmission scheme. An example of this type of network is illustrated in Fig. 2.7a.

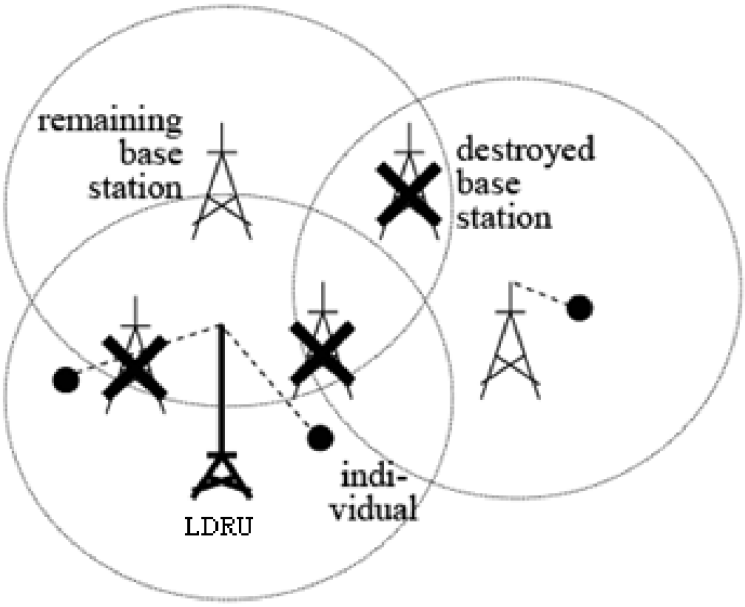
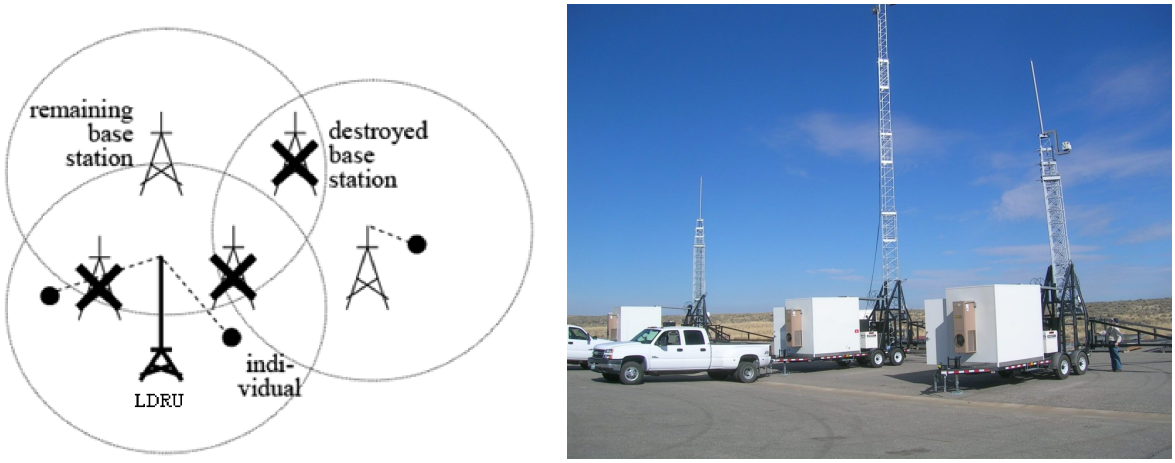


Figure 2.6: Emergency Network using an LDRU. Source: [4]



(a) Emergency Network using an LDRU.

(b) A LDRU COW (Cell on Wheels).

Figure 2.7: Use of LDRU for Emergency. Source: [4]

There are several types of LDRU, because basically a Locally Deployed Resource Unit (LDRU) is any unit that can be deployed on site in order to reestablish communications. One of these LDRU adaptations is called Cell On Wheels (COW), as illustrated in Fig. 2.7b. These types of units are cells (MRU) with wheels, so that they can be moved at any time to where necessary (as long as that location

has terrestrial access), and in useful time. These COWs have the advantage of being very compact, easily transportable and, the fact that they can be used for more than one purpose, for example, to create temporary local networks or to increase locally the capacity of an existing network. These devices are also cost-effective because two engineers are more than capable of setting up a COW [20].

Other recent versions of LDRU are the so-called Flying COWs using Unmanned Aerial Vehicles (UAVs). These vehicles can appear in many forms, such as balloons, drones or quadcopters, and they all carry a MRU to replace base station(s) that are not working or to provide coverage for difficult territory morphologies due to orographic obstacles [12, 21].

The complementary use of a system based on satellite communication is also possible. This alternative should be used when all, or almost all of the base stations in a wide area are inoperable, as shown by Fig. 2.8. To make this option feasible, the cell phones of the rescue team members and of the population need to be compatible with satellite communications and currently, although some members of the rescue teams have mobile equipment that meet this criteria, the majority of the population does not have equipment with satellite capabilities. This option is one of the most reliable because the satellite coverage is broader and reaches places where other types of communication do not offer coverage, such as mountain tops or deep forests.

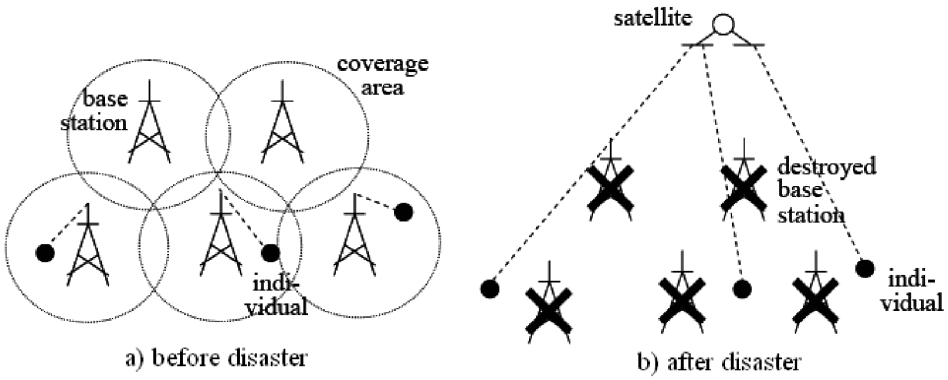


Figure 2.8: Emergency Network using Satellite communications. Source: [4]

In some cases, it is not possible to use a satellite-based network because it can be very expensive. In cases like this, one of the alternatives is to use an Ad-hoc network. Ad-hoc networks are formed of mobile devices close to each other (devices of the population and/or rescue teams) and which are configured to allow them to connect with each other and connect to phones capable of satellite (usually transported by rescue teams) or to an LDRU, forming an Ad-hoc network, as illustrated in Fig. 2.9. This type of network has some advantages over other types, such as the fact that the network is self-sufficient, quick to deploy and easily re-configurable [2, 4, 7].

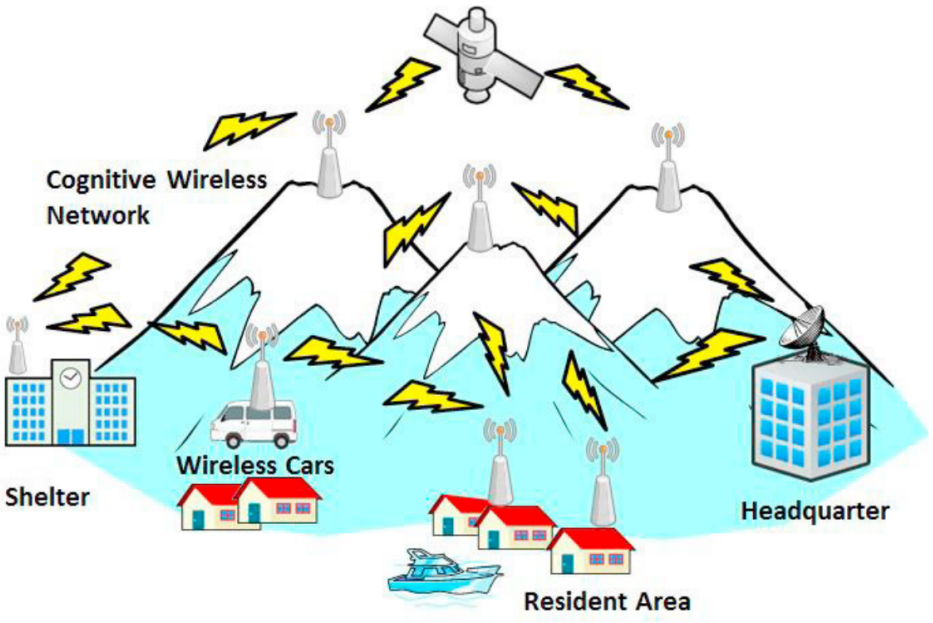


Figure 2.9: Emergency Network using an Ad-hoc Network. Source: [4]

2.2 Mobile Communication Technologies

Mobile communication technologies are developed primarily for use in commercial communications networks. Commercial networks are ”mass networks”, which host millions of users at the same time. Networks of this type are constantly updated regarding the technologies in use. Looking at the history of telecommunications, it is possible to verify that the evolution is continuous from the first day, regardless of the associated costs that this development and evolution entails.

2.2.1 Commercial Networks Requirements

Commercial networks are networks that generate revenue for the service providers that own them, so this type of network has to meet certain criteria so that users/customers are satisfied with the contracted service and so that the networks can operate the best way. Starting with the coverage requirement, operators are interested in providing coverage for areas with a high population percentage, that is, an area with many customers, so that most of the network infrastructure is concentrated and directed to these areas so that the service becomes profitable. In areas with a lower population percentage, if there is no stimulus given by the Government, there will probably be no service coverage in these areas and the population does not have access to these mobile services because the revenue from these users vs. the cost of the necessary infrastructure is not profitable.

In this type of network, the allocation of frequencies must be planned in advance throughout the

whole system, as this allocation is fixed and the service provider wants to maximize the number of users of the system, as more users means more revenue. To do this, along with the coverage requirement, more base stations and more smaller cells are used in order to increase the network infrastructure and certain modulation and frequency planning techniques are also used so that it is possible to increase the number of users simultaneously in the network and reduce possible interference.

As already mentioned, the use of commercial networks generates revenue for service providers, so it is necessary for customers to authenticate themselves so that the use of services can be controlled and invoiced to each customer.

Finally, operators can also offer some complementary services that add value to the primary voice call service, such as Short Message Service (SMS), call forwarding, conferences, among others.

2.2.2 Mobile Communications Technologies

In the 80's appear the First Generation (1G), where communications only allow voice transfer in analog mode with rates close to 2.5 kbit/s.

In the 90s, 2G appeared, which revolutionized the communications of the time. 2G Global System for Mobile Communications (GSM) allows voice transfer with good audio quality and reliable wireless communications, data transfer and Short Message Service (SMS). GSM uses Gaussian Minimum Shift Keying (GMSK) as a modulation scheme and Time Division Multiple Access (TDMA) as an access scheme and was originally designed to operate in the 900 MHz frequency band, with 125 channels of 200 kHz bandwidth each, but due to high utilization, it was later adapted to operate also in the 1800 MHz frequency band, which added 375 channels of 200 kHz each. Currently, GSM is capable of operating on more bands, as described in the table below [22–24]. In the original GSM, all voice and data are circuit-switched transmitted, which means that the necessary resources are previously allocated for each necessary transmission. This type of transmission is good for voice, because it allows low interference, has fixed bandwidth per transmission and the delay is constant, but it is less advantageous in relation to data transmissions, whose datarates are 9.6 kbit/s or 14.4 kbit/s.

Subsequently, General Packet Radio Service (GPRS) was developed in order to improve GSM data transport and Enhanced Datarates for GSM Evolution (EDGE) to increase data transfer speed and latency. GPRS changed the form of data transmission was made, using packet-switched transmission that allows the information to be divided into smaller packages and to allocate the necessary bandwidth flexibly, with theoretical datarates close to 170 kbit/s.

In Fig. 2.10 you can see a simplified GSM architecture. The GSM architecture is divided into two main subsystems, Base Station System (BSS) and Network Switching System (NSS), with BSS consisting of one or more Base Transceiver Statiobn (BTS) and one Base Station Controller (BSC), is connected to MS via the air interface and is responsible for managing radio connections, for encoding and decod-

ing the transmission and for adapting the transmission rate. The NSS also houses some important databases like Equipment Identity Register (EIR), Home Location Register (HLR) and Visitor Location Register (VLR) [25, 26].

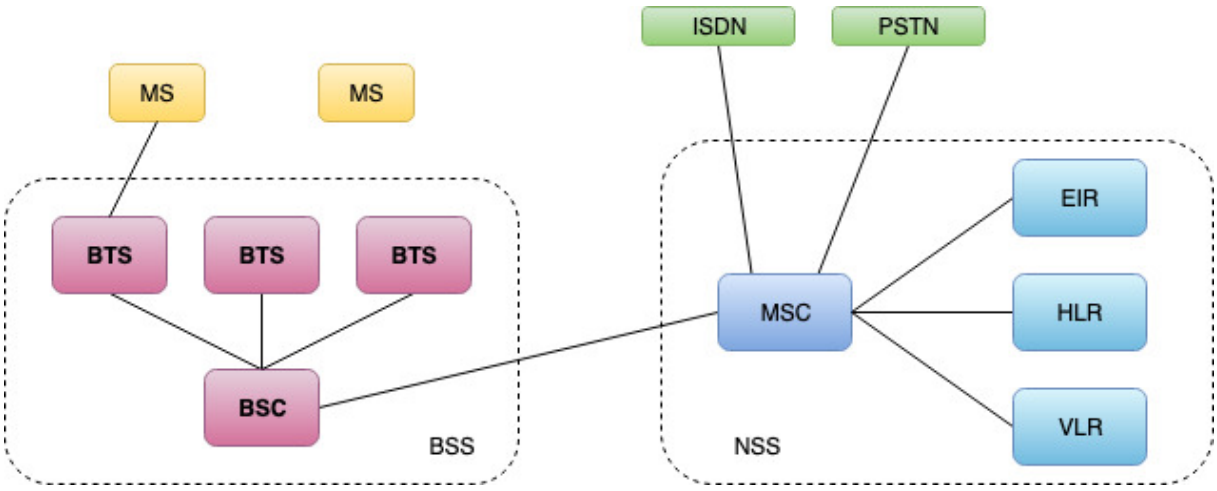


Figure 2.10: GSM architecture.

At the end of the 1990s, Third Generation (3G)/Universal Mobile Telecommunication System (UMTS) emerged. UMTS was designed taking into account a universal infrastructure that can accommodate existing and future services without the need to replace the entire infrastructure with each change. The main feature of this infrastructure architecture is the separation of access technology, transport technology, service technology and user applications. The main differences between GSM and UMTS are the redesigned Radio Access Network (RAN), now called UMTS Terrestrial Radio Access Network (UTRAN), and the best spectral efficiency. UMTS, also called Universal Terrestrial Radio Access (UTRA), combines the properties of the circuit switched voice network with the properties of the packet switched data network and, to do this, reuses some features of GSM and GPRS. To improve spectral efficiency, 3G uses Wideband Code Division Multiple Access (WCDMA) and Time Division-CDMA (TD-CDMA) and the operator's bandwidth has increased, which has improved the maximum data rate that can be achieved which is 2 Mbit/s in internal communications and low range and 384 kbit/s in external suburban communications [27]. Initially, UMTS was designed to operate in the 2 GHz frequency range and was later adapted to operate on more frequencies, including the frequency range where 2G operates and the ranges described in [28] as can be seen in Table 2.2 (Release 3GPP TS 25.101 v16.1.0) [25, 29, 30].

In Fig. 2.11 is possible to see a simplified UMTS architecture. This architecture can be divided into two main subsystems, UTRAN and Core Network. UTRAN consists of one or more Radio Network System (RNS) and each RNS has one or more NodeB and one Radio Network Controller (RNC) and connects to UE via the air interface. The Core Network has two main parts, one dedicated to circuit

switching and the other dedicated to packet switching and also has some databases and is responsible for switching and subscriber control.

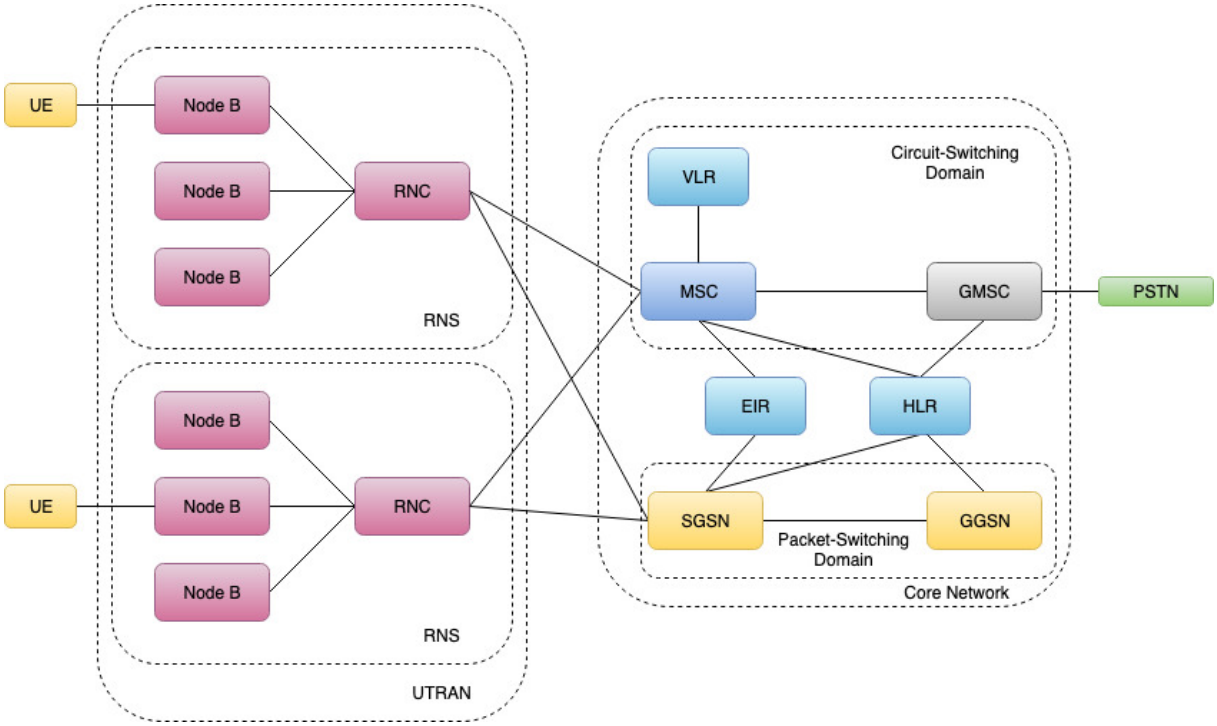


Figure 2.11: UMTS architecture.

Long Term Evolution (LTE), popularly (and mistakenly) known as 4G, was launched in 2004 as a "3G Long Term Evolution", driven by the need to bring new and more complex services to mobile communications. It is necessary to note that 4G is a mobile generation and LTE is the technology used to meet the requirements defined by the mobile generation and it is not the only possible technology to achieve these requirements, but it is the most relevant.

The biggest change presented in the system architecture was the fact that circuit switching will no longer be used, and LTE is a pure IP-based packet switched system. As you can see in the architecture shown in Fig. 2.12, the architecture of a 4G LTE system is divided into two main subsystems:

- Evolved Universal Terrestrial Radio Access (E-UTRAN): E-UTRAN, an evolution of UTRAN shown in UMTS, is the access network for a 4G LTE network and its main components are User Equipment (UE) (cellular terminals), Evolve NodeBss (eNBs) for macro-cells and Home-eNBss (HeNBs) for femto-cells. The main functions of a eNB are radio source management, routing user plan data to the serving gateway, scheduling resources to user equipment, transmitting paging and broadcast messages, measuring, reporting configuration for terminals mobility and scheduling.
- EPC: EPC has come to replace the packet switched domain in UMTS and has a flat IP subsystem design so that it can support high packet data rates with low latency. This entity is responsible

for handling mobility management functions and sessions and also contains Mobility Management Entity (MME), responsible for control management (such as location management), and is responsible for Service Gateway (S-GW), which manages all traffic E-UTRAN created by the user for EPC and vice versa and a Packet Data Network Gateway (P-GW) that is responsible for IP connectivity to external IP networks.

Initial LTE promised data rates until 100 Mbit/s in downlink communications and 50 Mbit/s in downlink communications, an even lower latency and a better spectral efficiency. Communication channels can now have 6 different bandwidth (1,4/3/5/10/15/20 MHz), and the access scheme is different to an uplink communication – Single Carrier-FDMA (SC-FDMA) – and to a downlink communication – Orthogonal Frequency Division Multiple Access (OFDMA).

Later, and to achieve the actual standards defined for the 4G mobile generation, LTE Advanced (LTE-A) was developed and it allowed to achieve data rates over 1000 Mbit/s in downlink communications and over 500 Mbit/s in uplink communications, and the maximum aggregated bandwidth is now 100 MHz, in a maximum of 5 carriers.

Initially, the frequency band allocated to LTE in Europe was the 800 MHz, 900 MHz, 1800 MHz, 2100 MHz and 2600 MHz. Later, there were added more frequency bands, such as the 450 MHz, 700 MHz – 900 MHz, 2.3 GHz – 2.4 GHz and 3400 MHz – 4200 MHz. In [31] is possible to see the detailed frequency bands that are available for LTE use [32, 33].

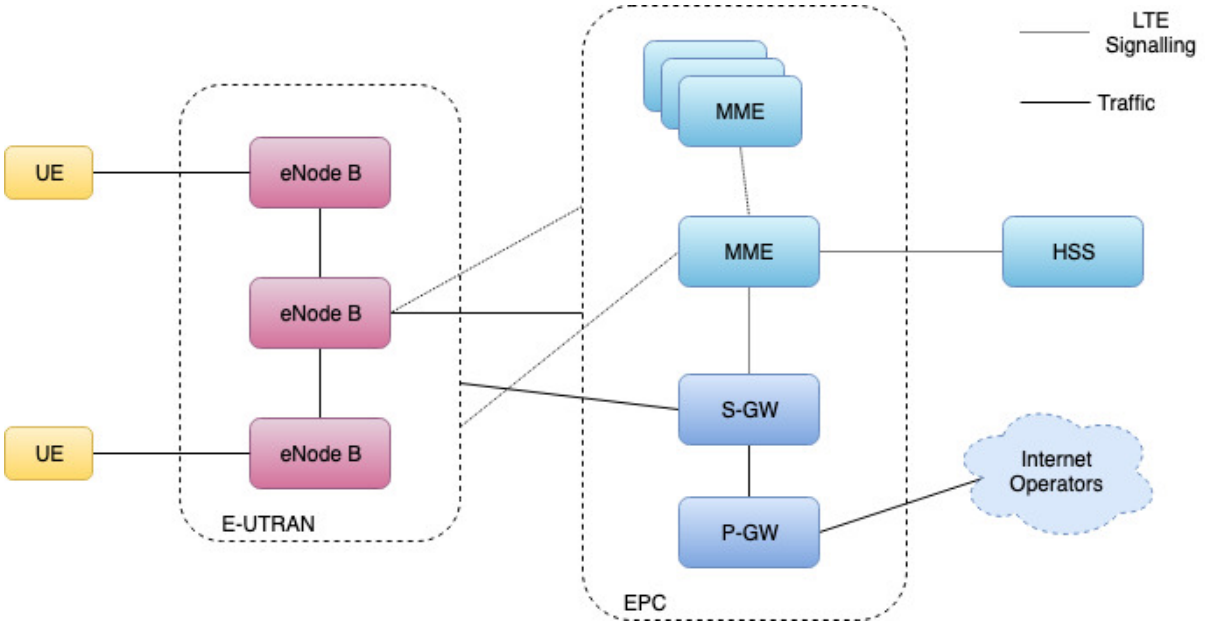


Figure 2.12: LTE architecture.

It was mentioned before that exist some LTE features (LTE inherent or post-added features) that are considered extremely important and extremely useful to Public Safety Network (PSN), but that are not

exclusive of PSN because these features can become very useful being an extra service that add value to service provider offer and become a source of revenues for the commercial network operators.

2.2.2.A LTE Proximity Services (ProSe)

One of the most essential requirements when creating a PSN-LTE network was the implementation of D2D communications and proximity services. The main function of LTE ProSe is to allow physically close devices to ”find” and communicate with each other without network support, which is a great advantage because it reduces the load on the network, saves network resources and radio resources, reduces communication latency and allows communication outside the network's coverage area.

It is possible to divideLTE ProSe into three main functions:

- ProSe Direct Discovery, where ProSe-enabled UE transmit/receive periodical signals and collect information about neighbor UE. This capability allows them to establish a direct communication channel between them. A ProSe-enable device is a UE that have permission to use ProSe services and this information is registered in Home Subscriber Server (HSS) along with all subscription information about each device.
- EPC-level discovery, where a UE is network dependent to discover UE neighbours.
- ProSe relaying allows extend network coverage area using a UE as a relay between E-UTRAN and an outside of the network UE, giving network coverage to this last UE or a UE can act as a relay between other two UE that are not in each other's range to communicate in a DMO.

For the ProSe services to work, it is possible to observe in Fig. 2.13 that it was necessary to make some changes to the LTE architecture, adding two new entities: ProSe Function, responsible for provide all necessary ProSe services, such as authentication, authorization request and data management, and ProSe Application Server (ProSe AS) that manages all connections at the application layer. More information about LTE Proximity Services (ProSe) can be found in 3GPP TS 23.303 [2, 17, 18, 34].

2.2.2.B Group Communication over LTE

Group Communication is considered the best way to deliver all types of data between multiple users (which can be mobile users on the scene or fixed users in a control center) simultaneously and LTE is a great enabler for this type of service because it is a broadband technology. To enable group communications, 3GPP define two main subareas:

- Group Communication System Enabler for LTE (GCSE) which focuses on the efficiency of data delivery in a group of users. This group needs management functions like parallel communication management and group management and this function is provided by the UE application layer and

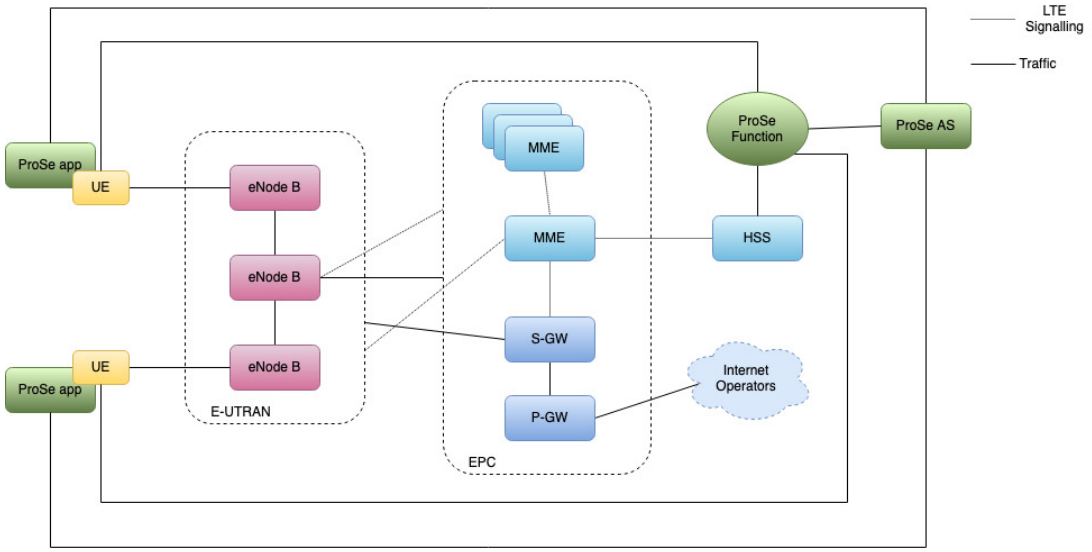


Figure 2.13: LTE Proximity Services (ProSe) architecture.

by the Group Communication System (GCS) AS in the network. GCSE services can be delivered by unicast, where Evolved Packet System (EPS) bearers deliver content to each UE individually or evolved Multimedia Broadcast Multicast Service (eMBMS), where content is delivered to UE using Multimedia Broadcast Multicast Service (MBMS) broadcast bearers in one-to-many transmissions. As it is possible to see in Fig. 2.14, for this method to work it was necessary to add some elements to the LTE network infrastructure: Broadcast Multicast Service Center (BMSC), responsible for seMBMS service scheduling and to start eMBMS bearer services; MBMS Gateway (MBMS GW) which delivers data to the group in question, allows session control and assigns multicast IP addresses; Multicast Coordination Entity (MCE) is responsible for admission control and resource management eMBMS.

- Mission-Critical PTT (MCPTT) is a service similar to PTT present in legacy PSS that ensures interoperability between PTT and LTE MCPTT. MCPTT depends on ProSe, GCSE and priority usage. ProSe services can be extremely useful in this case because enable communication with group members outside network coverage area through ProSe Relaying mechanism described above.

More details about group communications can be found in 3GPP TS 23.468 [17, 35, 36].

2.2.2.C Voice over LTE (VoLTE)

Voice over LTE (VoLTE) allows the delivery of voice communications using other data services over networks LTE and is considered a type of Voice over IP (VoIP), taking into account that LTE networks

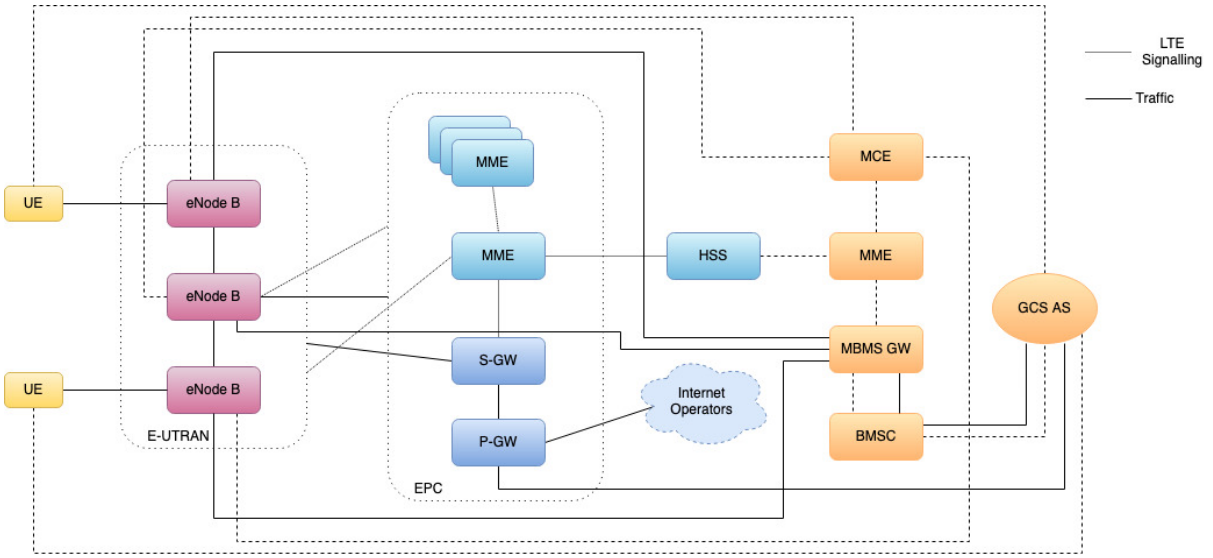


Figure 2.14: LTE Group Communication architecture.

are IP-based networks. This service can be delivered with IP Multimedia Subsystem (IMS) support (IMS is an architectural structure defined by 3GPP that enables the delivery of multimedia services over IP networks). The main difference between VoIP and VoLTE is the QoS offered because in VoIP voice does not take priority over other types of communication and call quality cannot be guaranteed, but in VoLTE, voice communications take precedence over other types of communications. VoLTE using IMS Multimedia Telephony Service (IMS MMTel) allows interoperability with legacy systems such as 2G or 3G, which represents a great advantage. In Fig. 2.15 it is possible to observe the position of IMS in an LTE architecture [17].

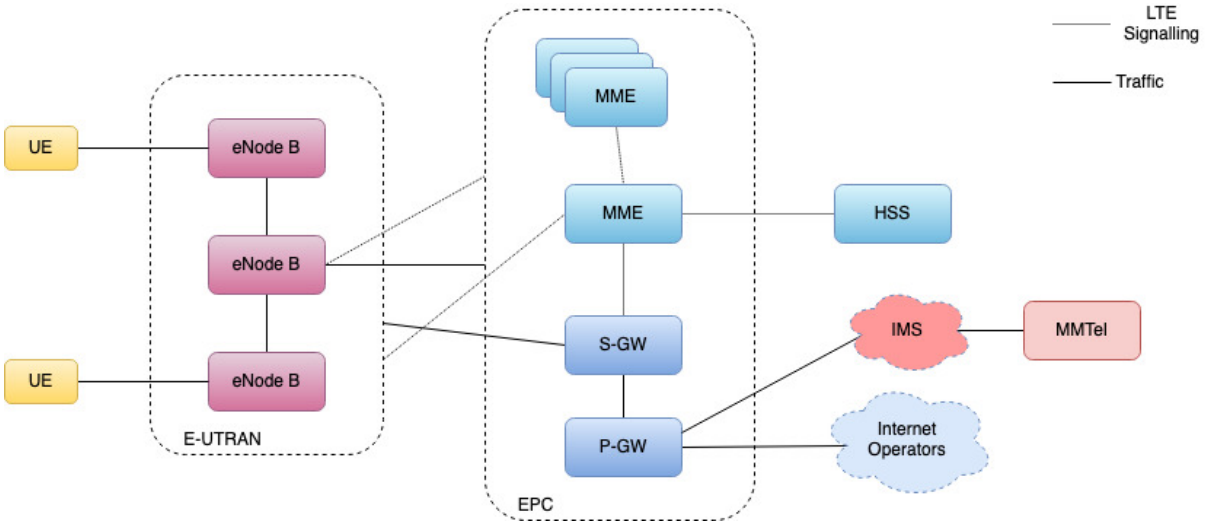


Figure 2.15: LTE IP Multimedia Subsystem (IMS) architecture

The Fifth Generation (5G) concept is relatively new and the 5G networks are being widely deployed

in 2020. 5G can still be considered an integral part of the LTE technology because from the point of view technological 5G is a continuation of 4G. The main differences between 4G and 5G are in terms of service, with greater versatility and flexibility of the network in various points of view, such as better spectral efficiency, more spectrum available, different bandwidths, allowing higher data rates, among others. 5G also has an intimate relationship with SDN and NFV in order to enable the desired network flexibility and programming.

Until now, gmobile network generations have been developed to serve only mobile communications. 5G has come to shake this paradigm because the development of this latest generation of mobile communications has as its main objective to serve different vertical markets such as healthcare, transportation sector, manufacturing, energy sector, among others. ITU - Telecommunication (ITU-T) and 5G Infrastructure Public Private Partnership (5GPPP) defined three different use case families, 1. enhanced mobile broadband, 2. massive machine type communications and 3. critical communications which, at first glance, have very different requirements between them. A large part of the 5G that will allow the fulfillment of these services is the Network Slicing that will be covered later in this document.

Latest ETSI standards that define 5G network requirements [37] state that these networks have the resources to provide peak data rates of 20 Gbit/s in downlink communications and 10 Gbit/s in uplink communications and that the frequency spectrum available is much broader, it includes the 4G spectrum, the so-called Milimetre-Wave (mmWave) and even the unlicensed spectrum. In general, the spectrum available for 5G use can be divided into three parts: 1. Low-band spectrum, the spectrum under 1GHz that is also utilized by 4G communications and that allows a good coverage area with good obstacle penetration, but with data rates under 100 Mbit/s (such as the ones offered by 4G); 2. Mid-spectrum band, that represents the spectrum between 1 GHz and 6 Ghz. These frequencies are able to provide a lower latency and a better throughput than the first ones, peak data rates of 1 Gbit/s but with some difficulties in penetrating obstacles; 3. High-band spectrum, the so called mmWaves that are frequencies above 6 GHz, what allows peak data rates in the order of tens of Gbit/s with extremely low latency, but with a very limited coverage and major problem in penetrating obstacles such as walls [38].

The possibility of using new parts of the frequency spectrum introduces the use of Heterogeneous Access Networks. Heterogeneous Access Networks are characterized by being composed of different types of cells such as Macro Cells, Small Cells and Spot Cells. Small cells are the cells that serve the mmWaves and allow network coverage of up to a few tens of meters, which implies the need to use many more cells than before, leading to a great densification of the network.

There are a few different views of what the 5G architecture should look like, such as Next Generation Mobile Network Alliance (NGMN) [39] and 5GPPP [40]. The main differences between them depend on the infrastructure division, [39] divided the architecture into three layers (infrastructure resources, business enablement and business application), more “generic” layers, while [40] divides architecture

into five layers (infrastructure, network function, orchestration, business function and service layers). But both are at the point where virtualization and slicing are essential to meet the different services needed.

In Table 2.2 it is possible to observe a comparison between 2G, 3G, 4G and 5G carrier bandwidth, frequency bands used and maximum data rates allowed by each technology.

Table 2.2: Commercial Networks Comparison

Technology	Carrier Bandwidth	Frequency Band [MHz]	Max. Data Rate
2G	200 kHz	380, 410, 450, 480, 710, 750, 810, 850, 900, 1800, 1900	9.6, 14.4 kbit/s
3G	5 MHz	700, 800, 900, 1400, 1700, 1800, 1900, 2100, 2500, 2600, 3400, 3500	384 kbit/s, 2 Mbit/s
4G	[1.4/3/5/10/15/20] MHz	450, 700, 800, 1400, 1600, 1700, 1800, 1900, 2000, 2100, 2300, 2400, 2500, 3400, 3500, 3600, 5000	100 Mbit/s
5G	$<$100 MHz in low and mid-band $<$1GHz in high-band	$<$1 GHz; 1 GHz - 6 GHz; $>$6GHz	20 Gbit/s

2.2.3 Public Safety Technologies Vs. Cellular Communications Technologies

Comparing the technologies used in PSN and commercial networks, the lack of development and evolution in PSN is notorious. In summary, as already mentioned, this is due to the fact that emergency networks do not generate revenue for those who own them (besides guaranteeing the safety of the population) and their number of users is quite low in comparison with commercial networks, which generate high revenues for their service operators and have a high number of users.

But why are recent technologies still not being used in Public Safety Network (PSN)?

One of the biggest reasons is that it is not financially possible to have a 3G, 4G,... network, entirely dedicated to emergency communications because these networks require a lot of expensive infrastructure and maintenance, expenses that governments cannot afford . To combat this, there are some solutions that allow commercial operators to share infrastructure with PSN operators, such as a public-private partnership between the State and one or more commercial operators. Previously, some basic requirements for the correct functioning of a PSN were mentioned, one of the most relevant requirements being the availability and reliability of the network. In an emergency situation, a commercial network can become congested and even fail due to the massive use of millions of users, so simple network sharing is not a viable solution. Considering this fact and the mobile technologies available until today, the possibility of new approaches to integration of LTE are beginning to be analyzed as the possibility of public-private partnerships, mainly with mobile network operators, where there are some different solutions for the integration of new mobile technologies in PSN, such as sharing network cells

and towers only, creating a totally new and private RAN for the PSS in question or sharing the total commercial network infrastructure for use of Public Safety, where some Service Level Agreement and technical solutions must be made to guarantee the necessary services and availability of the network for PSS [3].

Long Term Evolution (LTE) is not 100% compatible with the PSN requirements described above, but of all available technologies it is the one that most adapts and can be "easily" adapted to the necessary requirements. These changes and additions necessary for the current implementation of LTE can also be an advantage for commercial operators and add value to the service offered to the general population. The resources of LTE show that LTE can be a flexible network, especially due to the various possibilities in relation to the different sizes and numbers of cells that can be implanted, which transform LTE into a network highly scalable and on a network capable of supporting a large number of users. LTE networks are very oriented towards QoS and priority management concepts, which can be quite advantageous in a PSN. While not traditional PSN requirements, using a PSN based on LTE makes broadband applications possible and this can play an important role in public safety because it allows the transfer of images and videos in real time, using location systems, biometric readings, facial recognition, among other services. Unfortunately, using an LTE based on PSN is not just advantageous because, compared to LMRS PSN, networks LTE are much more exposed to security threats, mainly due to the large number and diversity of devices connected in the network, therefore, the constant update of the security protocols in the LTE network is a major need [17].

2.3 Software Defined Networking

SDN is a revolutionary way to manage and operate the traditional computer networks, i.e., the Internet infrastructure. This revolution is brought by the use of software to program all the network devices and by the centralized control of the network.

In traditional computer networks, the data plane and the control plane usually reside on the network device itself. The control plane is responsible for managing and updating the forwarding tables, tables that contain the necessary rules to deal with the packets forwarding. This plane is also responsible for processing various network protocols, which may have an influence on the forwarding table. The data plane is responsible for processing the incoming packets, and these packets can be buffered, scheduled, can see their header modified and can be forwarded. Using the forwarding table managed by the control plane, the data plane is able to handle most of the traffic autonomously, because for (almost) each packet, the data plane knows what action to take (this is called departure and action).

SDN has three fundamental characteristics: Plane separation, centralized control and network automation and virtualization. Plane separation consists of separating the data plane from the control

plane on network devices, the data plane being maintained on each network device and the control plane being removed from those network devices. It is well known that most routing protocols used can take advantage of an overview of the network, so SDN suggests the use of centralized control. This control is done by a logically " centralized " controller, which hosts the control plan, which autonomously manages the entire network. The controller has a global view of the entire network and gives simple instructions (install rules for what is now called " Flow tables ") for network switches whenever necessary. When you remove the control plane from network devices, they become just high-speed network switches. Network Virtualization consists of the abstraction of routing details and specification details, that is, it must be possible to think about the final objective without thinking about the physical details of the network. Network virtualization ends up reducing network costs and helps to reduce deployment time [41, 42]. Figure 2.16 provides a simple view of what a network SDN looks like.

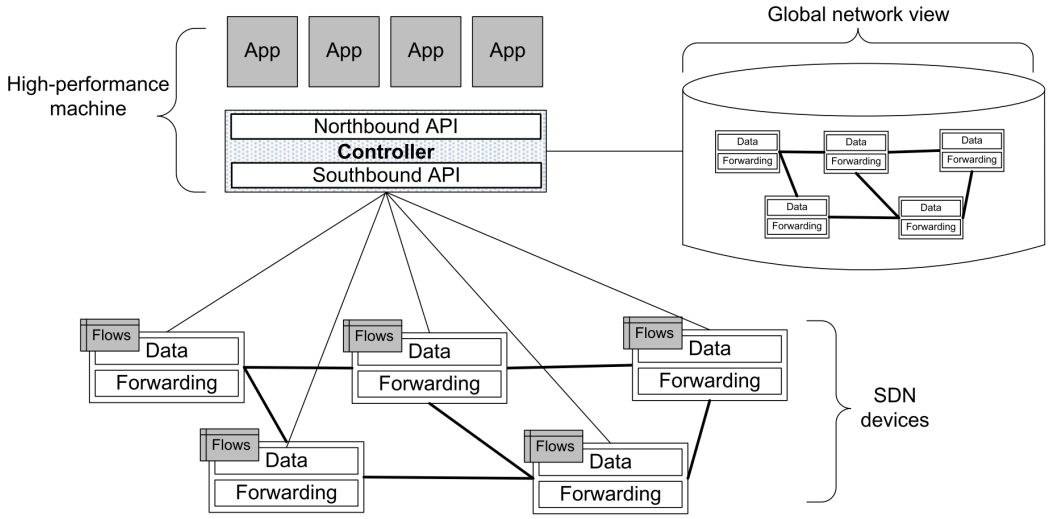
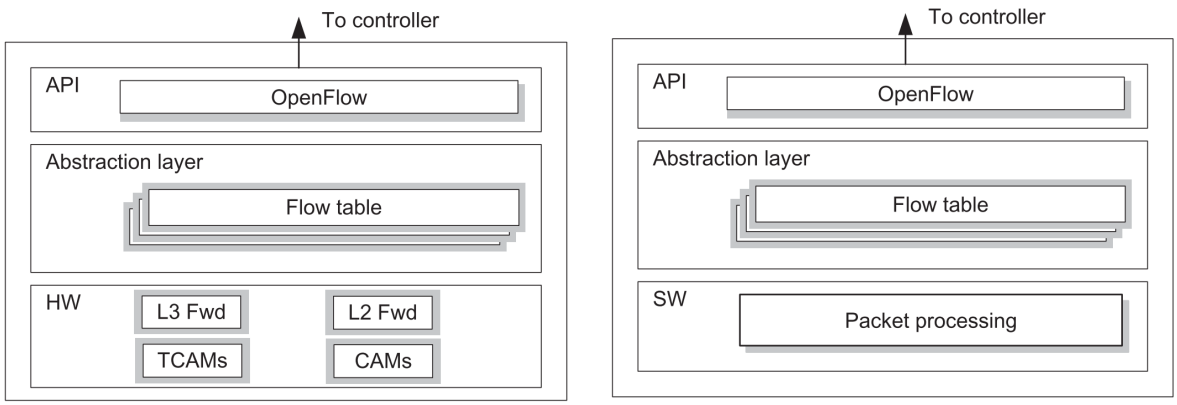


Figure 2.16: SDN Network view. Source: [41]

To operate, SDN needs three basic components: SDN devices, controller and applications. The SDN devices have only one function, the forwarding function and also contain the data that allow the proper function of this forwarding function. This data is represented in the form of flow, flows that are defined by the controller, and each flow describes a set of packets transferred from one network endpoint (or specific set of endpoints) to another network endpoint (or set of specific endpoints). To store information for all flows, each SDN device has " flow tables ", where sets of flow entries and the actions associated with each flow entry are recorded. Thus, every time a packet arrives at a SDN device, the device searches the flow table for a match for the identified flow. If there is a match with the flow identified in the flow table, it takes the appropriate action, otherwise the SDN device sends the received packet to the controller. The communication between the SDN device and the controller is performed through the call Southbound Application Programming Interface (API). This API corresponds to an abstraction

layer where the flow tables and packet processing functions reside, and these functions are different, depending on whether the network devices are virtual SDN switches or physical SDN switches, as can be seen in Fig. 2.17a and Fig. 2.17b [41].



(a) Physical Switch view.

(b) Software Switch view.

Figure 2.17: SDN Switch views. Source: [41]

The SDN controller has a real global view of the entire network, which allows to perform the best forwarding solutions. The controller is also responsible for abstracting the network from the applications. To help applications to respond to the packets that are forwarded to the controller by the SDN devices, the controller allows the applications in question to define flows that the controller will implement in the SDN devices. SDN applications communicate with the controller through the so called Northbound API, and they have as tasks to define the rules that SDN devices need in order to respond to the incoming packets, by setting and managing the necessary flows in the flow tables, managing traffic loads by the multiple possible paths and reacting to unexpected changes in the network topology.

2.3.1 SDN Controllers

The controller is the “intelligent” part of an SDN network because it is the entity that manages the entire network, from the topology perspective to the packet forwarding rules and the switch’s flow tables management, and it is the only entity that has a global view of the network.

The controller architecture, as illustrated in Fig. 2.18, provides two distinct interfaces : 1. the Northbound API, an interface dedicated to the communications between the controller and the applications; and 2. the Southbound API, an interface dedicated to the connection between the controller and the SDN devices through the utilization of southbound protocols.

Besides the two interfaces, the SDN controller architecture includes four core modules, one for end-user device discovery, another for network device discovery, another for network device topology management and another for flow management.

Currently there exists several different implementations of SDN controllers, being that those implementations can be open-source solutions, such as FloodLight, OpenDayLight (ODL), Open Network Operating System (ONOS) or can be commercial solutions provided by IBM, HP, among others [41].

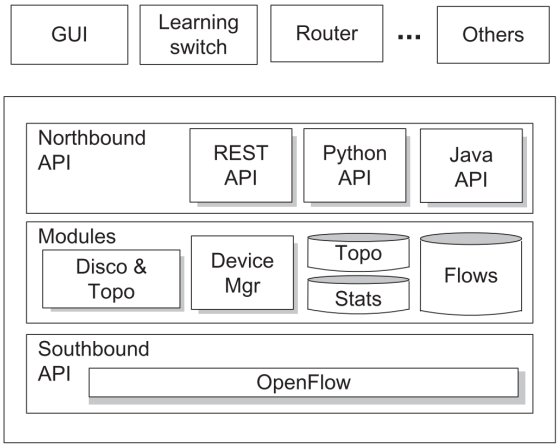


Figure 2.18: SDN Controller architecture. Source: [41]

The FloodLight Controller is a controller developed by the FloodLight Project, an OpenSource Project, and it is an OpenFlow-based Controller. It is written in Java and it is easy to adapt and create software to use with this controller [1].

The OpenDayLight Controller is managed by the Linux Foundation and it is also an OpenSource Project. This controller has the advantage of working with multiple protocols, which allows users to adapt the controller to the network that they are building and allows applications to retrieve network information by the Northbound API [2].

ONOS is another SDN controller that was created with features and characteristics having in mind the operational requirements of Service Providers. [3].

2.3.2 Southbound Protocols

So that the controller is capable to communicate with the network devices, it is necessary to use a protocol. Today there are some different southbound protocols such has OpenFlow and Network Configuration Protocol (NETCONF), among others.

The most used protocol is undoubtedly OpenFlow, a protocol that may be considered responsible for the birth of SDN. This protocol is not just responsible for the communication between the centralized controller and the network devices but also responsible for the expected behavior of the network devices.

[1] https://www.sdxcentral.com/networking/sdn/definitions/what-is-floodlight-controller/
[2] https://www.sdxcentral.com/networking/sdn/definitions/opendaylight-controller/
[3] https://www.sdxcentral.com/projects/open-network-operating-system-onos/

OpenFlow defines the format of the messages exchanged between the controller and the SDN switches.

The OpenFlow Protocol function consist in the exchange of a set of messages sent by the controller to SDN switches and by a set of messages sent by the SDN switches to the controller. These messages allow the controller to populate and modify the switch flow table by adding, modifying and eliminating flow entries. Then, the network device evaluates the incoming packet headers (and even some patterns in the packet payload) and finds the matching flow rules, being then able to match the corresponding action to apply to the packets of that flow. If the network device is not able to find a match for a specific packet, the device should send the packet to the controller and wait for instruction (i.e., new rule) on how to deal with the packet in question. In cases like that, the controller will update the flow table with the new entries, so that in a future similar case, the network device is already capable to deal with the packet in an autonomous way [41].

Another Southbound protocol that is becoming more and more popular is NETCONF. This protocol was designed with the intention of replacing Simple Network Management Protocol (SNMP). NETCONF is a management protocol, so it has the ability to configure the features that are exposed by every network device. NETCONF main features are the separation of configuration and state (operational) data, because configuration data is defined on the device itself and state (operational) data is defined by the device depending on the result of the device changes due to network events, the support for a feature similar to Remote Procedure Call (RPC), the support for Notifications and the support for transaction-based configurations [41].

Figure 2.19 compares OpenFlow devices and NETCONF devices being possible to see that OpenFlow only configures the low level of the device, while NETCONF can manage other features of the SDN device.

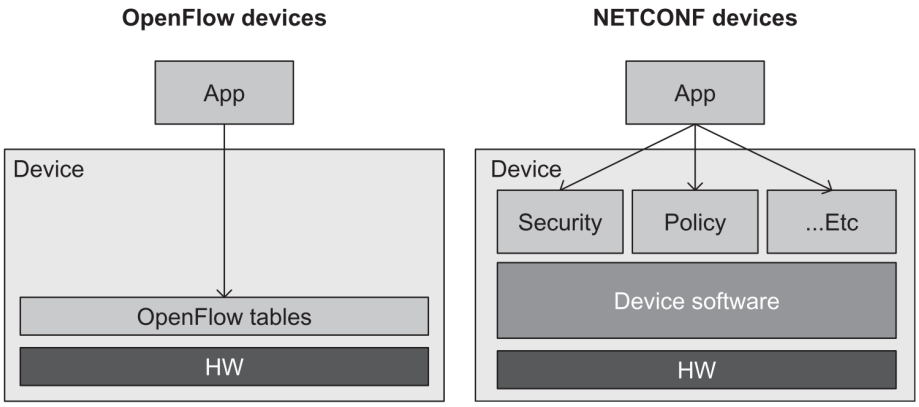


Figure 2.19: OpenFlow vs. NETCONF. Source: [41]

2.3.3 Network Functions Virtualization

Without NFV, each time that a new network service was launched (for example a Firewall, a Network load/traffic Balancer), it was necessary to acquire new system (appliance, or server) dedicated to that new service. Besides the monetary cost of these new equipment, it also was necessary physical space and power sources capable of hosting the new equipment and it also was necessary to perform the integration capability with already existing equipment. Companies did not always have financial availability, space availability and technical skills to fulfill all those requirements.

With NFV, these problems can be addressed in a different way, because NFV allows to implement network functions and specific device functions in a virtual way, using software in non-dedicated hardware devices such as high-volume servers, switches, storage units, among others.

The NFV and SDN association can be advantageous, because they can complement each other, but no one depends on the other. NFV objectives can be reached by using traditional mechanisms, but the utilization of an SDN approach can improve the system performance, can simplify the process and it is a major help in terms of compatibility with existing systems, and the NFV can add more flexibility and can improve the SDN scalability [9, 41, 43].

2.4 SDN, NFV and Network Slicing

A concept that comes up when we talk about network sharing is the concept of Network Slicing. Network Slicing allows the deployment of multiple virtual logic end-to-end network, isolated from each other (Network Slices), with different requirements and different resource needs between them, over a shared common physical infrastructure. Since the Slice's intention is the creation of end-to-end networks, both the RAN and the core network can be sliced. This concept is closely connected to fifth generation networks, but is not exclusive to them. The implementation of Network Slicing can be done based on SDN and NFV because the involvement of these two technologies brings greater flexibility and automation for the slice creation, operation and slice management.

[44] states that a possible Network Slice definition is something similar to "a set of network functions instantiated to form a complete logical network that meet the performance requirements of a service type(s)". In other words, in the end, a network slice is nothing more than a set of resources that work together to deliver the necessary features and to meet the established service requirements. One slice can be created to meet the specific necessities from a specific client or can be a more generic slice that is able to meet the requirements of multiple clients.

The necessary resources to the network slice creation and well function can be divided into two types: 1. Network Functions, that provide specific capabilities to the network so that the network can support and realize certain services and network functions are usually software instances running over

physical infrastructures; 2. Infrastructure Resources, that are not more than generic hardware with the necessary software to accommodate and connect the network functions.

Virtualization is a process with major importance for slicing activity because after the available resource virtualization, is much simpler to share those resources among the existent slices. After virtualization and separation of available resources, it is necessary to use a process that allows to manage and coordinate these resources. This process is called orchestration and as stated in [45] an orchestrator is software necessary to coordinate the various network processes used to create, manage and deliver the requested services. Open Network Foundation (ONF) [46] defines orchestration as the continuous process of collecting resources that meet customer requirements (policies and Service Level Agreements (SLAs)) in the best possible way. The orchestration function is from controller's responsibility.

In network slice definition, isolation is referred as an important requirement for slicing. This isolation will allow the correct operation for parallel slices sharing a common infrastructure and isolation can be divided into three sub-types: 1. Performance isolation, being that each slice has its own specific requirements that should be achieved, regardless what is going on in other slices; 2. Security and privacy isolation, because if security threats or security failures occur in one slice, that should not transpire nor affect the remaining slices and each slice security functions should be independent; 3. Management isolation, because each slice management should be done in a independent way, as if each slice represents a different network, and the management of one slice should not affect the management of the remaining slices [45].

While there is already a lot of knowledge and research on network slicing, there is little knowledge about RAN slicing, especially about network radio aspects managing. In the traditional SDN, the separation of the data plane and the control plane allows each equipment to make its own decisions, but this cannot be applied directly to the management of radio resources because the proximity between base stations can imply in interference if spectrum allocation is not well managed.

There are some entities and work groups such as European Telecommunications Standards Institute (ETSI), ITU - Telecommunication (ITU-T), Third Generation Partnership Project (3GPP) and Open Network Foundation (ONF) working on defining standards for 5G slicing and some of those standards will be approached next.

In [46], ONF elaborates a SDN-based architecture that can be applied to 5G slicing, have been ONF one of the first entities to develop a possible slicing architecture. Observing figure Fig. 2.20, is possible to notice that there exist two main contexts: 1. Client context, that allows a complete resource abstraction and supports the control logic that constitutes a network slice. Inside this context exists the Resource Group that contains the necessary resource set to slice's activity and these resources are managed by the controller; 2. Server context, that is similar to the previous context mas contains everything that is necessary to interact with the available underlying resources.

The Administrator entity is responsible for the controller and for configuring the policies that will be applied by the controller. The controller is responsible for managing all available resources, for managing the existing network slices and for implementing the policies transmitted to it by the administrator. In the architecture presented, the slices are represented as an analogy to the client's context [45–47].

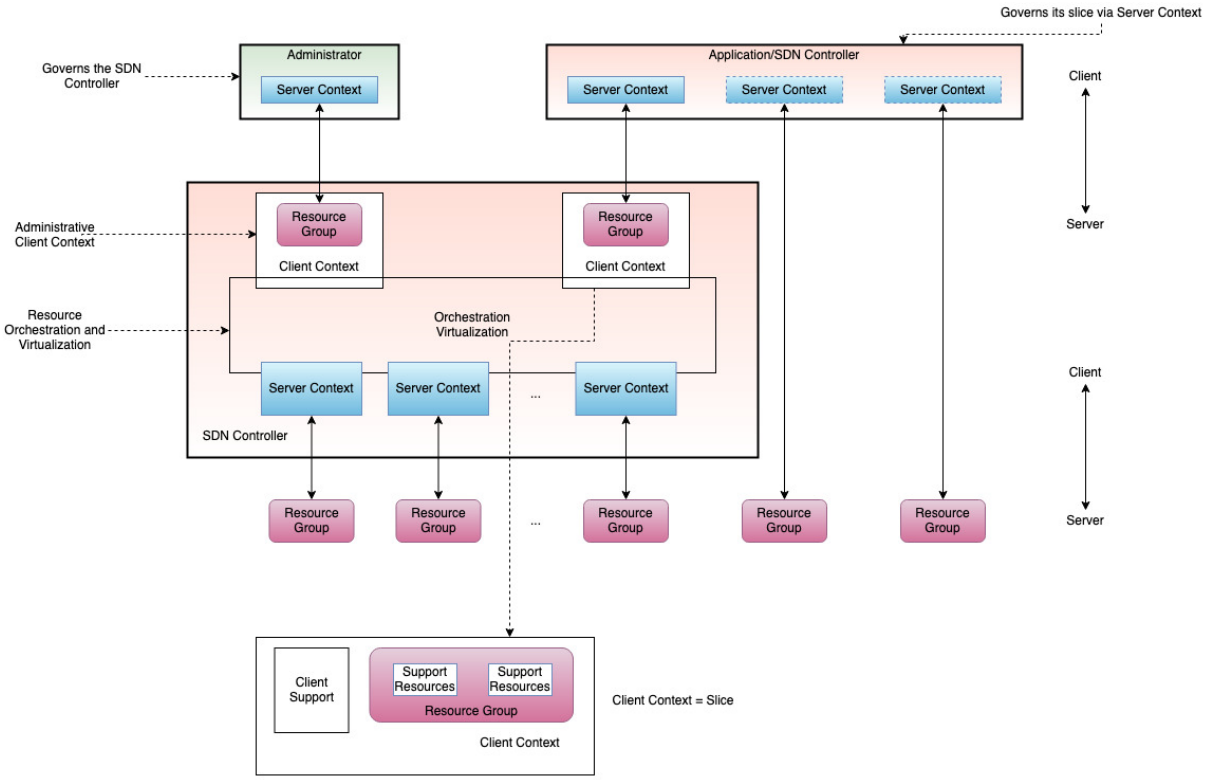


Figure 2.20: ONF SDN-based Slicing Architecture. Based on [46]

ITU-T developed the IMT-2020 Project [48] that it is dedicated to the definition of standards for the services offered by 5G networks. One of the most relevant services addressed in the document is the network slicing and it was also suggested a Framework for the slice management and orchestration. This framework can be divided into two sub-levels, 1. network slice life-cycle management level, where are included the functions used to create and manage the network slice instances and 2. network slice instances level, containing the functions instantiated in the actual network slices.

Of the few projects that exist on RAN softwarization, two are playing a more prominent role. SoftRAN [49], which proposes a centralized architecture through the abstraction of individual base stations to one "virtual big-base station", making control of each individual base station minimal. Each individual base station is now managed by a centralized controller that makes the decisions of the "big base station", maintaining a global view of the network. From the user's point of view, the individual base stations still exist and the handover is still managed in the traditional way.

Another relevant Project is FlexRAN [50], a platform responsible for separating the RAN data plane

from the RAN control plane, through a southbound API (similar to traditional SDN). FlexRAN objective is to give a flexible control plane through the utilization of virtualization, following SDN/NFV principles.

This project has two main components, the FlexRAN controller and the FlexRAN agent. The controller is connected to the agent present in each eNodeB of the network and these agents can act as local controllers because in addition to the limited view of the network they have, they deal with the control that the master controller can delegate to it. FlexRAN also uses a specific FlexRAN protocol that allows communication in both directions, so that the agent can send the status of eNodeB and relevant messages about the status of the network to the controller and for the controller to be able to transmit commands necessary for the best behavior of the agent. From the user's point of view, FlexRAN is irrelevant because it is transparent.

2.5 Public Safety Networks and Software Defined Networking

SDN and NFV technologies are starting to be taken into account when addressing the way to improve PSS, but there are not many projects or research efforts leading to that objective. This section presents some of the existing projects, studies and frameworks that relate SDN, NFV and PSS.

One research initiative, described in [51], is for a SDN application to improve the management and control of already existent technologies such as the UAV in Public Safety scenarios. UAVs are autonomous, unmanned planes, that can be used for a large variety of tasks, such as video surveillance, aerial photography, real-time imaging in rescue operations, communication recovery in disaster situations, among others. These devices have the capability of working together, forming an Unmanned Aerial Vehicle Network (UAVNet), as illustrated in the example of Fig. 2.21. SDN can become a major helper for managing this type of network because of the centralized control and the global network view provided by SDN, which becomes responsible for all the network functions, helping to achieve a better UAVs positioning, avoiding collisions, etc. Additionally, SDN can become really important in networks like this one because it allows a more precise trajectory control of each UAV individually, improving the network performance and operational efficiency. Usually, in these scenarios, each UAVNet is deployed having only one defined task, and so, the use of a centralized control allows for a better node orchestration, with the correct behavior and a correct data transmission even with the nodes in movement [51].

Project DAVOSS [52], created by NATO in 2018, foresaw and proposed for 2021 the design of a virtualized cloud-based architecture to improve some of the tasks performed by UAVs, such as border monitoring and counter-terrorist operations. This architecture will be based in SDN and NFV because the use of these two complementary technologies can effectively turn the system more automated and more autonomous. The centralized control that SDN brings to the network turns the network more efficient and with an optimized performance when combined with NFV, allowing for different traffic types

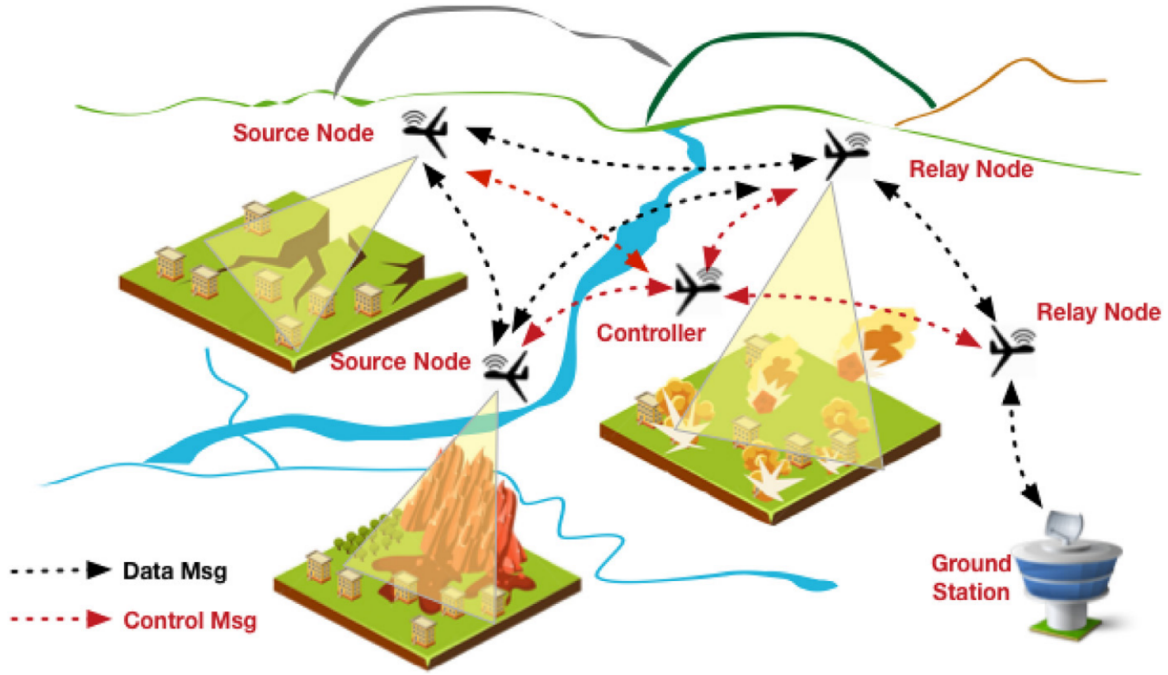


Figure 2.21: A Software-defined UAVNet. Source: [51]

to be handled in the best way and with the correct priority [52].

Project Loon [53], a project founded by Google, uses wireless balloon network stations to provide Internet access in remote areas, where Internet infrastructure does not exist. The ideas of Project Loon were adapted to provide communications in emergency situations in areas where, for example, COWs cannot get to, because those areas got inaccessible after a disaster. The configuration and control of the balloons is based in SDN, which allows a network auto-configuration involving more than one balloon, regarding its position (between certain limits) and ground stations that remains active. These balloons are a solution with small costs but, depending on the atmospheric conditions, they can be unstable and rugged. It is to note that the balloons are one form of a UAV, but this kind of system can be applied for other UAV types, such has drones [7, 53].

The SDN-ERS Framework, described and proposed in [54], deals with the critical response time of emergency communications and with the QoS of this type of traffic. The proposed SDN-ERS has the capability of considering network traffic with different priority levels, depending on the emergency situation in question. The goal of that framework is to offer the minimum end-to-end delay possible between users and emergency services, being that the delay changes considering the different priority levels of each packet. In SDN-ERS, the SDN controller plays the “dispatcher” role, having as main function to deal with the incoming messages to the right emergency service. The implementation is based on queuing techniques and QoS features to enable the traffic differentiation between regular traffic and urgent traffic, because every kind of traffic has its own priority level and to guarantee the minimum end-to-end delay.

When the controller is serving an urgent message, all the incoming messages go to the priority queue and wait for the moment when they are dispatched. In the right moment that a message arrives, it is classified accordingly with their priority level and its arrival time. If two messages with the same priority arrive almost at the exact moment, they are ordered in the priority queue accordingly with their precise arrival time [54].

The Network Embedded On-line Disaster (NEOD) Framework, described and proposed in [9] is a SDN-based catastrophe manager that has its focus on agility, accuracy, reliability and scalability problems. The NEOD architecture has two layers, being the first layer a disaster event detection and filtering segment, residing on an OpenFlow-based switch, and this layer includes event detectors, that uses already defined rules to monitor the events sent to them by an Event Publisher, a dynamic event detector manager, and a system event adaptation layer. The second layer has the NEOD manager that relates the received events with possible causes and predicts what are the events impossible to deal with. NEOD has three types of event detectors, being one the new flow attack, that consists in injecting randomly a huge flow number in an OpenFlow switch, another is the interface flapping, where the hardware interface of a switch suffers an hardware fail that creates “up” and “down” events, and the event storm that can occur in cases where one network object relate with many other objects changes its status multiple times [9].

The Decentralize-SDN (D-SDN) proposed in [55] allows to distribute the SDN centralized control when there are present more than one administrative authority. Logical control and physical control are distributed by a controller hierarchy that is composed by main controllers and secondary controllers. For a secondary controller be able to operate, it has to be activated by a main controller and the hierarchical structure of the controllers helps the control of plain availability and fault-tolerance. In the environments where PSN operate it is normal that the communications fail and so, this framework allows for a faster recovery because if the main controller fails, a secondary is capable of immediately replace it. This choice is made using a secure algorithm [9, 55].

The UNIFY Service Function Chaining (SFC) Framework [9] proposes a simplification of PSSs by using UNIFY, because in emergency situations it is possible that no one qualified to operate this kind of systems is present. The UNIFY framework defines a resource virtualization and a joint cloud utilization in a way to optimize resource management of the resources provided by all the available technologies [9].

2.6 Public Safety Networks and Network Slicing

The authors in [56] describe a possible solution for sharing infrastructures between commercial networks and Public Safety Networks, where only the RAN resources are shared and take advantage from the utilization of heterogeneous networks, typical from 5G and described above. One of the biggest

advantages from this project is the utilization of small cells, dedicated to the PSN and placed in strategical locations in a way to increase network coverage in catastrophe situations, creating a public safety dedicated RAN and a shared RAN. The shared RAN has two slices, the commercial slice and the public safety slice, also with two distinct core networks, the commercial core network and the Public safety core networks. It is also suggested a scheduler to manage the resource division.

3

Proposed Architecture

Contents

3.1 LTE Networks and Operation for Public Safety 47

3.2 Public Safety Networks and Network Slicing 51

3.3 Possible Architecture 52

As it was possible to understand in the previous chapter, Long Term Evolution (LTE) is the preferred technology to create a new, more evolved and more modern Public Safety Network (PSN). In this chapter some options will be presented on how LTE can be used to create these networks and how technologies like SDN and NFV can be associated with these networks.

3.1 LTE Networks and Operation for Public Safety

LTE was the technology chosen for this architectural proposal to create a better and more modern PSN that can replace legacy systems like TETRA. First, it is important to understand how a LTE network works in order to understand how this technology can be adapted to the requirements and features of emergency networks.

As mentioned earlier, LTE networks exhibit a big difference from previous systems, which is the fact that LTE is an IP-based purely packet-switched network. The circuit switched component of the previous systems was responsible for the voice transfer domain and in LTE, the voice transfer is now performed over IP, using, for example, VoIP, which is explained later in the document. The packet-switched domain is specialized in data transfer and is extremely necessary since the motivation for the development of LTE was the need for high volume data transmission and data applications in mobile communications.

LTE network can be divided into two major subsystems:

- Evolved Universal Terrestrial Radio Access (E-UTRAN), that is the LTE RAN, responsible for radio communications between User Equipment (UE) (mobile devices) and EPC. E-UTRAN main component is Evolve NodeBs (eNB) (LTE Base Stations), a logical component responsible for sending and receiving radio transmissions to and from UE handle by the eNB in question and for controlling some low-level operations of these UE. Each eNB can connect to EPC and to other eNB by different interfaces, being that these communications are performed by the underlying IP network.
- Evolved Packet Core (EPC), LTE core network, supports packet-switched domain access and has three main components: 1. Service Gateway (S-GW), responsible for forward data between E-UTRAN and P-GW, for allowing connection between LTE network and previous 3GPP systems and for collect information needed so that the network operator is able to bill for the used services. Each UE is assigned to a single S-GW, that can change according to UE movement; 2. Packet Data Network Gateway (P-GW) is the contact point between LTE network and the outside world, being that it can connect with the Internet, with IP media subsystem, operator server network, among others. P-GW is also responsible for address attribution to devices present in the network and each UE is assigned to one P-GW and can be assigned to more, according to UE services needs; 3. Mobility Management Entity (MME), responsible for controlling UE high-level operations, such as security and authentication questions, mobility management and data stream management not

related with radio questions. Each UE is assigned to only one MME but this MME can change according with the UE movement;These three components are, once again, logical components that can be aggregated in only one physical network component [32, 33].

3.1.1 LTE Network Infrastructure and Spectrum Sharing

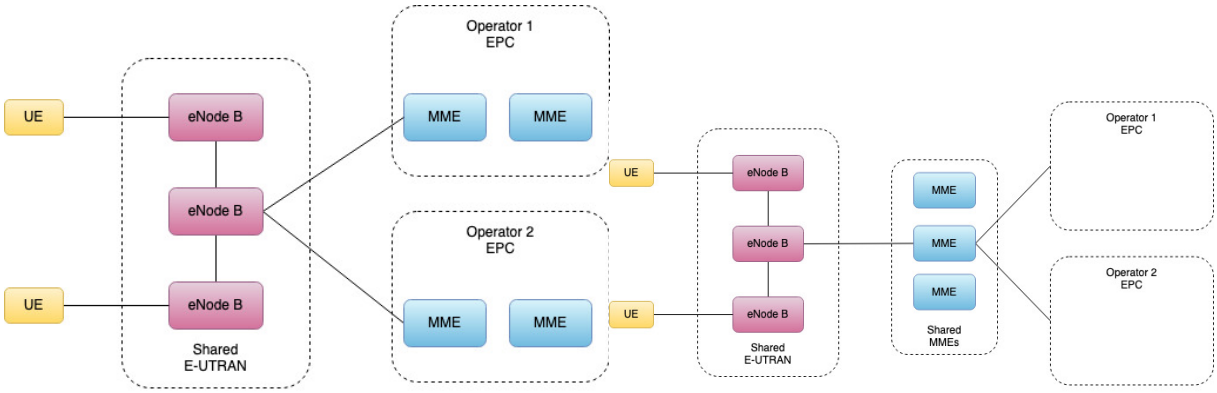
As already mentioned, the main factor that is delaying the evolution of Public Safety Systems is the significant cost of implementing a dedicated network of recent technology, such as LTE. To contradict this factor, sharing network infrastructure has been suggested in order to reduce implementation costs. This sharing can be defined as a process through which one or more operators share network infrastructure to provide a mobile service to their users [57] and can be done in several ways. Some of the most relevant sharing options will be described in this section.

Analyzing the architecture of the LTE network, it is possible to observe a natural division that stands out between the two LTE subsystems, E-UTRAN and EPC. When talking about LTE network sharing, it is possible to imagine three scenarios at first glance: sharing E-UTRAN, sharing EPC or sharing the entire network infrastructure. But sharing network infrastructure, especially when talking about Public Safety Network (PSN) is not so simple due to the strict requirements,to the security issues and critical communications that this type of systems presents and it is also possible to consider some hybrid solutions. Network infrastructure sharing can be classified as passive sharing, where non-active, without intelligence network elements, such as masts, sites, power sources, ... , are shared and in active sharing where network elements with some degree of intelligence, such as antennas or EPC are shared.

During a new network physical deployment, the most expensive network part is RAN so, RAN sharing is the most obvious option when trying to reduce new LTE-based network implementation costs. This network infrastructure sharing was considered when creating LTE standards and in standards set 3GPP TS 23.251 [58] two possible sharing architectures are defined:

- Multi-Operator Core Network (MOCN), where each network operator has a dedicated core network and exists a single unique RAN shared between the operators in question. In LTE case, E-UTRAN is connected to more than one EPC through S1 interface and no core network element is shared. An example of this shared architecture can be seen in Fig. 3.1a.
- Gateway Core Network (GWCN), where each network operator as a dedicated core network, but the MME is shared between the operators in question and not dedicated as in previous solution. E-UTRAN subsystem is also shared as in MOCN option. An example of this shared architecture can be seen in Fig. 3.1b. GWCN sharing option becomes less flexible and the differentiation level among the operators also becomes more reduced.

In addition to sharing network infrastructure, it is also necessary to manage spectrum resources.



(a) MOCN architecture. **(b)** GWCN architecture.

Figure 3.1: MOCN and GWCN architectures.

The available spectrum can be strictly divided between the operators sharing the infrastructure and each operator can only use the part of the spectrum allocated to it (operator 1 can use part 1 of the spectrum, operator 2 can use only part 2 of the spectrum , ...) or the available spectrum can be dynamically shared among the users of the operators in question. Sharing spectrum resources becomes more efficient because there is no strict division of available spectrum resources [59].

Besides the cost reduction, RAN sharing allow to increase network coverage in some areas such as rural areas where it was not convenient to deploy infrastructure to a single operator but when sharing the resources, it become advantageous. Spectrum resources sharing allows improving the spectral efficiency. Relatively to costs reduction, [57] states that passive sharing can reduce in 16%-35% Capital Expenditures (CAPEX) costs and in 16%-35% Operational Expenditures (OPEX) costs, active sharing without sharing spectrum resources can reduce in 33%-35% CAPEX costs and in 25%-33% OPEX costs, active sharing with spectrum resource sharing can reduce in 33%-45% CAPEX costs and in 30%-33% OPEX costs and that sharing the core network does not bring any significant savings.

As mentioned earlier, when dealing with emergency networks, security is a major problem and, therefore, sharing infrastructure with a commercial network may not be the most appropriate solution due to the difference in requirements and due to the security threats that commercial networks are exposed to. Another possible solution is the implementation of a new network infrastructure, managed by a private operator and shared by private networks with requirements similar to PSN requirements, such as private networks of security companies, networks of transport companies, networks of electricity providers, etc. Again, this share can be just sharing the RAN or sharing the entire network infrastructure.

One very important question regarding PSN sharing infrastructure with other networks, that suits all the presented solutions, arises from the PSN requirements, that is the communication priority. When an emergency communication network is sharing resources and infrastructure with other networks, the PSN communications and needs must have priority over the remaining networks that are sharing the

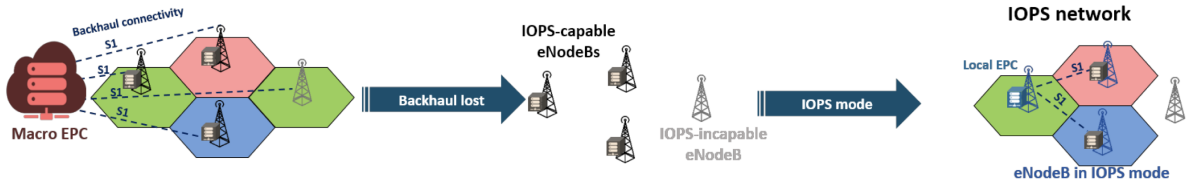
underlying infrastructure and, in an ideal case, the PSN may even need more resources than the ones initially allocated to it and this resource sharing and allocation should be possible.

3.1.2 Isolated E-UTRAN Operation for Public Safety

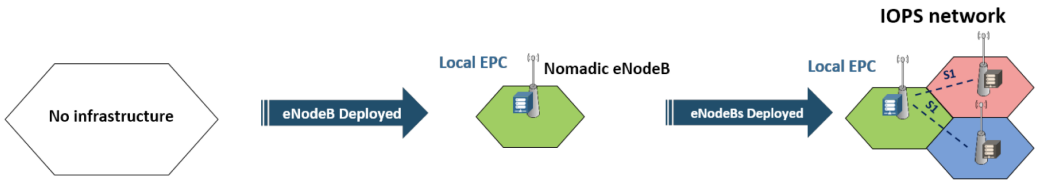
In Release 13 (3GPP TS 22.346, Release 13 [60]), 3GPP introduces the Isolated E-UTRAN Operation for Public Safety (IOPS) concept. The main goal of this concept is to maintain Public Safety communication operation even if the backhaul connectivity between eNodeB's and Core Network is destroy by some reason. IOPS operation is described in [61] and basically, when the backhaul connectivity between E-UTRAN and Core Network is not existent by some reason, IOPS allows the Public Safety users to still use local IP connectivity and voice communication.

There are two main IOPS scenarios, one, where the infrastructure exists and remains operational and only the backhaul connection is loss and the other, where the infrastructure does not exist or is also damaged along with the backhaul connection. In the case of the second scenario, some mobile units (such as LDRU or COW) must be deployed. So that the services still work in the best way, 3GPP suggests the use of a "Local EPC" that comprises the traditional EPC main functionalities. This local EPC can be located in one of the eNodeB or just be connected to one of them (see Fig. 3.2).

Fig. 3.2a shows the situation where the eNodeB still works but lost its backhaul connection. The eNodeB enters in IOPS mode and allows the communication to work. Fig. 3.2b shows the scenario where do not exist any infrastructure, the infrastructure is deployed and enters in the IOPS operation.



(a) IOPS in loss of backhaul.



(b) IOPS isolated.

Figure 3.2: IOPS network formation: (a) Following the loss of normal backhaul connectivity to the Macro EPC; (b) In an isolated location with no pre-deployed infrastructure. Source: [61]

IOPS operation goes as follow: The eNodeB enter in IOPS mode, has to establish connection with the MME present at the local EPC and then follows the standard LTE procedure.

3.2 Public Safety Networks and Network Slicing

In the previous section, the most "traditional" and best-known forms of network sharing were analyzed, which can be used to allow the sharing of network infrastructure between PSN and LTE commercial operators. With the rapid development of technology, a new form of network infrastructure sharing has recently emerged and, theoretically, can be applied to emergency and security networks - network slicing.

In previous solutions the core network sharing was not the most relevant neither advantageous, but in network slicing core network sharing is what brings most advantages because network slicing foundations affirm that the intention is to create multiple end-to-end logical networks capable to provide the network services required by the clients.

As previously stated in the document, PSNs are networks that support critical communications, where latency, delay and coverage play an important role. In addition, PSNs are networks that must always be available and must be resistant to any type of failure that may occur. Because it is such an important network, especially after disasters, and carrying such important communications, there must be mechanisms that allow the network to recover if it fails due to a catastrophe that may occur. Another important requirement is the scalability of the network, because in an emergency, the number of users may increase unexpectedly. So how can the network division meet and help PSN requirements?

As it was said before, network slices can function as logical networks, isolated between them, that share resources and an underlying physical infrastructure. These features make possible to PSN to take advantage of the most recent technology without the necessity of owning a dedicated infrastructure, what reduce significantly the PSN implementation costs. Relatively to the PSN requirements and how can 5G network slicing fulfill them:

1. Latency: using 5G technology is possible to enjoy from the lowest latency possible nowadays (close to 10ms in end-to-end low latency communications and close to 1ms in ultra-low latency cases);

2. Network coverage: Sharing RAN infrastructure with an already existent commercial network means sharing the existent network of base stations that provide a fine coverage of the national territory. But PSN operator coverage requirements are not the same as the commercial network operator. As [56] affirms, 5G enable the use of heterogeneous networks, where is possible to add base stations with different coverage power in places where the coverage is not enough, increasing the PSN coverage according to the requirements and creating a slice with exclusive base stations to the emergency network;

3. Availability and Resilience: According with [39] a 5G network enables 99.999% of availability and includes robustness mechanisms against climatic events. Resilience mechanisms are necessary,

such as in previous technologies, to ensure the network recuperation in case of failure. Some of the mechanisms described before to recover the network or increase coverage (such as COWs) can still be used. A big network slicing advantage is the isolation among slices. In case of a security threat or attack to one of the slices, that threat will be contained to the slice in question, without affecting the remaining ones;

4. Scalability: Another network slicing advantage is the dynamic resource allocation that allows to allocate resources among slices as needed. In a case of necessity, the orchestrator can allocate more resources to a specific slice and even re-allocate resources from one slice to another that needs them more, becoming slices highly scalable;

5. Priority: 5G allows to attribute priorities to the communications and/or slices. So, if exists one or more slices dedicated to emergency communications, these slices can have higher priorities then the remaining slices, which is extremely important for the resource allocation referred in the point above. In other slices is possible to attribute more priority to communications destined to emergency services.

3.3 Possible Architecture

A possible architecture that respects everything that was described until this point is the utilization of an LTE network, with a simplified architecture close to the one showed in Fig. 3.3. This architecture is based on the one described in [62].

This is a LTE network that can fit into different sharing situations, such as: a service provider network shared with PSS with dynamic resource allocation; a network that belongs to a private company and is shared with a PSS or a network dedicated to the various agencies that are part of a PSS. This network contains, in addition to the normal LTE network elements, a SDN controller, a Software Defined RAN (SD-RAN) controller and an orchestrator.

These additional elements allow greater programming and flexibility of the network, allowing the use of slicing. As previously mentioned, the network slice allows the creation and management of network slices, flexible and created on demand, with the necessary requirements for each “sub network” and isolated between them. A network with these characteristics can respond to a variety of scenarios, with different requirements, while minimizing the waste of network resources or, on the opposite hand, the lack of resources in a dedicated network.

The idea is to have a shared network, possibly with one of the solutions indicated above, and to use network slicing to manage and allocate network resources according to needs. Therefore, this flexible resource management will allow a great response to the need for PSN in any situation and almost on

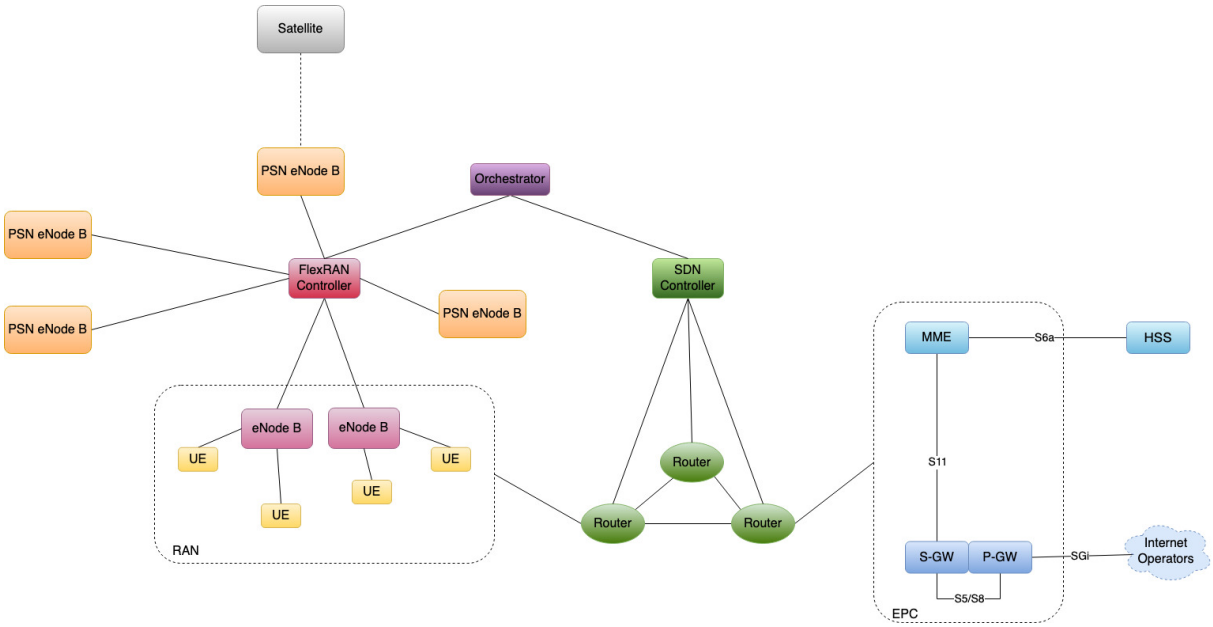


Figure 3.3: Possible solution architecture

.

demand, knowing that other network(s) that share the infrastructure with the PSN may suffer some break in service or problems in the quality of service in extreme situations, but this will be rare and occasional situations.

As previously mentioned, the main focus of coverage for the commercial service provider is in areas with a high population density, therefore, they will focus most of the infrastructure and ensure network coverage in those areas. This can be translated into a lack of coverage in rural and remote areas, especially in dense forests, mountains and similar places. These locations still need coverage from PSN as these locations are at risk from some catastrophes such as fires, missing persons, overthrown, etc. For this reason, it may be necessary, in case of network infrastructure sharing, to add some Public Safety Network (PSN) exclusive eNodeb in these areas.

In addition, it may be important for network redundancy to add a satellite communication link to PSN in order to guarantee communication in case of failure of other redundancy mechanisms.

In addition to the allocation of resources, the use of LTE and 5G allows the use of priorities so that the slice(s) corresponding to PSN can have more priority than other slice(s). In the remaining slices it is also possible to assign priority to certain communications.

The suggested network can be divided into two parts. The core network contains the traditional LTE core network elements along generic programmable switches, controlled by a regular SDN controller. The use of OpenDaylight is suggested in [62], because of its flexibility and great integration with multiple protocols.

The E-UTRAN part contains an SD-RAN controller. The most used one is FlexRAN [50], that is

a platform that encompass as a controller and an agent placed in each eNodeB. This platform allows separating RAN's control and data planes through a new southbound API (such as in traditional SDN). Assisted by NFV, FlexRAN is able to manage and coordinate the various RAN entities through the new and flexible control plane.

On top of the network exists an orchestrator, responsible for coordinate both controllers, coordinate both parts of the slices and guarantee a good network function as stated before.

An important part of a possible architecture like this is interoperability with legacy PSN, probably based on TETRA. This interoperability is important due to two main factors:

- The transition from a legacy system to a totally new system with new technologies is risky, so a transition phase where both technologies can coexist is very important to keep the system operable and functioning correctly.
- Especially in the early days of a new LTE-based PSN it is likely that coverage is still not ideal. A hybrid system capable of working with TETRA technology and LTE technology can be an advantage because in most countries, TETRA systems have national coverage, which can be an addition to these new systems coverage.

In this line of thought, there are some manufacturers that produce hybrid equipment, capable of operating with TETRA and LTE. Two examples are the Hyetra LTE multi-mode handsets [63] and TETRA + LTE Smartphone [64]. In general, these devices allow group communications and voice communications over TETRA technology and data services over LTE. This is an advantage because, as stated before, in case of lack of coverage LTE, voice communications are still guaranteed by the TETRA coverage and, in addition, the LTE data is available where coverage exists.

4

Demonstration

Contents

4.1 OpenAirInterface Emulator 57

4.2 CORE Emulator 58

4.3 Case studies 59

The fourth phase of DSRM is phase 4: Demonstration. Demonstration can be considered the first step for evaluating the artifact. In Demonstration phase will be described a set of case studies that will illustrate how the solution can be used in different emergency scenarios. In this chapter will also be described some emulation attempts.

4.1 OpenAirInterface Emulator

OpenAirInterface (OAI) is an open-source platform created by OpenAirInterface Software Alliance (OSA), a non-profit organization, with intent of offering an emulation for the study and development of 4G and 5G technologies. OAI is divided in two major parts: OAI EPC and OAI RAN. OAI EPC allows the deployment of HSS, MME and S-PGW modules while OAI RAN allows the deployment of the 4G and 5G UE and the 4G and 5G eNB. Besides total network emulation, OAI also allows the utilization of real and commercial equipment along network emulation.

OAI offers some pros in relation to other existing emulators such as the fact that it allows full network emulation and not just a simulation, integration of real and commercial components and the fact that it is in constant development. OAI also has some cons such as the fact that it has little publicly available information and some documents are out of date due to constant development.

For this experiment, a LTE test network was created using OAI full emulation and installed according to the OAI tutorials found in [65]. These tutorials are out of date, and it was necessary to make some changes to the emulator's code in order to work around some errors found during the deployment of the OAI emulator and it was also necessary to use some different commands from the indicated ones.

Network EPC was deployed in a Virtual Machine (VM) with Ubuntu 18.04 and 4 GB of RAM and the eNB along with the UE emulations where deployed in an Intel NUC machine with Intel Core i5 processor. It was used the develop version of both modules.

The initial idea was to test a LTE network emulation to prove that this technology respects and complies with the standards imposed by 3GPP for emergency and safety networks and, if possible, to implement a push to talk module with a server in core network to demonstrate and prove the communications operation with a group of customers. This last part was not possible due to the limitations of the OAI emulated clients.

The emulation is represented in Fig. 4.1 and contains the LTE core network, with the MME and the S-PGW, the MME connected to the core and one eNodeB to which can connect until four user equipment.

The first network element to be launch is the S-PGW followed by the HSS and the MME that connects to this last one. MME shows in real time the information about the nodes connected to the network. The eNodeB is now deployed and connects to the MME, showing up in the registry and then, the four UE are simultaneously launches and the network attach procedure can be observed in S-PGW, responsible

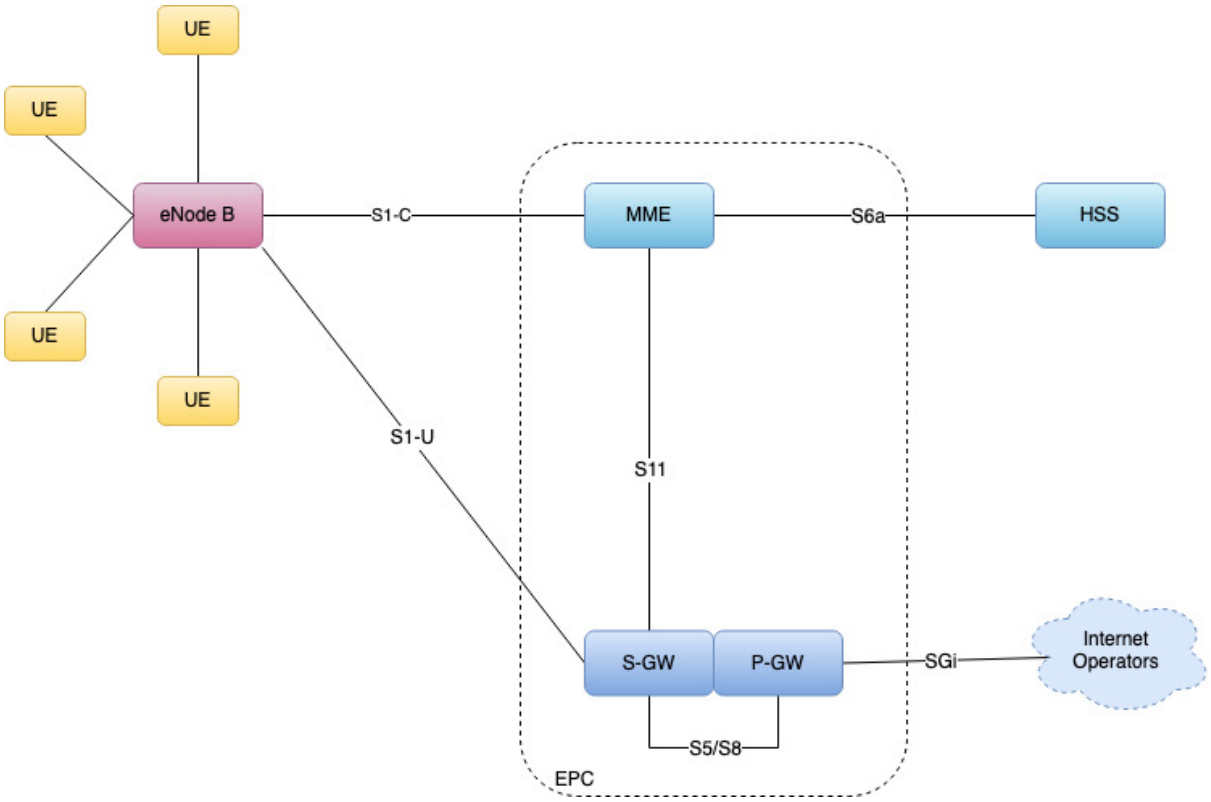


Figure 4.1: Simulation architecture

.

for the IP address attribution (following a defined IP address pool) and in MME that counts the nodes currently actives in the network.

This emulation complies with the LTE defined standards and is a great base for future evolution proposed moreover in the document, but unfortunately it was not possible to adapt it to our need in due time.

4.2 CORE Emulator

With the failure of our first emulation attempt, we decided to do a simpler emulation using CORE Emulator. With this emulator our idea was to deploy a network with some mobile nodes and have a ”mini” core wired network, where we wanted to deploy a PTT server and use the PTT client in the mobile nodes. An example of the test network can be observed in Fig. 4.2.

Unfortunately, we faced some issues while doing this attempt. To deploy the PTT module in the network it was necessary to have access to the internet from inside the emulation and after research and configuration attempts we were not able to put that communication to work, probably due to some CORE emulator bug or incompatibility with the systems used. We tried the emulator's installation in a

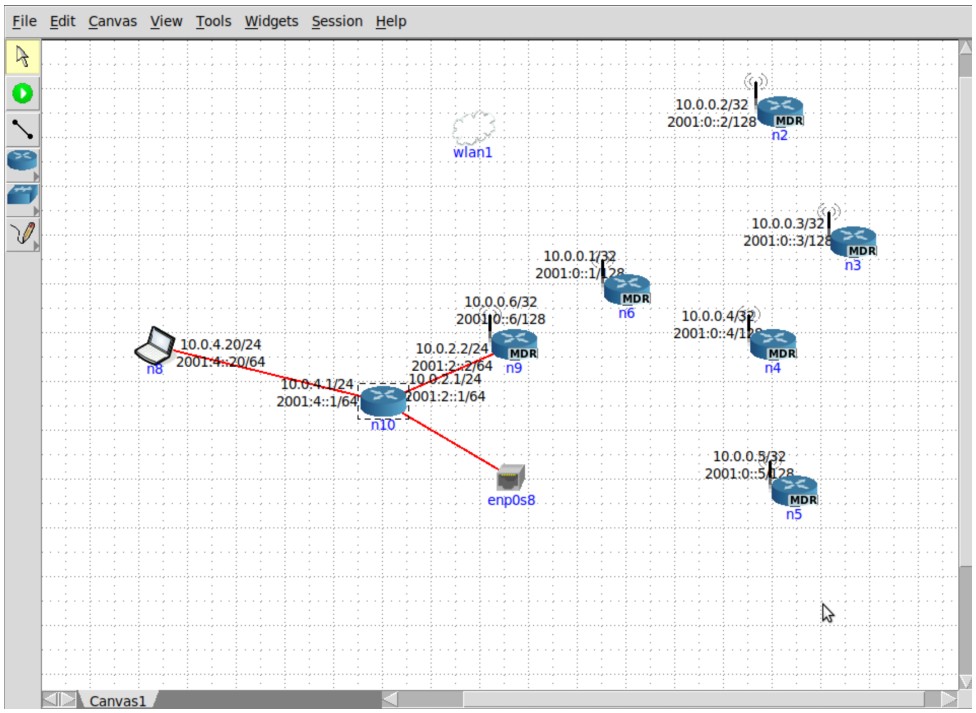


Figure 4.2: CORE Test Network

.

Ubuntu 18.04 VM and in a Ubuntu 18.08 native machine and the problem subsisted in both systems. This problem inhibits the second need we have for this emulation that was to have access to each emulated node Graphical User Interface (GUI), in a way to use the PTT selected application.

4.3 Case studies

4.3.1 Earthquake Disaster Scenario

The first scenario corresponds to an Earthquake in an urban area scenario defined by ETSI in [66]. A scenario like this one can or can not be predicted, has a short incident time (seconds or few minutes), the response to it can last days or weeks and the actors involved in the scene belong to many different teams and organizations.

The main characteristics of a scenario like this one are the high casualties number, the damage to infrastructures that can cause access limitation to get to the victims and, due to the fact that urban areas are highly populated areas, the need of emergency services is higher than the available resources. The communications can be affected by possible damage to infrastructure (power supply disruption, destroyed BS, among other factors) and by the high service demand of people trying to ask for help and trying to contact family and friends.

From the communications point of view, an earthquake scenario will probably be characterized by the high demand of service due to a high concentration of people in an urban area. This scenario has the advantage of being in an urban area so is probable that area has, supposedly, a good network coverage. But in an earthquake, there is a high probability of damage to the network infrastructure.

The requirements for emergency communications defined by ETSI are: Good quality (sufficient for good understanding) speech, short setup times for the calls and end to end delay below 400 ms and some specific services such as group communications, status monitoring to transmit data such as vital signs, location services, data services for a diverse number of data applications that have in common the need of throughput, the need of the information arrive to the destination in a certain time frame and the preservation of data integrity.

So, how the architecture suggested above in the document is able to respond to the needs and requirements of a scenario like this one?

- As stated before, it is possible that network infrastructure fails and it can be possible lack of coverage. To address this situation, it is necessary to add one or more post-disaster network recovery solutions, like the ones described before. A good solution in a case like this one is the usage of some type of Unmanned Aerial Vehicle (UAV) immediately after the disaster to recover the network, until it is possible to place some Cell On Wheels (COW) on the ground, which can take some time due to possible access limitations.

- An architecture like the one showed along with use of recent technologies brings the opportunity of using more services than the traditional ones like real-time image and video. In a situation like this scenario, the UAVs can play other roles besides the network recovery. UAVs can be equipped with cameras and transmit live images from the air that will offer a different scenario vision to rescue teams. This images can be very useful in human resource organization, victim identification, scenario state, organizing escape routes, among others.

- The use of SDN and NFV can be very useful in a situation that involves UAVs because it the devices are able to form a network between them and this technologies are very useful in managing and controlling a network in an autonomous way. Such as in the example [51], SDN can help managing and controlling the UAVNet by giving the controller a global view of the network and take the appropriated decisions having this view in mind. This can be extremely important in matters of coverage, to adapt the UAVs position so that the main goal of providing additional coverage and allowing the network to recover from some failure can be better fulfilled.

- Network slicing will allow the allocation of resources necessary to Public Safety Network (PSN), even if that allocation implicates general population communication service break, if the network infrastructure is shared with a commercial network. Emergency communications are more relevant

and priority in this scenario than the general population ones. The slice(s) correspondent to the PSN will have a higher priority than the remaining slices. This will ensure that all the communications deriving from PSN slice(s) will have priority over all other communications. Inside emergency communications slices is also possible to attribute priorities to the different types of communications that exist. The distress call from the general population can be assured by the use of communication priorities in the remaining communications inside commercial/general slices.

- The choice of LTE as the elected technology allows to positively respond to ETSI emergency communication requirements because LTE allows the usage of Mission-Critical PTT (MCPTT), group communications, proximity and location services and data and multimedia services, and is able to respond to setup call time and delay requirements as it was stated until now on the description and analysis of the many technologies involved. Besides that, the infrastructure that exists for LTE networks nowadays can be considered resilient and redundant and is always possible to add some mechanism such as some of the described before to add redundancy and resiliency to the network.

4.3.2 Mass Transportation Accident Disaster Scenario

The second scenario corresponds to an Mass Transportation Accident (MTA) in a rural environment defined by ETSI in [67]. In this scenario a train collided with a road vehicle. These accidents can not be predicted, have a considerable number of victims in different states of need, the actors involved in the scene belong to many different teams and organizations, the action is limited to a confined geographic area what, joined with the state of the access, can be translated in access limitations. Communications in rural environments can present sparse communications coverage.

From the communications point of view, a scenario like this may gather more people than usual in a small area. This, in an urban environment would not be a problem, but in a rural environment it can be one because the network infrastructure is not prepared to serve many people at the same time in remote areas like the one described in this scenario. Here it will be needed to add some solution to the network to increase network serving capability for specific communications, such has the public safety agencies communications.

The requirements for emergency communications defined by ETSI are basically the same as in the previous scenario: Good quality (sufficient for good understanding) speech, short setup times for the calls and end to end delay below 400 ms and some specific services such as group communications, status monitoring to transmit data such as vital signs, location services, data services for a diverse number of data applications that have in common the need of throughput, the need of the information arrive to the destination in a certain time frame and the preservation of data integrity.

- As stated earlier, it will be needed to add some solution to the network to increase network serving capability for specific communications. Here, has in the previous scenario, the more suitable solutions are the utilization of some sort of COW to provide extra coverage and extra network resources to fulfill the need of the rescue teams.
- Once again, the architecture presented suits this situation because slicing can be useful because, as the resources can be scarce it is even more important to manage them and distribute them in the most adequate way through the existent slices to try to serve the need of emergency communications. This resource distribution through the slices can be done on demand, what is a major advantage in this scenario because the number of actors on scene can change in a matter of minutes or hours and the network is able to positively respond to these changes. The priorities usage can be useful here too, especially among emergency communications because some can have more priority than others.
- The choice of LTE as the elected technology allow to positively respond to ETSI emergency communication requirements because LTE allows the usage of Mission-Critical PTT (MCPTT), group communications, proximity and location services and data and multimedia services and is able to respond to setup call time and delay requirements.

5

Conclusion

Contents

5.1 Conclusions 65
5.2 Limitations and Future Work 65

In this final chapter will be described the conclusions taken, will be addressed the system limitations and the future work that can be realized in this regard.

5.1 Conclusions

After analyzing the standards and technologies PSSs that are currently used, it is possible to understand that the systems used to protect the population still depend on outdated technologies and still have many undesirable flaws such as lack of resilience and interoperability appropriate. Public Safety Technology is an area with a lot of room for evolution, mainly with the use and integration of the latest technologies. With the intensive study carried out on the various technologies available on the market and those that are now emerging, it is clear that it is possible to create new and better protection systems for the population.

Legacy systems like TETRA are capable of serving the basic communication needs in Public Safety matters but not much more. Recent technologies like LTE secure the basic PSN requirements, offer better network performance (latency, call establishment times, delays, data speed, ...) and offer new relevant services (geolocation, real-time image and video, ...) than legacy systems.

Besides that, recent technologies like Software Defined Networking (SDN) and Network Function Virtualization (NFV) also described in this document are a great addition to the mobile technologies because it allows the flexibility and programability of the network, what bring new opportunities in sharing networks and reducing costs.

Fortunately, some research efforts started to appear, with proposals and projects using new technologies in Public Protection and Disaster Relief (PPDR), but there is still plenty of room for innovation in this area.

5.2 Limitations and Future Work

Given everything that was described in the evaluation of the proposal, it is clear that the next steps would be the total emulation of the suggested network followed by the testing of some specific features of emergency communications in the emulated network such as a push to talk module and/or group communications. First, it would be necessary to take the emulation performed using OpenAirInterface and integrate Software Defined Networking (SDN) into it, by integrating FlexRAN, as a RAN controller and possibly OpenDayLight as a core network controller. It will also be necessary to integrate a new node in order to be able to orchestrate the network.

Then, it is necessary to make some changes to the emulator's base code so that it is possible to access the virtual machine of each node to allow actions to be performed within each user's equipment

or, instead of using emulated UE, integrate android equipment as end user emulation. Any of these solutions will, in theory, allow applications to run on OpenAirInterface LTE network user terminals.

Then, a great test that we wanted to do was to deploy a server application in the core network were it is supposed to be deployed an application like Push To Talk (PTT) and/or group communication and run that application in each user to prove that this type of applications can run in networks with characteristics close to the ones described.

Regarding System limitations, network slicing still have some uncertainties, specially regarding the much needed isolation, of all types. Critical systems such as Public Safety Network (PSN) cannot suffer from interference from other systems.

The possibility of implementing a completely new and redesigned Public Safety System (PSS) is, unfortunately, scarce. As stated earlier, this type of networks and systems is very limited by Politics and Governmental ties, so implementing a solution like the suggested one is a very slow process, with many barriers and obstacles. Only Time, obsolescing and, unfortunately, catastrophic events, have been the drivers for modernization of this type of infrastructures.

Bibliography

[1] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 12 2007.

[2] D. Câmara and N. Nikaein, Eds., *Wireless Public Safety Networks 1*. ISTE Press Ltd and Elsevier Ltd, 2015.

[3] R. Ferrús and O. Sallent, *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*. John Wiley & Sons, Ltd, 2015.

[4] D. Srinivasarao, P. D. Pradeep, and B. A. Kumar, "A Survey of Emergency Communication Network Architectures," *International Journal of u- and e-Service, Science and Technology*, vol. 8, no. 4, pp. 61–68, 4 2015.

[5] W. Yu, H. Xu, J. Nguyen, E. Blasch, A. Hematian, and W. Gao, "Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions," *IEEE Access*, vol. 6, pp. 70 397–70 425, 2018.

[6] C. M. Machuca, S. Secci, P. Vizarreta, F. Kuipers, A. Gouglidis, D. Hutchison, S. Jouet, D. Pezaros, A. Elmokashfi, P. Heegaard, S. Ristov, and M. Gusev, "Technology-related disasters: A survey towards disaster-resilient Software Defined Networks," in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2016, pp. 35–42.

[7] V. Y. Kishorbhai and N. N. Vasantbhai, "AON: A Survey on Emergency Communication Systems during a Catastrophic Disaster," *Procedia Computer Science*, vol. 115, pp. 838–845, 1 2017.

[8] L. Borenovic and M. Simic, "Test measurements considerations for LTE as future public safety communication technology," in *55th International Symposium ELMAR-2013*, 2013, pp. 243–246.

[9] M. Wetterwald, D. Saucez, X.-n. Nguyen, and T. Turletti, "SDN for Public Safety Networks," Tech. Rep., 2016.

[10] M. Mihailescu, H. Nguyen, and M. R. Webb, “Enhancing wireless communications with software defined networking,” in *2015 Military Communications and Information Systems Conference (MilCIS)*, 11 2015, pp. 1–6.

[11] A. Alnoman and A. Anpalagan, “On D2D communications for public safety applications,” in *2017 IEEE Canada International Humanitarian Technology Conference (IHTC)*, 7 2017, pp. 124–127.

[12] A. Kumbhar, F. Koohifar, I. Güvenç, and B. Mueller, “A Survey on Legacy and Emerging Technologies for Public Safety Communications,” *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 97–124, 2017.

[13] M. Mikulic and B. Modlic, “General system architecture of TETRA network for public safety services,” in *2008 50th International Symposium ELMAR*, vol. 1, no. September, 2008, pp. 10–12.

[14] K. Mehboob, I. M. Umair, and M. S. Ahmed, “TETRA technology: A modern private cellular system,” *2005 Student Conference on Engineering Sciences and Technology, SCONEST*, 2005.

[15] W. Xu, H. Xiang, and H. Yang, “TETRA protocol interfaces features and potential applications in railway,” in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 2, 2002, pp. 1086–1088.

[16] TCCA, “TETRA.” [Online]. Available: https://tcca.info/tetra/tetra/

[17] A. Jarwan, A. Sabbah, M. Ibnkahla, and O. Issa, “LTE-Based Public Safety Networks: A Survey,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1165–1187, 2019.

[18] B. Bertenyi, “LTE Standards for Public Safety–3GPP view,” in *Critical Communications World, 21st-24th May 2013*, no. May, 2013. [Online]. Available: http://www.3gpp.org/IMG/pdf/2013_05_3gpp_ccw.pdf

[19] G. M. S. Association, “Public Safety LTE Networks : State of the Market and Device Ecosystem,” pp. 1–14, 2018.

[20] DAEL, “COW Technical Specifications,” p. 82502, 2002.

[21] A. Merwaday and I. Guvenc, “UAV assisted heterogeneous networks for public safety communications,” *2015 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2015*, pp. 329–334, 2015.

[22] ETSI, “ETSI TS 1 151 021 V13.3.1 (2017 17-02),” vol. 0, pp. 0–26, 2016.

[23] ——, “ETSI TS 137 104 V15.3.0 (2018-07),” vol. 0, 2018.

[24] ——, “ETSI TS 145 005 V9.12.0 (2012-10),” vol. 0, pp. 0–234, 2011.

[25] M. Sauter, *From GSM to LTE*. Wiley, 2011.

[26] G. Heine, *GSM Networks: Protocols, Terminology and Implementation*, 1999, vol. 23, no. 2.

[27] ETSI, "ETSI TR 101 111 V3.0.1 (1997-11)," vol. 48, pp. 230–231, 1985.

[28] ——, "ETSI TS 125 106 V10.2.0 (2012-07)," *Handbook of Computer Networks*, vol. 2, pp. 699–715, 2011.

[29] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, and V. Niemi, *UMTS Networks Architecture, Mobility and Services*, 2nd ed. Wiley, 2005.

[30] J. P. Castro, *The UMTS network and radio access technology : air-interface techniques for future mobile systems*, 2001.

[31] ETSI, "ETSI TS 136 101 V14.3.0 (2017-04)," *European Telecommunications*, vol. 0, p. 70, 2008. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136100_136199/136101/08.02.00_60/ts_136101v080200p.pdf

[32] C. Cox, *An Introduction to LTE, LTE-Advanced, VoLTE and 4G Mobile Communications*. Wiley, 2014.

[33] E. Dahlman, S. Parkvall, and J. Skold, *4G LTE/LTE-Advances for Mobile Broadband*. Elsiver, 2011.

[34] 3GPP, "3GPP TS 23.303," Tech. Rep. Release 15, 2018.

[35] ——, "3GPP TS 23.468," Tech. Rep. Release 15, 2019.

[36] 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.

[37] ETSI, "ETSI TR 138.913 "5G; Study on scenarios and requirements for next generation access technologies"," vol. 0, p. 40, 2018.

[38] GSMA, "5G Spectrum: GSMA Public Policy Position," *Gsma*, no. July, pp. 1–10, 2019. [Online]. Available: https://www.gsma.com/spectrum/wp-content/uploads/2016/06/GSMA-5G-Spectrum-PPP.pdf

[39] Next Generation Mobile Networks Alliance, "5G White Paper," Tech. Rep., 2015. [Online]. Available: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[40] G. A. W. Group, "View on 5G Architecture," Tech. Rep. Feb, 2020. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2019/07/5G-PPP-5G-Architecture-White-Paper_v3.0_PublicConsultation.pdf

[41] C. Black, P. Goransson, and T. Culver, *Software Defined Networks*. Elsevier.

[42] M. S. Olimjonovich, "Software Defined Networking: Management of network resources and data flow," in *2016 International Conference on Information Science and Communications Technologies, ICISCT 2016*. IEEE, 2016, pp. 1–3.

[43] ETSI, "Network Functions Virtualisation,An Introduction, Benefits, Enablers, Challenges & Call for Action," in *SDN and OpenFlow World Congress*, no. 1, 2012, pp. 1–16.

[44] G. Brown, "4G & 5G-Ready Network Slicing," Tech. Rep.

[45] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 80–87, 2017.

[46] Open Networking Foundation, "TR-526 "Applying SDN Architecture to 5G Slicing"," Tech. Rep. 1, 2016.

[47] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Computer Networks*, vol. 167, 2020.

[48] ITU-T, "IMT-2020," Tech. Rep., 2017.

[49] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "SoftRAN," p. 25, 2013.

[50] X. Foukas, N. Nikaein, M. M. Kassem, M. K. Marina, and K. Kontovasilis, "FlexRAN: A flexible and programmable platform for software-defined radio access networks," *CoNEXT 2016 - Proceedings of the 12th International Conference on Emerging Networking EXperiments and Technologies*, pp. 427–441, 2016.

[51] Z. Zhao, P. Cumino, A. Souza, D. Rosário, T. Braun, E. Cerqueira, and M. Gerla, "Software-defined unmanned aerial vehicles networking for video dissemination services," *Ad Hoc Networks*, vol. 83, pp. 68–77, 2019.

[52] R. Bassoli and F. Granelli, "Rapid Deployment of 5G Services Using Drones and other Manned and Unmanned Aerial Vehicles," pp. 219–230.

[53] L. Nagpal and K. Samdani, "Project Loon: Innovating the connectivity worldwide," in *RTEICT 2017 - 2nd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, Proceedings*, 2017, pp. 1778–1784.

[54] M. Rahouti, K. Xiong, T. Chin, and P. Hu, “SDN-ERS: A Timely Software Defined Networking Framework for Emergency Response Systems,” in *2018 IEEE International Science of Smart City Operations and Platforms Engineering in Partnership with Global City Teams Challenge (SCOPE-GCTC)*, 4 2018, pp. 18–23.

[55] M. A. S. Santos, B. A. A. Nunes, K. Obraczka, T. Turletti, B. T. d. Oliveira, and C. B. Margi, “Decentralizing SDN’s control plane,” in *39th Annual IEEE Conference on Local Computer Networks*, 2014, pp. 402–405.

[56] D. Marabissi and R. Fantacci, “Heterogeneous Public Safety Network Architecture Based on RAN Slicing,” *IEEE Access*, vol. 5, pp. 24 668–24 677, 2017.

[57] BEREC, “BEREC Report on infrastructure sharing,” Tech. Rep. 18, 2018. [Online]. Available: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8164-berec-report-on-infrastructure-sharing

[58] 3GPP, “3GPP TS 23.251,” vol. 0, no. Release 15, 2018.

[59] Alcatel, “Network Sharing in LTE,” 2010.

[60] ETSI, “ETSI TS 1 122 346,” vol. 0, 2016.

[61] J. Oueis, V. Conan, D. Lavaux, R. Stanica, F. Valois, J. Oueis, V. Conan, D. Lavaux, R. Stanica, F. Valois, L. T. E. Isolated, J. Oueis, V. Conan, D. Lavaux, R. Stanica, and F. Valois, “Overview of LTE Isolated E-UTRAN Operation for Public Safety,” 2017.

[62] K. Ramantas, E. Kartsakli, M. Irazabal, A. Antonopoulos, and C. Verikoukis, “Implementation of an SDN-enabled 5G experimental platform for core and radio access network support,” *Advances in Intelligent Systems and Computing*, vol. 725, pp. 791–796, 2018.

[63] Hyetra, “Hyetra LTE multi-mode handsets.” [Online]. Available: https://hytera.co.uk/lte

[64] Tisscom, “Tisscom - TETRA + LTE Smartphone.” [Online]. Available: https://tisscom.ru/en/catalog/devices/tetra-lte-smartphone-innovative-tactilon-dabat-device

[65] OpenAirInterface, “OpenAirInterface Wiki.”

[66] ETSI, “Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 1: Earthquake,” European Telecommunications Standards Institute, Tech. Rep. TS 103 260-1, 2015.

[67] ——, “Satellite Earth Stations and Systems (SES); Reference scenario for the deployment of emergency communications; Part 2: Mass casualty incident in public transportation,” European Telecommunications Standards Institute, Tech. Rep. TS 103 260-2, 2015.