UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA MAGISTRALE IN
ICT FOR INTERNET AND MULTIMEDIA

MISSION CRITICAL SERVICES: EVOLUTION OF QoS MANAGEMENT OVER 5G NETWORKS

Relatore: Prof. / Dott. Stefano Tomasin

Laureando/a: Carlo Maria Plazzotta

Correlatore: Dott. Giuseppe Merlino

ANNO ACCADEMICO 2021 – 2022

Data di laurea 13/10/2022

University of Padova

Department of Telecommunications Engineering

Master Thesis in ICT for Internet and Multimedia

Mission Critical Services: evolution of QoS Management over 5G networks

Supervisor

Professor Stefano Tomasin

University of Padova

Co-supervisor

Doctor Giuseppe Merlino

Alea s.r.l.

Master Candidate

Carlo Maria Plazzotta

Academic Year

2021-2022

Abstract

Fifth generation technologies are now present in many sectors of the IT market. Companies, entities and operators are moving to understand how to adapt their products to this technological advance and how to exploit its benefits. In the same way, Mission Critical Services (MCS) and all their stakeholders are also affected by this evolution of the network and therefore it becomes necessary to understand how Quality of Service (QoS) management, the cornerstone of MC communications, can be carried out and supported in the new 5G networks. The intent of this thesis is to understand how 5G networks and MC communications can coexist, exploiting the benefits that the 5G cellular technology brings with it. Two possible solutions and/or strategies are therefore presented in order to allow MC communications on 5G networks.

The first is based on the concept of "network slicing" which allows to define on the same physical infrastructure a set of independent logical and/or virtual networks capable of operating simultaneously.

The second strategy uses the innovative architecture of the 5G Core network (5GC), where each element of the network, called Network Function (NF), is an independent virtual entity that communicates with the other network functions through the different services they offer to be invoked or invoke in turn. In particular, the N5 interface is exploited to manage the QoS rules, which are fundamental for the creation of MC services.

Contents

Listing of figures

Listing of tables

Listing of acronyms

3GPP ..... 3rd Generation Partnership Project

5G ..... 5th Generation

5GC ..... 5th Generation Core network

AF ..... Application Function

gNB ..... New Generation Base Station

IMS ..... IP Multimedia Subsystem

ITU ..... International Telecommunications Union

KPI ..... Key Performance Indicator

MCS ..... Mission Critical Services

NF ..... Network Function

NFV ..... Network Function Virtualization

NG RAN ..... New Generation Radio Access Network

NR ..... New Radio

PCC ..... Policy and Charging Control rules

PCF ..... Policy Control Function

PTT ..... Push-to-Talk

QCI ..... Quality-of-service Class Identifier

QoS ..... Quality of Service

RTP ..... Real-time Transport Protocol

SBA ..... Service Based Architecture

SDN ..... Software Defined Networking

SIP . . . . . Session Initiation Protocol

SLA . . . . . Service Level Agreements

UE . . . . . User Equipment

URI . . . . . Uniform Resource Identifier

1 Introduction

Public safety emergencies like natural disasters, fires, terrorist attacks, and, in general, situations where human life is in danger, are progressively more and more frequent, and the public security forces need increasingly high-performance tools to intervene quickly and effectively.

For this reason, for some years now, several global organizations in the telecommunications sector, such as the 3rd generation partnership project (3GPP), have begun to invest in the standardization of Mission Critical Services (MCS). They have the purpose of providing reliable emergency communications on the public cellular network, to allow the exchange of multimedia information, both audio and video, in real time, guaranteeing a higher priority than other communications in the network.

Users of MC services require their suppliers to strictly comply with certain Service Level Agreements (SLAs). It thus becomes of fundamental importance, for the companies that provide these services, to understand how to intervene on the mobile network to manage and obtain optimal Quality of Service (QoS) levels.

In this context, Fifth Generation (5G) networks can play a key role by providing improvements in various aspects, such as low-latency, high availability, and reliability.

Moreover, the new structure of the 5G network, much more flexible and adaptable to the different needs of users, allows the creation of multiple logical networks, tailored to specific use cases and requirements, that run on the same infrastructure independently from each other. Such a concept is called Network Slicing.

The objective of this essay is to analyze the QoS management over the new 5G cellular net-

works in order to guarantee high priority MC communications. To do so the Network Slicing technology and the *Npcf_PolicyAuthorization* service active on the N5 interface of the 5G Core network (5GC) have been studied.

The rest of this thesis is organized as follows:

- Chapter 2 explains the major benefits and features that 5G technologies brings with it, showing the reference architecture of a 5G telecommunication network and presenting the characteristics of its main functional elements. Next, it overviews the main properties of the Mission Critical Services and how they are implemented over the actual 4th generation (4G) cellular networks. Finally, it describes which are the most relevant key points and problems between 5G networks and MC communications.
- In Chapter 3 the Network Slicing technology is exploited. After its definition, different application scenarios are considered and a list of performance indicators is presented in order to hypothesize the creation of a dedicated Network Slice for MC communications.
- Chapter 4 is dedicated to the development of the N5 interface and the tools used to create the testbed infrastructure.
- Chapter 5 presents the results achieved and the QoS management over the N5 interface.
- Concluding remarks are reported in Chapter 6.

2
State of the Art

2.1 5G Cellular Wireless Network

By now owning a mobile phone that makes calls, sends messages and allows the exchange of different types of media is within the reach of an increasing number of people.

This increase in users, also called User Equipments (UEs), also determines a growth in the number of connections that the cellular network must support and guarantee.

Furthermore, in recent years, the type of messages that users exchange is changing too: photos, videos, video calls, live streaming, etc. are types of messages increasingly present in cellular networks and require more performing connections.

It is in this context that the fifth-generation (5G) technological standard for cellular networks fits.

The International Mobile Telecommunications-2020 (IMT-2020), called also 5G, is a program issued by the International Telecommunication Union (ITU) with the purpose of improving the current fourth-generation (4G) of mobile networks in several aspects.

5G technology aims to achieve greater efficiency and versatility in supporting network applications through the exploitation of some major features and benefits:

- **Increased speed and bandwidth:** with an important spectral efficiency enhancement, 5G networks target higher data rates (up to 10 Gbps) and an improved available spectrum (high bands of 30-40 GHz);

- **Low latency:** to support "real time" applications like autonomous driving, critical communications and industrial automation, 5G networks had to invest a lot of resources to guarantee very low latency times (below 5 milliseconds);

- **Software defined network and network function virtualization:** due to the wide range of applications to which 5G provides communications services, the New Radio (NR) architecture has been designed to allow a possible "softwarization" of network functions. Consequently, software defined networking (SDN), network function virtualization (NFV) and cloud computing are fundamental technologies for making full use of the power of a 5G network [1];
- **Density:** the number of users and devices that exploits the network is increasing very fast, so 5G network have to support a larger amount of connections, up to 1000000 connections/km^2, while maintaining very high availability;
- **Power consumption:** the 5G mobile network aims to reduce power consumption by 90% with respect to 4G. This is a very important benefit for applications where efficiency is the key problem, like Internet of Things (IoT) devices.

The features listed above are the most important and discussed ones, but they are just some of the many innovations that 5G brings with it.

One of these novelties is certainly the 5G Core Network Architecture that it is discussed in the next section.

2.2 5G Network Architecture

The 5G Network is divided in two parts: the New Generation Radio Access Network (NG RAN) and the 5G Core Network (5GC). The NG RAN oversees the direct connection with the UE, like cellphone, computer or remotely controlled machine, and links UEs to the Core Network. It includes base stations, called New Generation Node Base (gNB), antennas and all those components necessary to provide wireless connectivity to the UEs.

The 5GC is the part of the network handling the functionalities of the cellular network and the routing of the data to and from external data networks. The 5GC is composed of several elements called Network Functions (NFs). Up to 4G, for each function a specific hardware and software was deployed, with 5G, functions are implemented in software which can be run at different locations in space and time. This design choice allows the network to react to the many and different users' needs with high flexibility and scalability, adapting network resources to the specific requested workload.

The 5GC NFs support a collection of services and each NF offers one or more services to other NFs in the network. These services are made available over Service Based Interfaces in the Service Based Architecture (SBA). Therefore, the functionalities supported in a specific NF are provided and accessible over API [2].

For each interaction between network functions, one of these acts as "Service Consumer", and the other as a "Service Producer". As defined in [3] and [4], SBIs use HTTP/2 protocol with JSON as the application layer serialization protocol. Network Functions interact among them exploiting the HTTP GET, PATCH, POST, PUT and DELETE methods. At each HTTP request or response, there are mandatory and/or custom headers to be used, together with the appropriate Uniform Resource Identifiers (URI) in compliance with what defined by the standards.

2.3 5G Network Elements

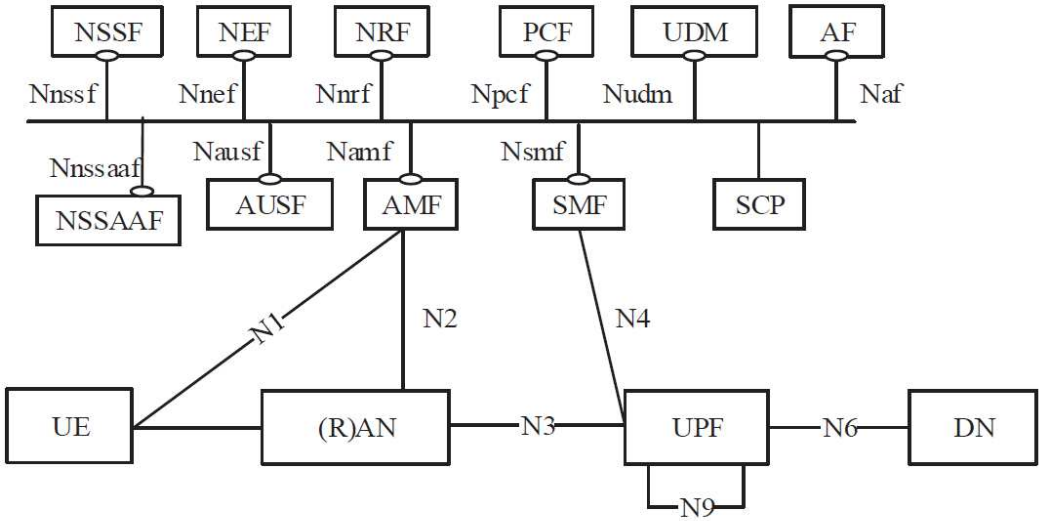

Figure 2.1: 5G system architecture.

The standard [5] defines more than 20 NFs for the 5G System architecture, but not all of those are necessary for a 5G network to work. In Figures 2.1 and 2.2, taken from [5], are shown some of the most important NFs with their offered services and available interfaces.

Below are listed and presented the most relevant NFs for this thesis work.

AMF – Access and Mobility Management Function

The AMF is the second entry point to the core network from the RAN, it supports establishing encrypted signaling connections towards UEs, allowing these to register, to be authenticated, and to move between radio cells in the network. The AMF relays all session management-

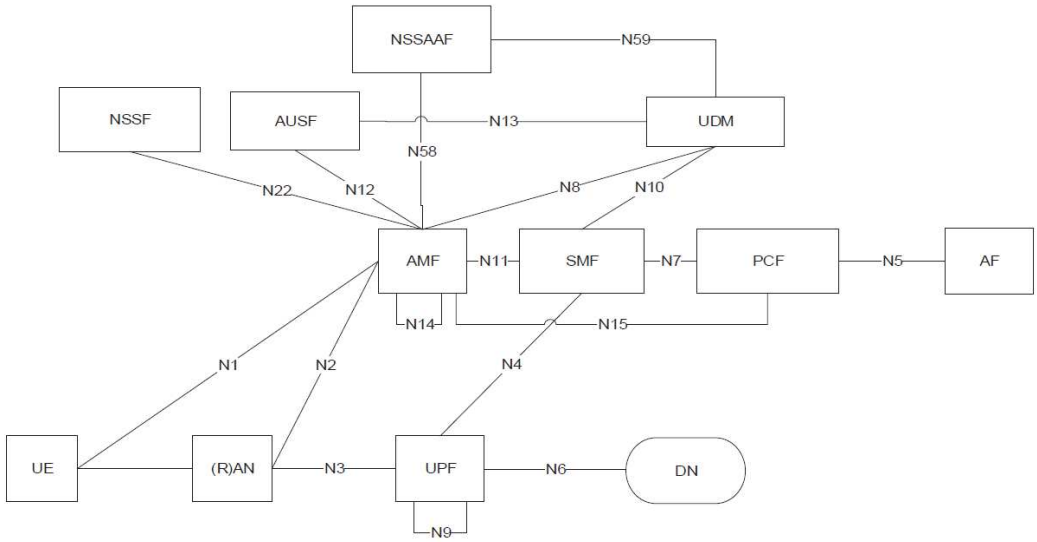

Figure 2.2: 5G system architecture in reference point representation.

related signaling messages between the devices and the SMF Network Function. Furthermore, the AMF relays UE policy messages between the PCF and the UE.

SMF – Session Management Function

The SMF has the responsibility to setup of the connectivity for the UE towards Data Networks as well as managing the User Plane for that connectivity. The SMF is the control function that manages the user sessions including establishment, modification and release of sessions, and it can allocate IP addresses for IP PDU sessions.

The SMF interacts with other NFs through service based interfaces, and it also selects and controls the different UPF network functions that can be present in the network.

The SMF interacts with the PCF Network Function to retrieve policies which are used by the SMF to configure the UPF for the PDU session.

UPF – User Plane Function

The UPF processes and forwards user data. The functionality of the UPF is controlled by the SMF. It interconnects with external IP networks and acts as an anchor point for the UEs towards external networks. The UPF performs various types of processing of the forwarded data: it generates charging data records and traffic usage reports, it can apply "packet inspection", analysing the content of the user data packets for usage either as input to policy decisions, or as basis for the traffic reporting.

5G Core UPF can be deployed in series and separately from the rest of the network, e.g. one UPF distributed towards the edge of the network, and one UPF located in a more central

network site.

The UPF can also apply Quality-of-Service (QoS) marking of packets towards the radio network or towards external networks. This can be used by the transport network to handle each packet with the right priority in case of congestion in the network.

NRF – Network Repository Function

The NRF is a repository of the profiles of the NFs that are available in the network. The purpose of the NRF is to allow service consumer (e.g., an NF) to discover and select suitable service producers i.e., NFs and NF services without having to be configured beforehand.

When a new instance of a network function deployed or changed, e.g., due to scaling, the NRF is updated with the new profile information. The NRF profile can be updated by the NF itself or by another entity on behalf of NF. The NF profile in the NRF contains information like NF type, address, capacity, supported NF services and addresses for each NF service instance.

UDR - Unified Data Repository

The UDR is the database where various types of data are stored. Important data is of course the subscription data and data defining various types of network or user policies. UDR storage and access to data is offered as services to other NFs, specifically UDM, PCF, and NEF.

UDM – Unified Data Management Function

The UDM is a front-end for the user subscription data stored in the UDR. The UDM uses subscription data that may be stored in UDR to execute application logic like access authorization, registration management and reachability for terminating event e.g., SMS.

When a UE attaches to the system the UDM authorizes the access and performs several checks of supported features, barring and restrictions due to e.g., roaming.

The UDM generates the authentication credentials that the AUSF use to authenticate UEs.

The UDM also keeps track of which AMF instance is serving a specific UE and also the SMF(s) that is serving its PDU sessions.

AUSF – AUthentication Server Function

The AUSF is responsible for handling the 3GPP and non-3GPP authentication in the home network, based on information received from the UE and information received from the UDM.

PCF – Policy Control Function

The PCF provides policy control for sessions management related functionality, for access and mobility related functionality and for UE access selection and PDU session selection related functionality.

For session management the PCF interacts with application functions and the SMF to provides authorized QoS and charging control for service data flows, PDU session related policy

control and event reporting for PDU sessions.

The PCF also interacts with the AMF for the access and mobility policy control and provides policy information to the UE (via the AMF). These policies include discovery and selection policies for non-3GPP networks, session continuity mode selection policy, network slice selection policy, data network name selection policy and more.

NSSF – Network Slice Selection Function

The NSSF selects the (set of) network slice instances for the UE and the set of AMFs that should serve the UE. The AMF can be dedicated to one or more network slices.

The NSSF also determines the allowed and configured NSSAI (Network Slice Selection Assistance Information) and, if needed, the mapping to the subscribed S-NSSAIs (Single - Network Slice Selection Assistance Information).

NEF – Network Exposure Function

The NEF supports the exposure of events and capabilities from the 5G system towards applications and NFs inside and outside the operator's network. Examples of events that can be made available in 3GPP Release 15 are the location of UE, reachability, roaming status, and the loss of connectivity.

The NEF can also support provisioning of foreseen UE behavioural information, this information can be further used in, e.g., the AMF to tune the system and UE behaviour.

The NEF can in addition support external applications to manage for specific QoS and/or charging. It can be used by authorized applications to request specific QoS/priority handling for a session, and for setting applicable charging party or charging rate.

NWDAF – Network Data Analytics Function

The NWDAF is a function that can collect data, perform analytics and provide the results to other NFs. The network functions may adapt their behaviour based on the reported results from the NDWAF. The PCF and NSSF can consume network analytics from the NWDAF and e.g., NSSF may use the network slice load level information for slice selection.

Data collected from the NWDAF can also be consumed by an artificial intelligence system in the network in order to independently and dynamically contact other NFs so that the network adapts and changes its operative status.

AF – Application Function

The AF is a 3GPP representation of applications either inside or outside the operator's network that interacts with the 3GPP Core Network. Applications may interact and influence some aspects of the 5G core, they may influence traffic routing (e.g., an edge computing application), they may access the exposure function to interact with the PCF to influence QoS and charging policies. Applications considered trusted by an operator may be allowed to interact directly with relevant Network Functions. Other AFs may use the external exposure framework

via the NEF to interact with relevant NFs.

2.4 Mission Critical Services (MCS)

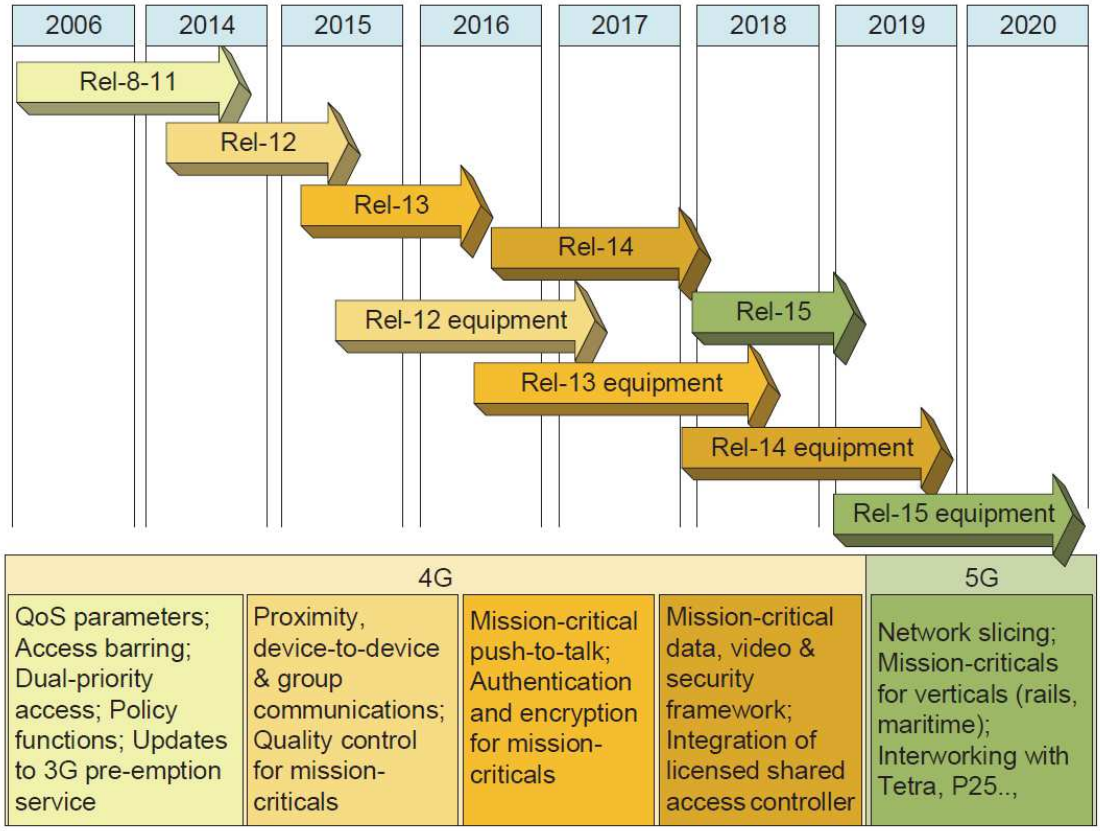

Figure 2.3: Mission Critical Services in 3GPP standardization.

Public safety is a relevant issue that needs to be faced every day. Emergencies and accidents are unpredictable events and the different safety operators, e.g., policemen, firefighters, and first aid workers, must be able to respond promptly and effectively.

Therefore, in order to optimize the intervention of these operators through fast and effective communications, a platform for mission critical (MC) communications and MC Services has been a key priority of 3GPP in recent years and is expected to evolve into the future by taking more requirements, from different sectors of the global critical communications industry [6].

In Figure 2.3 it is possible to see the evolution of the supporting technologies, included in different releases of 3GPP standardization, developed to enable critical communications over

commercial networks [7].

Traditionally public safety communications services have been provided with narrowband professional mobile radio (PMR) systems such as terrestrial truncated radio (TETRA) and Tetrapol in Europe and project 25 (P25) in North America [7].

From Release 13 the trend went towards commercial mobile broadband networks, e.g., long term evolution (LTE), with the standardization by 3GPP of Mission Critical Push-to-Talk (MC PTT), completed in 2016.

MCPTT was the first major step in a series of MC Services and functionalities demanded by the market. In Rel-14, completed in 2017, 3GPP added new MC Services and enhancements to its repertoire of standardized applications (Enhancements to MC PTT, MC Data, and MC Video).

In the first phase of 5G system, i.e., in Release 15, all the mission-critical services are enhanced and interworking with other systems such as TETRA is used so that services are provided to mission critical users with different radio interfaces.

Release 16, issued in March 2020, was a major release for the MC Services project, not least because it has brought the IMT-2020 submission, for a full 3GPP 5G system, to its completion. As part of it, MC Services were extended to address a wider business sector than the initial rather narrow public security and civil defence services for which they had originally been developed. The same standards could be used for commercial applications (from taxi dispatching to railway traffic management), bringing enhanced reliability to those MC Services through wider deployment, and reduced deployment costs due to economies of scale.

More 5G system enhancements are reaching maturity with the completion of Release 17, that is currently being developed, and with them more possibilities and features for MC Services are under study.

Below are briefly presented the three main categories of Mission Critical Services that are now available in the market.

Mission Critical Push-To-Talk (MC PTT)

MC PTT was firstly defined by 3GPP in [8]. The MC PTT Service can be used for public safety applications and also for general commercial applications (e.g., utility companies and railways).

It makes use of capabilities included in Group Communications System Enablers and Proximity Services, with additional requirements specific to the MC PTT Service.

A Push To Talk service provides a method by which a smartphone can be used as a walkie-talkie. In fact, through the MC PTT Service application installed on the device, a user con communicate with another user by pressing a button on his smartphone.

The MC PTT Service is intended to support communication between several users (a group call), where each user has the ability to gain access to the permission to talk in an arbitrated manner. However, the MC PTT Service also supports Private Calls between pairs of users.

The MC PTT Service allows users to request the permission to talk (transmit voice/audio) and provides a deterministic mechanism to arbitrate between requests that are in contention (i.e., Floor control). When multiple requests occur, the determination of which user's request is accepted and which users' requests are rejected or queued is based upon a number of characteristics (including the respective priorities of the users in contention). MC PTT Service provides a means for a user with higher priority (e.g., MC PTT Emergency condition) to override (interrupt) the current talker.

MC PTT Service also supports a mechanism to limit the time a user talks (hold the floor) thus permitting users of the same or lower priority a chance to gain the floor.

Mission Critical Data (MC Data)

MC Data is defined in [9]. MC Data defines a service for Mission Critical Data services. As well as voice services, current mission critical users have been increasing their use of data services, including low throughput services on legacy networks and data services on commercial networks. This need will continue to grow with the creation of the new multimedia services. The MC Data service needs to provide a means to manage all data connections of mission critical users in the field and provide relevant resources to the ones who need it. For example mission critical users already use event manager software along with the voice system.

The MC Data Service will reuse functions including end-to-end encryption, key management, authentication of the sender, etc. in order to provide group communications for data services. As for all mission critical services, users affiliate to groups in order to receive communications directed to the group. In addition, the MC Data Service will provide a set of generic capabilities such as: messaging, file distribution, data streaming, IP proxy, etc. Also, the MC Data Service will provide specific services such as conversation management, data base enquiries, internet access, robots control.

Mission Critical Video (MC Video)

MC Video service, as defined in [10], includes:

- video capture and encoding of video information;
- secure streaming and storing of the video information;
- video decoding and rendering of the video information;
- processing of the video information, including the ability to annotate video frames and recognize video features;
- mission critical and public safety level functionality (e.g. group sessions, affiliations, end-to-end confidentiality, emergency type communications) and performance (e.g. low latency);
- definition and configuration of MC Video groups and applications;

- configuration of the MC Video users' profiles and of the MC Video UEs;
- interoperability with other services and systems.

While the streaming of video is part of the MC Video Service, the non-real-time or offline transfer of a video clip stored as a file containing video data is covered by the MC Data Service.

MC Video makes use of many of the same capabilities that were originally defined for MC PTT and now are mostly specified at stage 1 in the MC Common Requirements (MC CoRe) specification [11]. Such capabilities include, but are not limited to, Group Communication, Group Management, Affiliation, Security and Confidentiality.

This thesis work fits between Rel-16 and Rel-17 where the 5GC network with its features and how they can be reached from external applications has already been presented by the 3GPP as well as MC Services are well defined and launched by now. However, the concrete connection among 5GC and MC Services has yet to be developed and it is at this point that this thesis aims to give a solution.

2.4.1 Mission Critical Services over 4G

MC communications, as seen above, were born and developed at the same pace as the evolution of 4G networks.

Key enabling technologies for critical communications over 4G networks were device-to-device (D2D) communications and proximity services (ProSe), group communications, MC PTT, MC Video, and MC Data, quality of service (QoS) and prioritization mechanisms including pre-emption and end-to-end security.

To access the MC Services, like MC PTT, each user has its own credentials and level of power that defines what he can and cannot do.

Often, during an emergency, several operational teams (called Groups in MC Services) are organized in order to better manage the communications between the various components. They are then entrusted with a basic MC identity whose possibilities of action are limited. In each team a reference person is defined who is responsible for it and who has an MC identity able to organize and manage the communications of his team (for example, defining the type of communications that a user can make or deciding who in that moment may or may not transmit, etc.). Some figures are then set up to organize and command all the different operational teams (called Administrators) and monitor the global situation (called Dispatchers). These users usually have the highest possible privileges and are able to: create, modify and delete the different communication groups, they can add, remove or move the different users in the various communication groups, they can dynamically modify the various privileges of

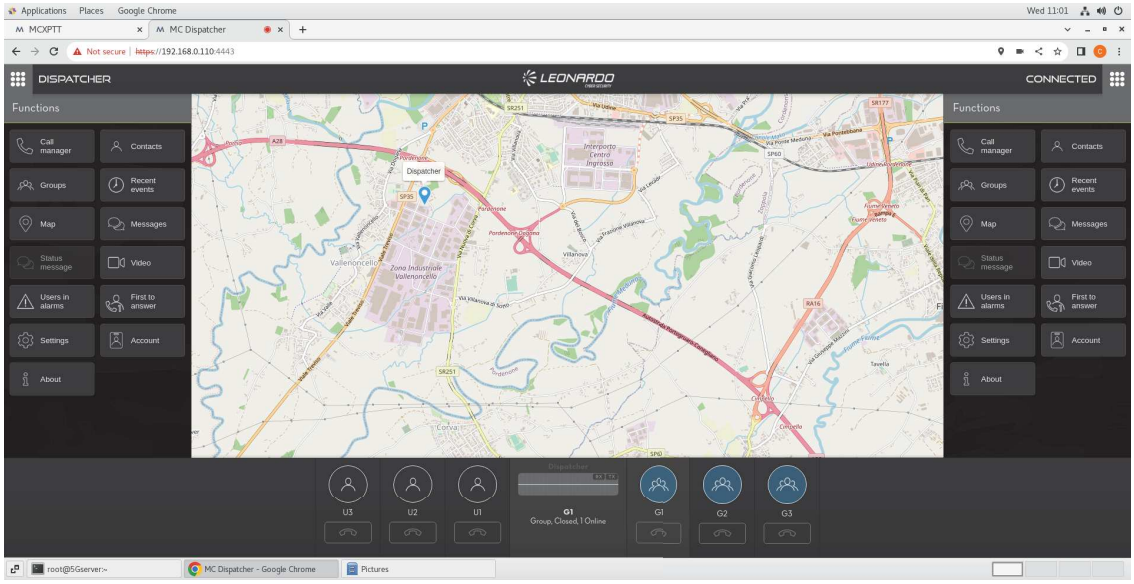

Figure 2.4: Alea S.r.l. Dispatcher point of view.

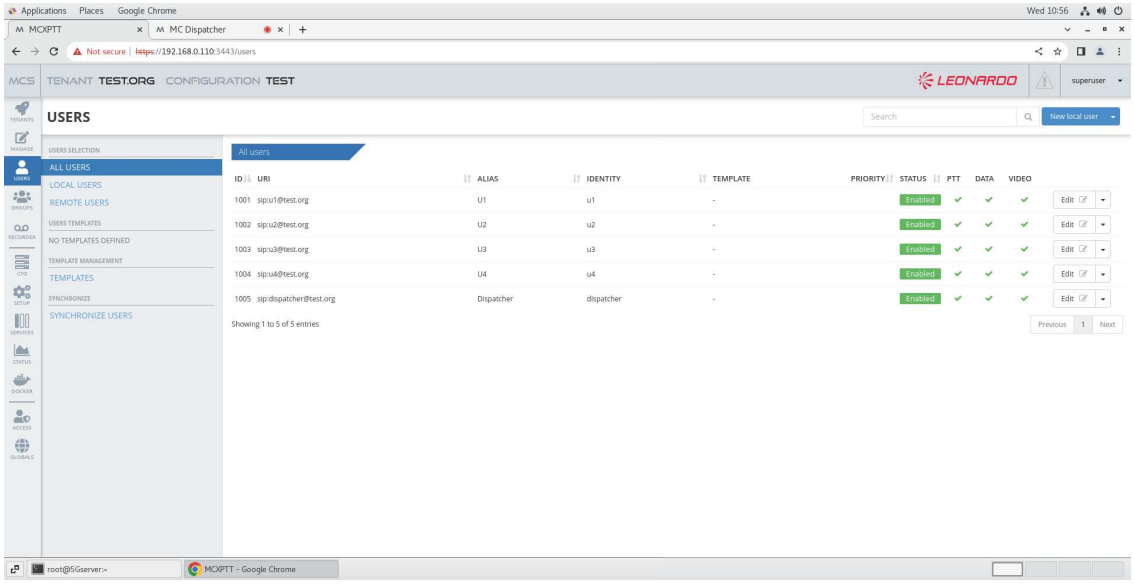

Figure 2.5: View of all users from Administrator.

each individual user or group and can monitor and record all communications that occur during an emergency as well as view the position of each individual user on the map. In Figure 2.4 we see the Dispatcher point of view taken from the MCX application provided by Alea S.r.l.: the lower part shows all the different group calls with their users, while the right and the left show various tools to monitor and manage all the different mission critical communications

that are going on in the area. In Figure 2.5 we see the point of view of the Administrator taken from the MCX application provided by Alea S.r.l. In particular the image shows the list of all the users with their ID, Uniform Resource Identifier (URI) and what type of communications they can perform. Note that on the right is possible to edit the configuration and privileges for each user.

As it is possible to see in Figure 2.5, each user is defined by an URI that starts with the word *sip*. This because Mission Critical services, whether they are PTT, Data, or Video, are managed by the Session Initiation Protocol (SIP). SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls, and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these [12].

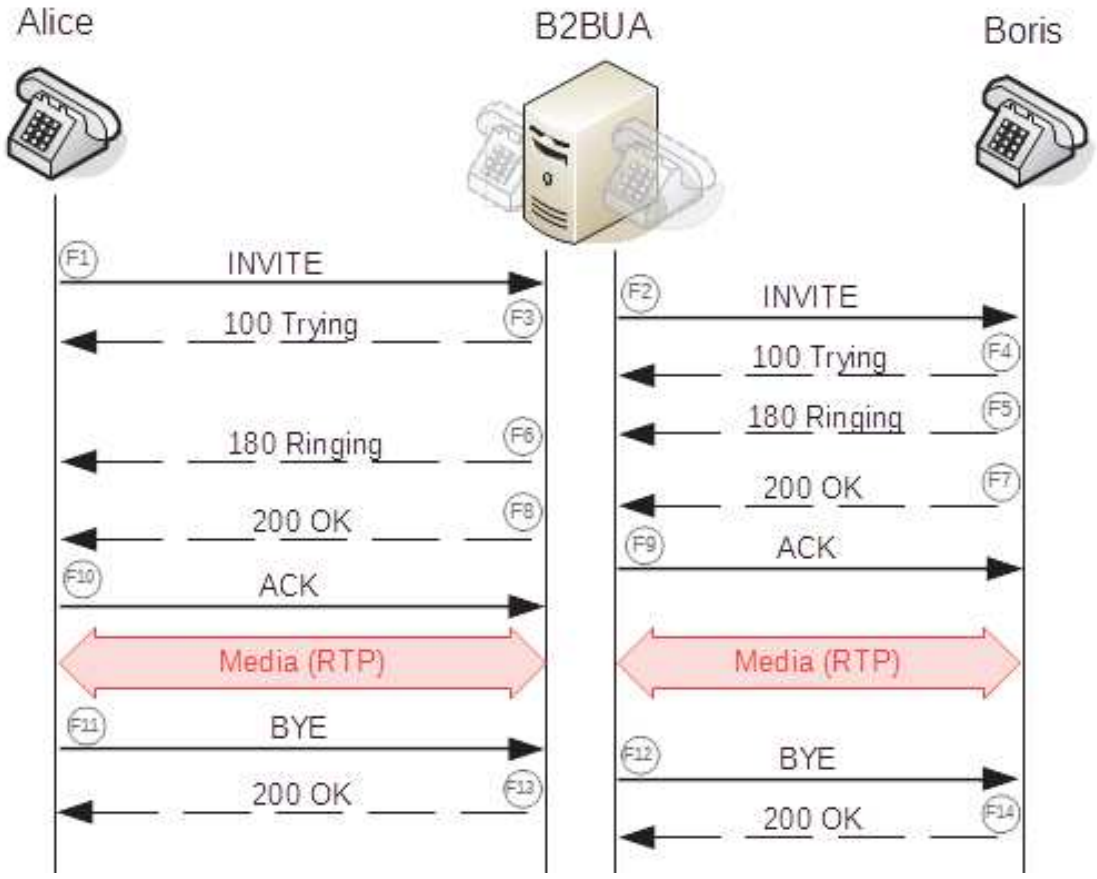

Figure 2.6: Example of establishment of a SIP session.

SIP works in conjunction with several other protocols that specify and carry the session me-

dia. Most commonly, media type and parameter negotiation and media setup are performed with the Session Description Protocol (SDP), which is the payload of SIP messages. SIP can be used with the User Datagram Protocol (UDP), the Transmission Control Protocol (TCP), and the Stream Control Transmission Protocol (SCTP). The protocol may be encrypted with Transport Layer Security (TLS). For the transmission of media streams (voice, video) the SDP payload carried in SIP messages typically employs the Real-time Transport Protocol (RTP) or the Secure Real-time Transport Protocol (SRTP) [13].

Figure 2.6 shows an example of call carried out by the SIP protocol.

Critical communications need low latency, high priority together with high availability and reliability, therefore, various QoS control mechanisms must be used to guarantee these required features.

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

The QoS Class Identifier (QCI) is a mechanism used in 3GPP LTE networks to ensure carrier traffic is allocated the appropriate QoS as depicted in Table 2.1. For each QCI class a resource type that is either guaranteed bit rate (GBR) or non-guaranteed bit rate (NGBR) is given and every QCI is associated with a priority level. Note that MCS has the highest priority in the defined QCI classes, with priority level 5 as the highest priority level.

In the 4G LTE network, enforcement of QoS policies is based on several mechanisms. Creation of dedicated bearers and dynamic QoS control is enabled through the Policy and Charging Rules Function (PCRF), an element in the Evolved Packet Core (EPC or the LTE Core Network).

The PCRF controls the provisioning of policy and charging control (PCC) rules on the Service Control Gateway. Dynamic policy control takes place when a dynamic-policy-control policy and charging enforcement function (PCEF) profile is assigned to a subscriber.

To directly communicate with the PCRF to install, activate, modify or deactivate a rule on the Service Control Gateway PCEF at any time, the Application Function (in this case a Mission Critical Server) shall use the Rx interface. The definition of the Rx interface and its functionalities are given in [14].

The protocol over the Rx interface is based on Diameter, which implements different commands that can be carried in the Diameter message as AVPs (Attribute Value Pair) collection.

2.4.2 5G and MCS: key points and main problems

5G technology comes as an evolution of the cellular networks that currently exist and therefore many of the previous mechanisms used in 4G networks continue to be supported. At the

Table 2.1: 3GPP LTE QCI.

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

same time, however, it introduces many innovations with the aim of improving the general performance of the cellular network.

For these reasons, some tools in 5G networks are simply a development of those previously used in 4G (e.g., 5G QCI mechanism and N5 interface), while others are entirely new (e.g., Network Slicing).

The QCI mechanism in 5G is called 5G QCI or 5QI and a very similar table (Table 2.2), like Table 2.1, is defined. However the difference is that 5QI applies to a flow, carried at some point in a bearer, while QCI applies to a bearer within which certain types of flows are expected.

To guarantee to MC communications the QoS policies and rules defined in Table 2.2, a solution can be the interaction over the N5 interface between the Npcf_PolicyAuthorization service provided by the PCF NF present in the 5G Core and the AF (in this case the Mission Critical Server in the SIP Core).

Table 2.2: 3GPP 5G QCI (5QI).

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget	Packet Error Rate	Default Maximum Data Burst Volume	Default Averaging Window	Example Services
1	GBR	20	100 ms	10^{-2}	N/A	2000 ms	Conversational Voice
2		40	150 ms	10^{-3}	N/A	2000 ms	Conversational Video (Live Streaming)
3		30	50 ms	10^{-3}	N/A	2000 ms	Real Time Gaming, V2X messages, Electricity distribution - medium voltage, Process automation - monitoring
4		50	300 ms	10^{-6}	N/A	2000 ms	Non-Conversational Video (Buffered Streaming)
65		7	75 ms	10^{-2}	N/A	2000 ms	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66		20	100 ms	10^{-2}	N/A	2000 ms	Non-Mission-Critical user plane Push To Talk voice
67		15	100 ms	10^{-3}	N/A	2000 ms	Mission Critical Video user plane
75							
71		56	150 ms	10^{-6}	N/A	2000 ms	"Live" Uplink Streaming
72		56	300 ms	10^{-4}			
73		56	300 ms	10^{-8}			
74		56	500 ms	10^{-8}			
76		56	500 ms	10^{-4}			
5	Non-GBR	10	100 ms	10^{-6}	N/A	N/A	IMS Signalling
6		60	300 ms	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100 ms	10^{-3}	N/A	N/A	Voice, Video (Live Streaming) Interactive Gaming
8		80	300 ms	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		90					
69		5	60 ms	10^{-6}	N/A	N/A	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
70		55	200 ms	10^{-6}	N/A	N/A	Mission Critical Data (e.g. example services are the same as 5QI 6/8/9)
79		65	50 ms	10^{-2}	N/A	N/A	V2X messages
80		68	10 ms	10^{-6}	N/A	N/A	Low Latency eMBB applications Augmented Reality
82	Delay Critical GBR	19	10 ms	10^{-4}	255 bytes	2000 ms	Discrete Automation
83		22	10 ms	10^{-4}	1354 bytes	2000 ms	Discrete Automation
84		24	30 ms	10^{-5}	1354 bytes	2000 ms	Intelligent transport systems
85		21	5 ms	10^{-5}	255 bytes	2000 ms	Electricity Distribution - high voltage

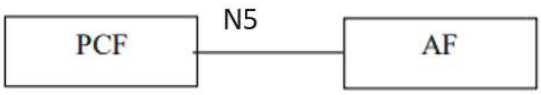

Figure 2.7: N5 interface.

This interface is the evolution of the Rx interface available in the EPC between PCRF and AF, since the PCRF function is no more present in the 5GC network.

The Npcf_PolicyAuthorization Service, as defined in [15] and in [16], authorises an AF request and creates policies as requested by the authorised NF service consumer for the PDU (Protocol Data Unit) session to which the AF session is bound to.

Another possible solution to ensure that 5G networks can support MC communications in

any environment is the exploitation of the concept of Network Slicing which is covered in the next Chapter.

3 Network-Slicing Based MC Networks

Today's market increasingly favors communication to a targeted audience: the cases in which, regardless of the product or service offered, the goal was to reach as many people as possible and how to focus on quantity is less relevant. The vertical market aims to meet these new needs, focusing on a well-defined customers.

To guarantee these different services, over-the-top operators (OOT), i.e. companies that traditionally act as controllers or distributors of services, media contents, and application via Internet, have specific QoS requirements to fulfill, established with service level agreements (SLAs) and assessed by key performance indicators (KPIs).

In this scenario, the flexibility of the 5G architecture offers a perfect solution to meet the needs of such a market: Network Slicing.

3.1 Definition

Network Slicing is a paradigm, where logical networks/partitions are created with appropriate isolation, resources and optimized topology to serve a purpose or service category (e.g., use case/traffic category) or customers (logical system created "on demand") as defined by 3GPP in [17].

This is possible thanks to the new scalable and flexible nature of 5G networks that permits to implement NFs as pieces of software embedded in light virtual machines (e.g., Docker) and executed using a cloud infrastructure, whose servers are spread all over the 5G network and are interconnected by an agile SDN (Software Defined Network). By using such a cloud-based deployment, there is a complete decoupling of the NFs from both the execution hardware and the interconnecting network infrastructure. Cloud-based deployment of the 5G network also makes it possible for a tenant to create an isolated ICT environment, formed by specific instances of control and user plane NFs. Such an isolated environment is actually a 5G slice [1].

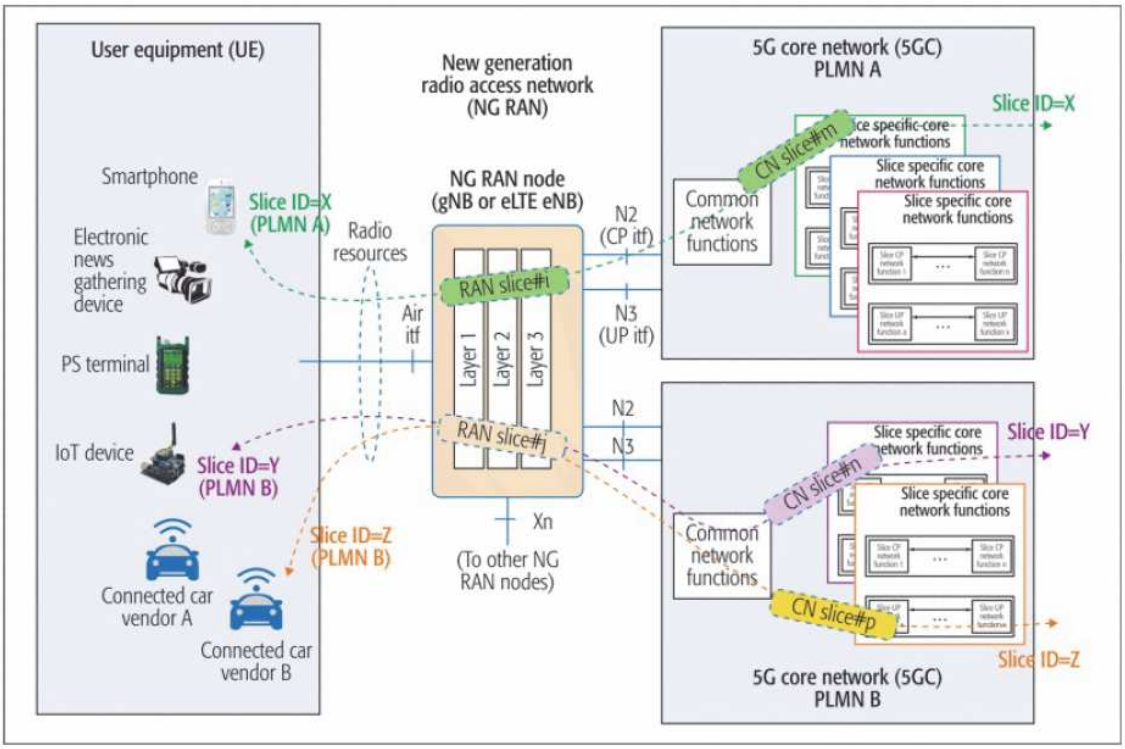

Figure 3.1: 5G Network Slicing Example.

A network slice may span several domains, including radio access networks, core network running on distributed cloud infrastructure, and transport networks supporting flexible virtual function placement.

Note that different network slices may co-exist in the same physical network, thanks to Network Function Virtualization (NFV) paradigm, which is exactly what explained above, i.e., the replacement of network appliance hardware with virtual machines. In the same way, a user equipment can have multiple services operating on different network slices at the same time, e.g., a car link can be used for autonomous driving and on-board entertainment.

By exploiting the network slicing technology, it is therefore possible to consider the development of a logic network, for MC communications, which is independent, adaptable to the type of service and the state of the network, and with guaranteed resources.

In [18], developed by the *Services and system aspects* group of 3GPP, are described the technical performance metrics used for standardizing the 5G cellular communication systems. However the operational requirements presented by the standard focus mainly on the industrial automation applications, while are missing communication requirements specific to MC-related services and use cases.

In the following section, the metrics specified by [18] for automation and control services, e.g., discrete automation motion control, electricity distribution, and remote control, are used to characterize different MC services, as already done by [19] to describe new healthcare services.

3.2 MC Services Performance Requirements

To work properly, MC Services need high levels of service availability and reliability to carry out fast and effective communications, requiring mechanisms to guarantee, to their users, high levels of priority, inter-user prioritization and preemption.

To this end, it is first of all necessary to define the requirements that these services demand and that the network slice must therefore satisfy.

The metrics considered to determine the MC performance parameters are:

- **End-to-end Latency**: the time that takes to transfer a given piece of information from a source to a destination, measured at the communication interface, from the moment it is transmitted by the source to the moment it is successfully received at the destination;
- **Jitter**: measure of latency uncertainty, due to errors and non-idealities in communications;
- **Survival Time**: maximum packet delay still tolerated by the application to operate properly;
- **Communication Service Availability**: percentage of the time in which the communication service is up. The service is considered in down state when a packet is not received within a given time constraint (larger than the sum of end-to-end latency, jitter, and survival time);
- **Reliability**: percentage value of the amount of sent network layer packets successfully delivered to a given system entity within the time constraint required by the targeted service, divided by the total number of sent network layer packets;
- **User Experienced Data Rate**: minimum acceptable data rate to satisfy the user experience of a specific service;
- **Payload Size**: average size of the data packet;
- **Traffic Density**: communication data rate per unit area, based on the assumption that all applications within the area require a given user experienced data rate;

- **Connection Density**: number of connected devices per unit area, under the assumption of full penetration of 5G networks;
- **Service Area Dimension**: volume of the geographic area where the service is available;
- **Position Accuracy**: maximum uncertainty of user position.

To give true values to the metrics above presented, three different scenarios have been identified among a large variety of potential MC services: train automation and control, intervention of the police in a city, and a forest fire.

This choice is intended to consider the cases that are most often cited when talking about MC services and that represent a challenge for their communications requirements. Such as the need for emergency communications on high-speed transportation, the organization of operations through critical communications in urban areas, where coverage is greater, but the number of users connected to the network is also greater, and in rural areas where the traffic density is very low and also the network coverage is less efficient.

Smart railways

Rail is one of the most sustainable, innovative, and safest transportation modes available today. High-speed train travel is only possible using effective train control. A train driver without train control loses situational awareness and cannot react fast enough at speeds above 180 km/h.

In Europe, the standard railway control-command and traffic management system is the European Train Control System (ETCS). This system is currently enabled by the Global System for Mobile Communications – Railway (GSM-R), the standardization of which has been driven mainly by the International Union of Railways (UIC) [20].

To ensure that the requirements arising from railways are addressed by the evolving 5G systems, the UIC has formed an FRMCS (Future Railway Mobile Communication System) functional working group. This working group has defined various applications that should be guaranteed by the FRMCS, grouping them into three main categories, that is, (1) applications that are essential to train movements and safety or legal obligations, (2) applications that improve the performance of railway operations, and (3) applications that support railway business operations in general.

The first category includes all those operations that require critical communications, such as: trackside maintenance, public emergency call, platform alerts, on-train safety communication, railway emergency, remote control, maintenance warnings, ground-to-ground voice call, automatic train control/operation, monitoring and control, and train integrity.

It is evident that these different FRMCS applications listed above demand exchange of voice, video, and/or data requiring low latency and high reliability communication. 3GPP has specified the performance requirements for these applications in [21].

Trains are operated at speeds up to 500 km/h. Under these conditions voice, video, and data communication are to be provided.

In addition, the relative braking distance of a rail vehicle is an important indicator of the safety, which is significantly influenced by the transmission reliability between train and controller at low speeds up to 40 km/h. This mainly applies to the entry and exit of trains in the station area or displacement manoeuvres within marshalling yards.

To support various voice, video, and data categories,the following rail communication scenarios shall be considered:

- Standard Data Communication for operational purposes;
- Voice Communication for operational purposes;
- Critical Data Communication for operational purposes;
- Critical Video Communication for operational purposes;
- Very Critical Data Communication;
- Very Critical Video Communication;

Table 3.1 summarizes the communication requirements, taken from [18], [21], [22], and [23], for each rail communication scenario listed above. Each kind of critical communication present in the table is represented by a number enclosed in parenthesis. These numbers are then reported in Figure 3.2 to show where and how such critical transmissions may occur in the railways scenario.

Emergency in an urban environment

In this scenario, a shooting in a central bank of a medium sized city is considered. The public safety resources of the city involve several police squads and medical personnel.

In such a situation, MC communications must be guaranteed to coordinate the different teams and to monitor the health conditions of each involved person.

In particular, voice calls may be established between elements of the same squad and between squad-leaders and the emergency coordination center. In addition, video calls may be carried out to show what first responders see on site, in case of irruption in the bank, or in case of need for medical assistance.

The urban environment represents a further obstacle to the success of critical communications. The presence of civilians in the surrounding area that want to share multimedia data or start calls to inform about what they see, will load the network. Therefore, to work correctly the MC services require guaranteed resources and service availability.

Table 3.1: Performance requirements for smart railways.

Scenario	Type	End-to-end latency (ms)	Jitter (ms)	Survival Time (ms)	Communication service availability	Reliability	User experienced data rate	Payload size[1]	Traffic density	Connection density (devices/train)	Service area dimension	Position accuracy (m)
Smart Railways	Standard Data communications (1)	< 500	20	100	99.9%	99.9%	1 Mbps up to 10 Mbps	Small to large	Up to 100 Mbps/km	1000	100 km along rail tracks	< 10
	Voice communications (2)	< 100	10	100	99.9%	99.9%	100 Kbps up to 300 Kbps	Small	Up to 1 Mbps/line km	Medium	200 km along rail tracks	< 10
	Critical Data communications (3)	< 500	20	100	99.9999%	99.9999%	10 Kbps up to 500 Kbps	Small to medium	Up to 10 Mbps/km	1000	100 km along rail tracks	< 10
	Critical Video communications (4)	< 100	10	100	99.9%	99.9%	10 Mbps	Medium	Up to 1 Gbps/km	Low	200 km along rail tracks	< 10
	Very Critical Data communications (5)	< 10	2	25	99.9999%	99.9999%	100 Kbps up to 1 Mbps	Small to Medium	Up to 100 Mbps/km	1000	200 km along rail tacks/2 km along rail tracks urban or station	< 1
	Very Critical Video communications (6)	< 10	2	100	99.9%	99.9999%	10 Mbps up to 30 Mbps	Medium	Up to 1 Gbps/km	Low	200 km along rail tacks/2 km along rail tracks urban or station	< 1

[1] Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.

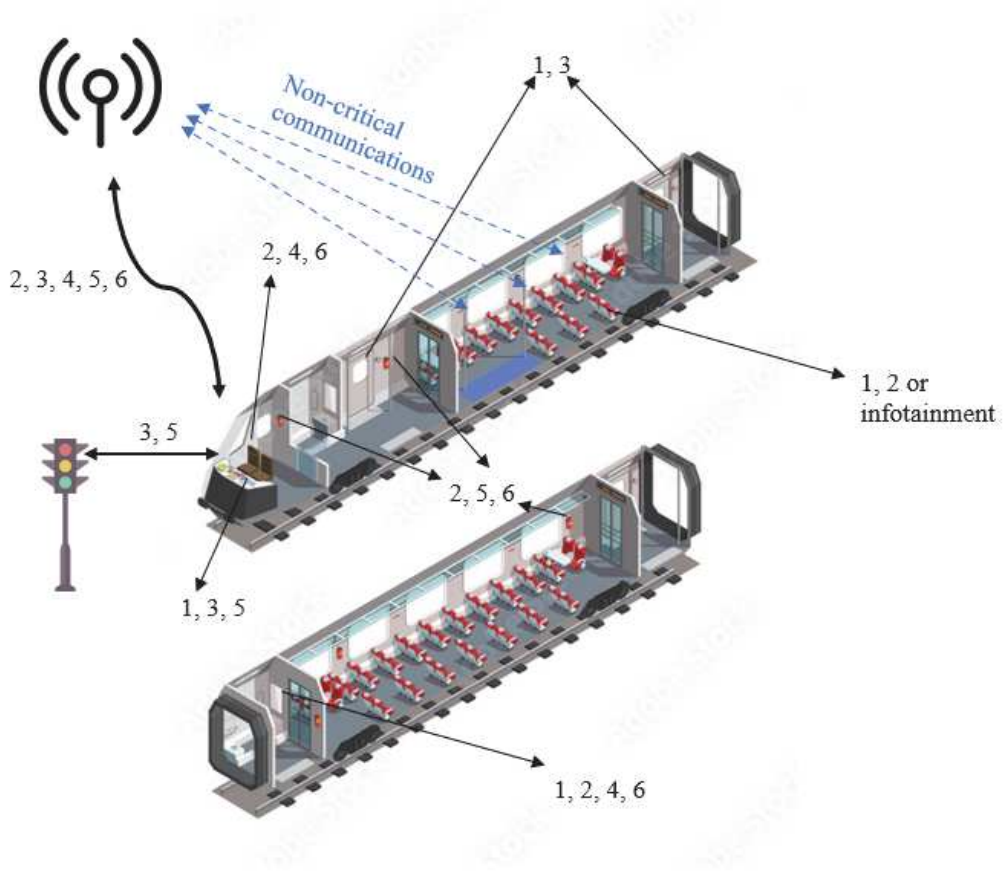

Figure 3.2: Smart railways scenario. Critical communications example..

Another fundamental point, in these situations, is to obtain the accurate position, both indoors and outdoors, of each operator present in the emergency area. In this way, in case of injuries or accidents, it is possible to quickly identify the injured person and intervene effectively.

Table 3.2 shows the performance requirements needed to carry out MC communications for this kind of scenario. The values are obtained from [22], [23], [24], and [25].

Like Smart railways case, Figure 3.3 presents a simple example of urban environment and the critical communications, listed in Table 3.2, that may occur.

Emergency in a rural environment

In the considered scenario are present different teams of firefighters that operates in a for-

Table 3.2: Performance requirements for MC communications in urban environments.

Scenario	Type	End-to-end latency (ms)	Jitter (ms)	Survival Time (ms)	Communication service availability	Reliability	User experienced data rate	Payload size[1]	Traffic density (Gbps/km^2)	Connection density (devices/km^2)	Service area dimension	Position accuracy (m)
Emergency occurrance in urban environment	MC Data communications (1)	200	20	100	99.999%	99.99999%	100 Kbps up to 1 Mbps	Small to large	1	10 000	10^3 x 10^3 x 50	< 10 outdoor
	MC Voice communications (2)	60				99.99%	100 Kbps up to 400 Kbps	Small				<1 horizontal and < 2 vertical indoor
	MC Video communications (3)	100				99.999%	10 Mbps up to 30 Mbps	Medium				

[1] Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.

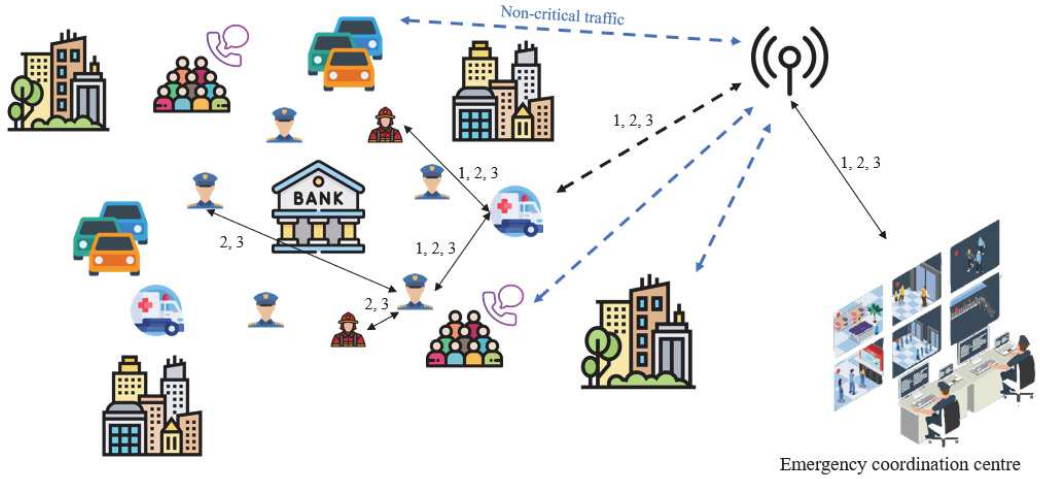

Figure 3.3: Emergency in Urban scenario. Critical communications example..

est to extinguish a fire. Compared to the previous scenario, the main problem, in the case of emergency in such a rural area, is the lack of network coverage.

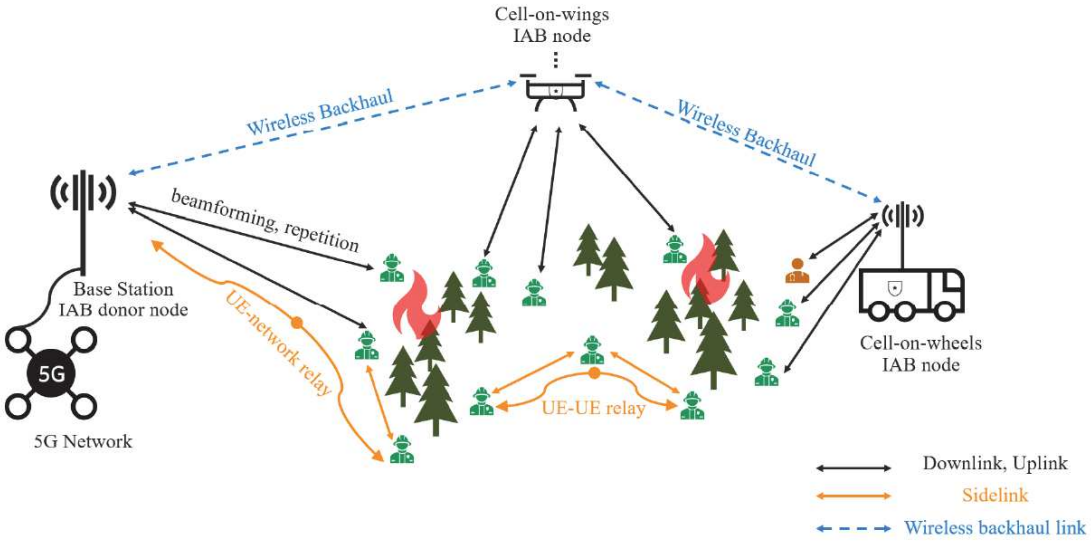

Figure 3.4: 5G NR coverage solutions to provide limitless connectivity for public safety MC communications.

In this regard, 5G New Radio (NR) offers rich features for network coverage extension, which can be applied for providing good coverage for MC communications. As shown in Figure 3.4, examples of NR coverage solutions include using beamforming to increase the signal

strength for intended UEs in a specific area, and using integrated access backhaul (IAB), with drones carrying Base Stations (BSs) [26], for multi-hop networks relaying or for enabling deployable networks. In addition, NR supports sidelink (SL) including SL relaying to provide coverage in areas where network infrastructure is not available or damaged [27].

Also in this situation, first responders typically work in groups and require group communications to efficiently coordinate their operations, and real-time accurate positioning of first responders is essential for improving their safety and situational awareness.

Firefighters can perform voice calls to coordinate their operations and video calls to show the status of the fire. The area of intervention can be quite large and distant from the operative center, in this way availability of service and latencies are among the most important challenges from a communication perspective.

Table 3.3 summarizes the performance requirements to guarantee MC communications in this rural environment [18] [22] [23] [25].
It is worth to note that availability and reliability values are equal to those of the urban scenario. Indeed, to work properly, MC communications require high availability and reliability regardless of the scenario considered.

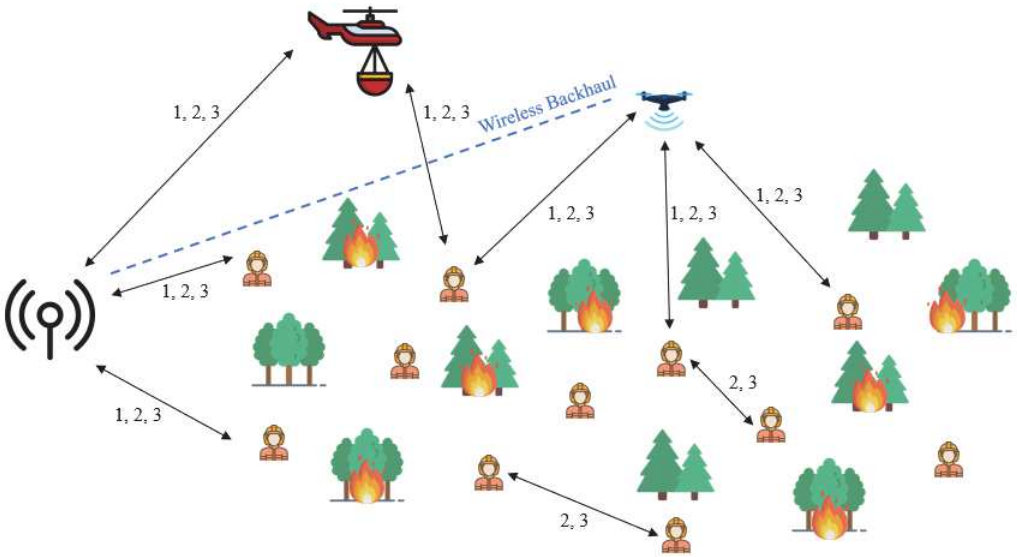

Figure 3.5: Emergency in Rural scenario. Critical communications example.

Figure 3.5 shows an example of the Rural scenario considered. The numbers refer to the critical communications listed in Table 3.3.

Table 3.3: Performance requirements for MC communications in rural environment.

Scenario	Type	End-to-end latency (ms)	Jitter (ms)	Survival Time (ms)	Communication service availability	Reliability	User experienced data rate	Payload size[1]	Traffic density (Mbps/km^2)	Connection density (devices/km^2)	Service area dimension	Position accuracy (m)
Emergency occurance in rural environment	MC Data communications (1)	230	20	100	99.999%	99.99999%	100 Kbps up to 1 Mbps	Small to large	100	100	10^4 x 10^4 x 10	< 10 outdoor
	MC Voice communications (2)	100				99.99%	100 Kbps up to 400 Kbps	Small				
	MC Video communications (3)	150				99.999%	10 Mbps up to 30 Mbps	Medium				

[1] Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.

3.3 Network Slicing and MC communications

The International Communication Union (ITU) defined three general target categories for 5G cellular networks:

- **Enhanced mobile broadband (eMBB)** for high capacity and high speed, with peak data rates of greater than 10 gigabits per second (Gbps), compared to 100 megabits per second (Mbps) to 1 Gbps typically available with LTE. Suitable for services like streaming of high quality videos, fast large file transfers, etc.;
- **Ultra-reliable and low latency communications (URLLC)** targeting high reliability and low latency, around 0.25 ms versus 10ms with LTE. For applications including industrial automation, remote control systems, etc.;
- **Massive machine type communications (mMTC)** for an extremely large number of potential internet of things (IoT) devices (massive IoT). The devices would have connection density of about one million devices per km^2.

Considering the MC Services use case, stringent requirements are mainly related to latency, user experienced data rate, high numbers of users connected, availability, and reliability. The scenarios described above fall at the intersection between the three 5G target slices. For example, a video streaming communication to assess the surrounding situation of a safety operator requires low latencies (URLLC) and an understandable transmission, thus with a sufficient bit rate (eMBB). Therefore, the need to define a Network Slice suitable for MC Services becomes clear.

The parameters listed and described in the previous Section give an indication of how the new Network Slicing technology, brought by 5G, can be a great opportunity to be exploited for MC services. MC service providers can, indeed, negotiate with network operators for an appropriate Network Slice to be developed and made available in case of need.

The MC network thus created, possibly exploiting cloud computing, is expected to connect all the MC services. It includes control entities for specific critical services (e.g., emergency management and monitoring operations) and communication entities for network supervision, security, and management. Connection among devices is provided by the 5G cellular network through data gateways and new-generation node-bases (gNBs).

Creating, managing and closing a Network Slice may require a considerable effort both in terms of resources, time and complexity. However, it would guarantee higher efficiency in the use of the network and would guarantee a more certain availability of the service for all involved users.

Network Slicing is certainly a brilliant innovation that in the future more and more companies, organizations, and users will exploit and develop. In particular, for MC communications, an interesting implication would be the possibility not only of creating previously a Network Slice, but also of being able to dynamically modify it once deployed in the field, being able to alter its parameters according to the emergency situation.

4

N5-Interface Based MC Networks

Users who use MC services require effective emergency communications and therefore strict compliance with certain KPIs. In this thesis two ways have been considered to satisfy these performance requirements: the Network Slicing technology, which was discussed in the previous chapter, and the use of the N5 interface, which allows you to communicate directly with the Core of the 5G network.

Network Slicing technology allows the creation of multiple logical networks over the same physical network by effectively distributing the available resources. Realizing a Network Slice can be very complicated and expensive and requires several tools and techniques, including: SDN (Software Defined Networking) to enable dynamic, programmatically efficient network configuration in order to improve network performance and monitoring; NFV (Network Function Virtualization) to virtualize network node functions into building blocks that may connect, or chain together, to create and deliver communication services; a scheduler/orchestrator that dinamically coordinates all the different network components that are involved in the lifecycle of each network slice based on previously defined algorithms; clearly define the total resources available and how to distribute them according to the services to be provided; sign agreements with network owners (like MNOs, Mobile Network Operators), and many others.

The second solution takes into account the N5 interface. This connection links the PCF, in particular the *Npcf_PolicyAuthorization* service, with the Application Function, in this case a Mission Critical server external to the 5G core network, which requires the establishment of some specific policy control rules.

When the user accesses the 5G network and has an active PDU session, he is associated with a specific network slicing which can be a default or specific to the service for which he accesses the network, based on the configuration of the network in question. Certain performance parameters are therefore associated with his PDU session, such as max throughput, latency, priority,

qci, etc., based on the rules defined for that particular network slice. Each NF of the 5GC stores, for each PDU session, the information relating to its function and makes it available to the other NFs through specific services and interfaces.

In particular, the policy rules that define the QoS performance for each PDU session are stored and managed in the PCF. This information is accessible and editable through the *Npcf_PolicyAuthorization* service via the N5 interface.

By sending specific HTTP messages it is possible to perform various operations: receive notifications about events that impact the PDU sessions involved, install new policy rules, modify existing policy rules or even delete certain rules. In this way it is possible to intervene directly within the network to establish or change particular policy rules of a PDU session according to the service needs. In the case of MC services, the goal is to give greater importance to MC communications than the others, increasing the bit rate in the downlink or uplink, authorizing traffic only to certain IPs, requesting a higher priority level, etc.

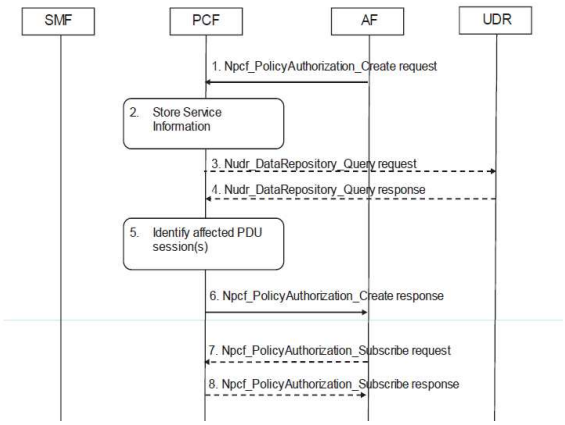

Figure 4.1: AF triggers PCF-initiated Policy Association Modification procedure.

Depending on the rules set, the PCF will communicate the changes made to the other NFs, and each of them, consequently, will take care of updating their stored data, guaranteeing the required performances and, in turn, communicating these changes to the NFs concerned. In this way the entire 5G network is reorganized so that the required QoS is satisfied, thus also redistributing the resources within the Network Slice previously associated with that PDU session.

In Figure 4.1, followed by Figure 4.2, are shown all the necessary steps, within the 5GC, to apply the policy rules transmitted in the body of an HTTP request received and authorized by the PCF through the N5 interface.

In this case the *Npcf_PolicyAuthorization_Create* service is invoked to create an application session context in the PCF to install some policy rules for a specific PDU session, more details

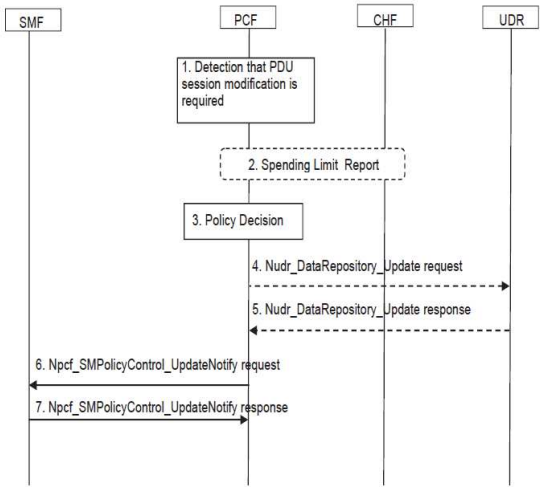

Figure 4.2: Interactions between SMF, PCF and CHF for PCF-initiated Policy Association Modification procedure.

about this operation will be provided in 5.3. Just note that a single HTTP requests triggers the PCF to contact others NFs in order to apply the policy rules demanded.

Using a Network Slice, the network adapts and redistributes the resources dynamically based on the number and type of active sessions. With the Network Slicing technology it is possible to perform QoS management across all domains of the 5G network: from physical access to the network, where it is possible to develop a RAN slice scheduling framework [28], to control specific configurations of the transport network and custom software elements in the core network. Therefore, according to certain algorithms, the NS operates in an optimal way without the need to authorize requests from outside.

Through the N5 interface, on the other hand, the network reorganizes and manages resources based on commands sent by an authorized AF, in this case an MC server within the IP Multimedia Core Network Subsystem (IMS).It will take care to request certain levels of QoS every time an MC communication is initiated, whether it is an audio or video call or emergency call, sending specific requests using the aforementioned interface.

This Chapter describes the solution based on the N5 interface.

4.1 The Npcf_PolicyAuthorization Service

The *Npcf_PolicyAuthorization* service authorises an AF request and creates policies for the PDU session to which the AF is bound to. This service allows also the NF service consumer to subscribe/unsubscribe to the notification of events (e.g. access type change, usage report,

access network information report, etc.).

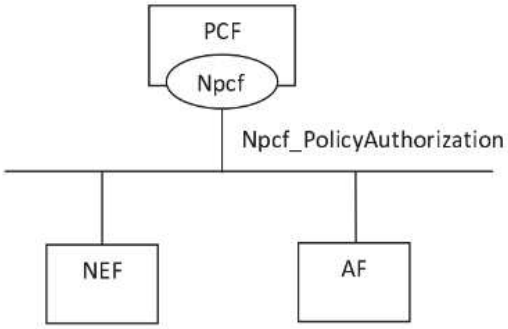

Figure 4.3: Npcf_PolicyAuthorization service Architecture, SBI representation.

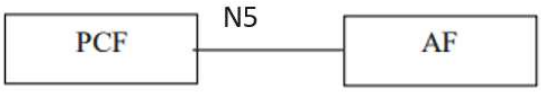

Figure 4.4: Npcf_PolicyAuthorization service Architecture, reference point representation.

The AF is not the only NF service consumer of the *Npcf_PolicyAuthorization* service. Also the NEF (Network Exposure Function) can request policy enforcement through it, as shown in Figure 4.3. In this thesis, only the connection between AF and PCF is studied and developed, as shown in Figure 4.4, because it implies one less step and therefore is more efficient.

The Policy and Charging control related 5G architecture is described in 3GPP TS 23.503 [16] and 3GPP TS 29.513 [29]. While 3GPP TS 29.514 [30] provides the stage 3 definition of the Policy Authorization Service of the 5G System.

The communication between the service and the AF is carried out through the HTTP/2 protocol. HTTP/2 leaves all of HTTP/1.1's high-level semantics, such as methods, status codes, header fields, and URIs, the same. What is new is the way in which the data is framed and transported between the client and the server [31]. In this way, the HTTP requests and responses can be built without new structural changes compared to those already used in previous versions.

The *Npcf_PolicyAuthorization* service provides different operations and each of these can be invoked by the AF through the proper HTTP request, as defined in [30]. At each HTTP

Table 4.1: Npcf_PolicyAuthorization service operations.

Service Operation Name	Description	Initiated by
Npcf_PolicyAuthorization_Create	Determines and installs the policy according to the service information provided by an authorized NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Update	Determines and updates the policy according to the modified service information provided by an authorized NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Delete	Provides means to delete the application session context of the NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Notify	Notifies NF service consumer of the subscribed events.	PCF
Npcf_PolicyAuthorization_Subscribe	Allows NF service consumers to subscribe to the notification of events.	AF, NEF
Npcf_PolicyAuthorization_Unsubscribe	Allows NF service consumers to unsubscribe to the notification of events.	AF, NEF

request the PCF will send an HTTP response signalling if the request has been accepted or rejected or misunderstood.

The service operations, defined for the *Npcf_PolicyAuthorization* service, are shown in Table 4.1.

The following paragraphs illustrate the tools used to develop the N5 interface through which these service operations, provided by the *Npcf_PolicyAuthorization* service, have been invoked and tested.

4.2 List of the used tools

To develop and test the N5 interface, different components are needed. The idea is to simulate a UE that accesses the 5GC network through the 5G New Radio, trying to establish and carry out an MC communication. Once the PDU session is active, some HTTP requests to modify the QoS parameters for that session are sent to the *Npcf_PolicyAuthorization* service.

For this purpose, the following elements are necessary: a 5GC that includes the *Npcf_PolicyAuthorization* service, a UE and RAN (Radio Access Network) simulator, a MC service to carry out critical communications and the HTTP/2 messages.

Open5GS

Open5GS is a C-language Open Source implementation of 5GC and EPC, i.e., the core network of New Radio (NR) and LTE network. Open5GS Open Source files are made available under the terms of the GNU Affero General Public License and are accessible on GitHub[1].

The 5GC was initially an implementation of an EPC (4G) core network. At the end of 2019 the project was updated to support the 5G architecture. Today Open5GS includes both

[1] https://github.com/open5gs/open5gs

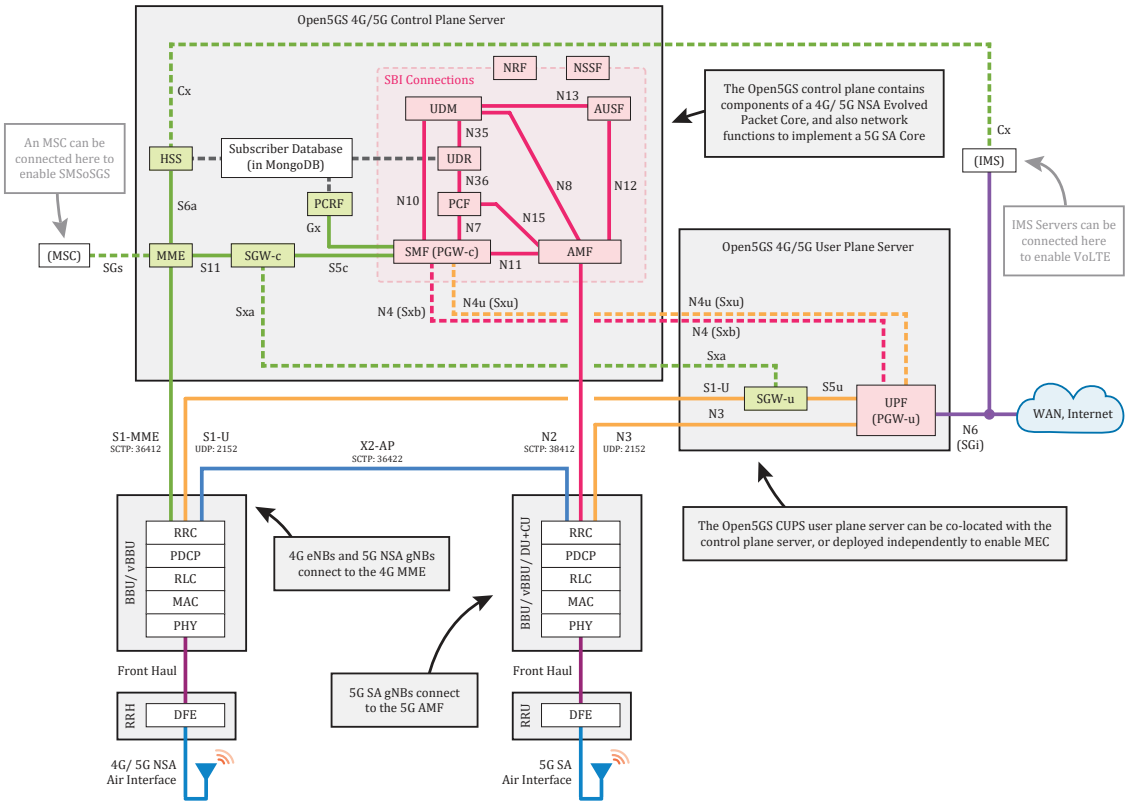

Figure 4.5: Open5GS architecture.

5GC and EPC implementations allowing for 5G non-standalone (NSA) and standalone (SA) deployments. The complete architecture of the network is shown in Figure 4.5 where the 5G SA network is colored in pink while the 4G components are colored in green.

Each component is a different network element or virtual network function and it is coded in a separate script so it can be run individually. This separation allows for the network deployment to be fully customizable using only the required VNFs.

For the purpose of this thesis only the 5G SA Core deployment has been used and it contains the following functions:

- AMF - Access and Mobility Management Function
- SMF - User Plane Function
- UPF - User Plane Function
- AUSF - Authentication Server Function
- NRF - NF Repository Function

- UDM - Unified Data Management
- UDR - Unififed Data Repository
- PCF - Policy and Charging Function
- NSSF - Network Slice Selection Function
- BSF - Binding Support Function

The core has two main planes: the control plane and the user plane. These are physically separated in Open5GS as CUPS (control/ user plane separation) is implemented.

Control plane functions are configured to register with the NRF, and the NRF then helps them discover the other core functions.

The 5G SA core user plane is much simpler, as it only contains a single function. The UPF carries user data packets between the gNB and the external WAN. It connects back to the SMF too.

With the exception of the SMF and UPF, all configuration files for the 5G SA core functions only contain the function's IP bind addresses/ local Interface names and the IP address/ DNS name of the NRF.

By default the different VNFs communicate with each other using the 127.0.0.x local loopback address space, but they can be customized in the configuration files.

The Open5GS project is very interesting and advantageous because it is compliant with the Release-16 of the 3GPP standard and it is compatible with many different Linux distributions, such as Alpine, Ubuntu, Fedora, CentOS, FreeBSD, and MacOSX.

UERANSIM

UERANSIM, is the open-source state-of-the-art 5G UE and RAN (gNodeB) implementation. It can be considered as a 5G mobile phone and a new generation base station in basic terms. The project can be used for testing 5G Core Network and studying 5G System.

All source code and related files including documentation and wiki pages are dual licensed with the GNU General Public License and a commercial license and are available on GitHub[2].

UERANSIM can be installed only on Linux systems and is completely developed using the C++ programming language. Once the repository is cloned and built, five files are made available to start using the UE and gNodeB (gNB):

- **nr-gnb**, the main executable for the 5G gNB (RAN)

[2]https://github.com/aligungr/UERANSIM

- **nr-ue**, the main executable for the 5G UE
- **nr-cli**, CLI (Command Line Interface) tool for 5G gNB and UE
- **nr-binder**, a tool for utilizing UE's internet connectivity
- **libdevbnd.so**, a dynamic library for nr-binder

nr-ue and **nr-gnb** accepts configuration files as parameters. With the first is possible to set the identity of the UE (supi, mcc, mnc, ecc.), the number of PDU sessions for that UE, the network slice for a specific PDU session, ecc.

The gNB configuration file instead offers the possibility to modify the mcc/mnc fields, the IPs for the interfaces with the AMF, UPF, and UE, the supported list of slices by the gNB, ecc.

There are three main interfaces in UE/RAN perspective:

- Control Interface (between RAN and AMF in the 5GC)
- User Interface (between RAN and UPF in the 5GC)
- Radio Interface (between RAN and UE)

The Control Plane has two interfaces in turn:

- NAS (Non-Access Stratum) is in control of the UE and implements several features like primary authentication and key agreement, security mode control, identification, initial and periodic registration, UE and Network initiated de-registration, UE initiated PDU session establishment, UE and Network initiated PDU session release, and paging.
- NGAP (NG Application Protocol) is in control of the RAN and supports PDU session resource setup, PDU session resource release, initial context setup, UE context release (NG-RAN node initiated and AMF initiated), UE context modification, initial UE message, paging, NG setup, and error indication.

From the User Plane perspective, the RAN implements GTP protocol for user plane and currently only IPv4 is supported.

UERANSIM Radio Interface does not implement 5G radio protocols below the RRC layer and 5G radio is partially simulated over UDP protocol over port-4997. So, PHY, MAC, RLC, and PDCP are not implemented in UERANSIM.

Like Open5GS, the UERANSIM project is compliant with many of the 3GPP fundamental control plane features and some of them are in progress. This allows us to have a complete simulated scenario, i.e. UE, gNB, and 5GC in accordance with the 3GPP guidelines.

MCXPTT

MCXPTT is a product developed by Alea S.r.l.[3]. Alea's interest in emergency communications began in 2012 with the development of the XPTT system, an enhanced PTT (Push-to-Talk) for smartphones (iOS and Android) with a web control platform for business users. With the development of MC communications by the 3GPP organization (Rel-13 in 2016), Alea S.r.l. began to get interested in MC services and developed MCXPTT, a technology for the transmission of data and PTT in emergency situations compliant to the Mission Critical standard of 3GPP.

MCXPTT is a system that ensures the immediacy of communication services and allows the user to decide, disclose, and carry out the most appropriate operational actions.

In a critical situation, MCXPTT is a system that provides maximum information, thus allowing you to arrive at the right decision in the shortest possible time.

MCXPTT, used in critical situations:

- guarantees private, group and broadcast calls;
- emphasizes emergency communications with respect to other ongoing communications;
- allows the creation of video streaming;
- ensures the exchange of text messages, photos, files, even of large dimensions;
- locates users and displays the entire scenario on a map;
- provides useful information: user status, GPS accuracy, battery level and charge, aggregated data with alarm events, etc;
- guarantees user authentication with a login and keys exchange for security.

MCXPTT involves the use of an Android Client application, Figure 4.6, and an Operational Center, Figure 4.7, both conceived and optimized according to a design that guarantees ease of use and system efficiency.

The administration web portal allows you to configure each single parameter of the system in a simple way in order to satisfy any operational requirement; a dedicated section of the web portal allows access to information, data, records with search functions and KPIs.

MCXPTT supports all three 3GPP standardized MC services: MC PTT, MC Video and MC Data.

[3] https://www.aleasrl.com/

Figure 4.6: MCXPTT smartphone app.

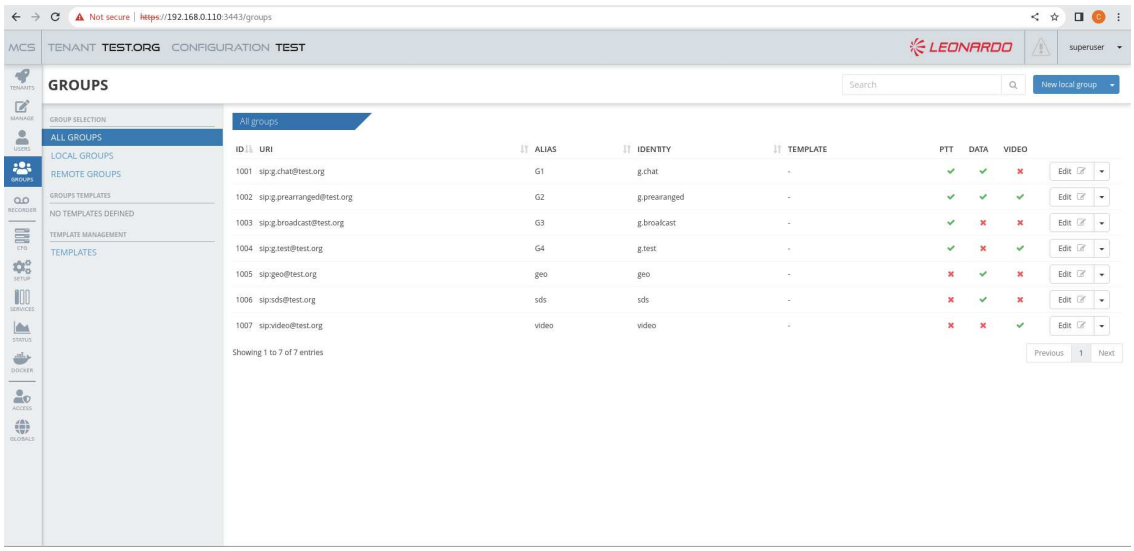

Figure 4.7: MCXPTT Operational Center.

In particular in this thesis, to verify the functionality of MC communications through the 5G network, an MCXPTT client and an MCXPTT server (operational center) were installed on two different virtual machines and different types of tests, that the developers of Alea S.r.l. normally carry out to verify the functionality of their application, were performed.

Through these tests several steps of an MC communication can be verified: from the simple but fundamental establishment of an MC call (test 100), to an effective exchange of small audio packets (test 103, Figure 4.8) or even the transfer of more complex audio files while simulating

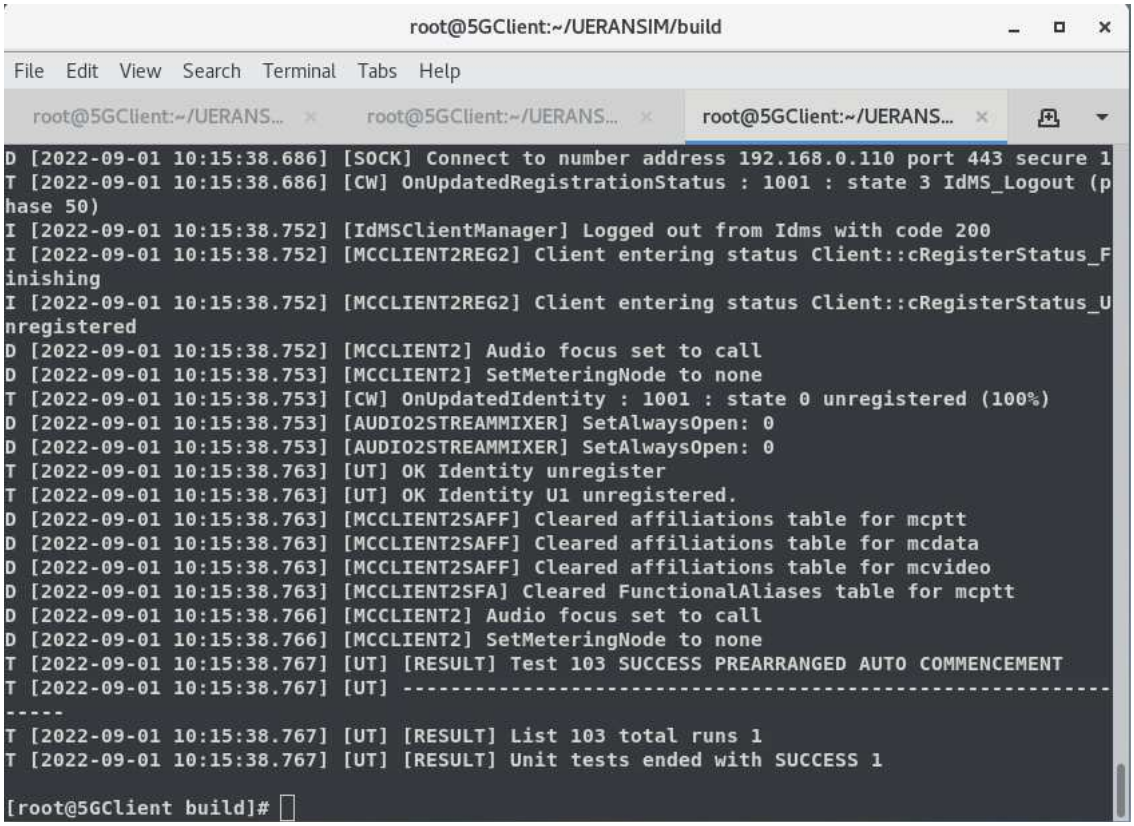

Figure 4.8: Terminal view of Test 103 completed successfully.

a large number of active users (test 480).

libcurl

The HTTP/2 requests necessary to establish, modify or remove the policy rules were created using the library *libcurl*. Libcurl is a free and easy-to-use client-side URL transfer library, supporting a high number of protocols including HTTP/2. It is the library on which the most well-known command-line tool, *curl*, is built. Curl is an open source software, available on GitHub[4], used in command lines or scripts to transfer data.

To simulate the behavior of the MC server inside the network, the HTTP requests were made in the form of scripts using the C++ programming language.

Libcurl provides several APIs for the C language. In this case, the synchronous Easy interface is the basis for the HTTP requests. The *curl_easy_init* function must be used when using libcurl's "easy" interface to init a session and get a handle (often referred to as an "easy handle"),

[4]https://github.com/curl/curl

which is used as input to the easy interface functions.

Then it is necessary to set all the options wanted in the upcoming transfer, like the URL, the protocol (HTTP/2), etc. To do this the *curl_easy_setopt* function shall be adopted. The *curl_easy_setopt* man page[5] has a full index of the almost 300 available options.

CURLOPT_URL is the only option really mandatory, as otherwise there can be no transfer. Another commonly used option is *CURLOPT_VERBOSE* that will help see what libcurl is doing, which is useful when debugging.

When all is setup, *curl_easy_perform* is used to tell libcurl to perform the transfer. It will then do the entire operation and will not return until it is done (successfully or not).

After the transfer has been made, it is possible to set new options and make another transfer, or, if no more operations are needed, to cleanup the session by calling *curl_easy_cleanup*.

In the next paragraph are shown the configurations and the outputs of the HTTP requests' scripts.

4.3 Architecture and configuration procedure

The testbed infrastructure comprises four physical machines: a Desktop PC, two notebooks and a router. More information about the resources of the nodes are listed in Table 4.2.

Table 4.2: Physical resources of the adopted hosts.

	Dell Desktop PC	Acer Notebook	HP Notebook
CPU	Intel Core i3-10100T	Intel Core i7-2630M	AMD Ryzen 5 5600H
Memory	8 GB	8 GB	8 GB
Storage	256 GB	1 TB	470 GB

The Dell Desktop PC, provided by the Alea company, hosts the Open5GS 5GC Control plane network and two CentOS 7 Virtual Machines (VMs) for the MCXPTT product, one for the MCXPTT client application and the UERANSIM simulator and one for the MCXPTT server. In the ACER notebook is installed the Open5GS 5GC User plane network.

In this way Control plane and User plane are separated according to the CUPS (Control Plane User Plane Separation) paradigm. The objective is to completely decouple the user or data plane functions from the control plane functions, in order to allow them to scale independently accordingly to the different data traffic and control traffic. Moreover, it is possible to reduce latency by selecting user plane nodes which are closer to the RAN or more appropriate for the intended utilization of the UE.

[5] https://curl.se/libcurl/c/curl_easy_setopt.html

The HP notebook acts as MC server and it is the node that sends the HTTP requests to the PCF in the 5GC.

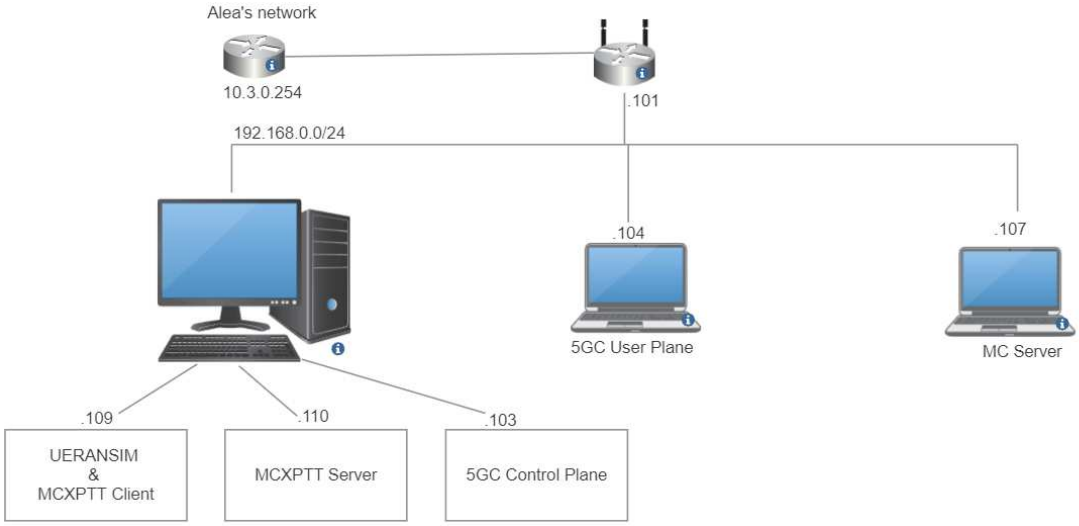

Figure 4.9: Network Architecture.

All hosts and VMs are connected to a common sub-network that has Internet connectivity through the Alea's private network. The machines' addresses are in the range 192.168.0.0/24, so that they can freely communicate with each other. Since all the NFs inside the 5GC has local address, i.e., 127.0.0.0/8, it is needed to modify the configuration files of those NFs that must be reachable from the outside, like AMF, SMF, PCF, and UPF. In this way AMF, SMF and PCF can be reached at 192.168.0.103 while the UPF has address 192.168.0.104.

Also the gNB and the UE must be appropriately configured.

The Mobile Country Code (MCC) and Mobile Network Code (MNC) are setted to 001 and 01 respectively, that are the numbers identifying a test wireless mobile network. Then the gNB has to know the addresses of the AMF and the UPF for the control data flow and the user data flow, and its own address, i.e., 192.168.0.109, in order to be contacted by UE, AMF and UPF.

The UE configuration files requires the setting of the SUPI, i.e., IMSI (International Mobile Subscriber Identity) for the UE, the MCC/MNC fields, the permanent subscription key assigned for this specific UE and the Operator code value. It needs also to know the gNB address in order to access the network.

Furthermore, the Open5GS 5GC, to authenticate the UE trying to access the network, needs to have stored in its UDR MongoDB database the subscriber profile. To do so Open5GS provides a web interface shown in Figure 4.10. Here it is possible to set the different parameters that must be equal to the ones set in the UE configuration file.

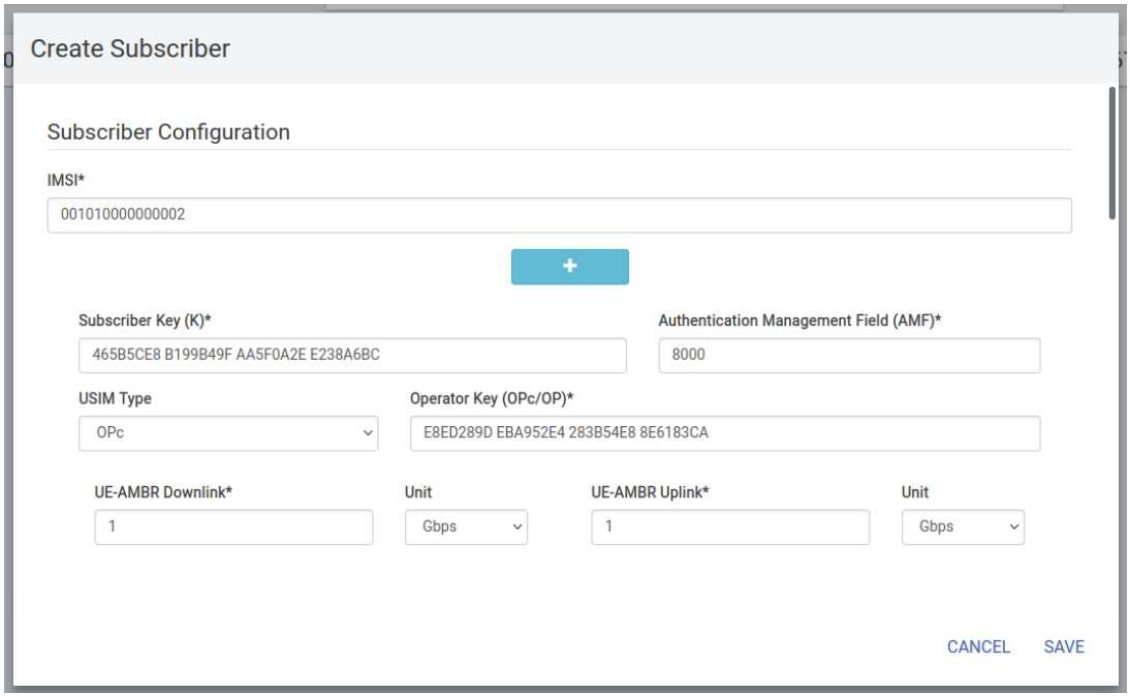

Figure 4.10: Open5GS WebUI interface.

Once the UERANSIM gNB is connected to the AMF and to the UPF, the UE script can be launched using the *nr-ue -c myconfig.yaml* terminal command and a PDU session is created.

In a 5G network, PDU sessions are created to provide end-to-end user plane connectivity between the UEs and a specific data network. In order to test the connection through the User Plane Function, UERANSIM creates a virtual TUN interface for each established PDU session. It is possible to simulate user plane traffic originating by a specific UE by sending packets through the corresponding TUN interface, Figure 4.11.

In conclusion, unlike the Network Slice, which automatically guarantees certain performances from the moment of access to the network until the end of the connection, the QoS management through the N5 interface requires a further step, and takes care to implement certain policy rules only when it is necessary to carry out an MC communication by transmitting the IP address and port number identifying for that session.

However, creating a Network Slice requires a great deal of cost, maintenance of the Network Slice life-cycle and complexity, although it probably offers a more complete and effective solution. From this point of view, the development and use of the N5 interface is more convenient in terms of complexity and resource consumption.

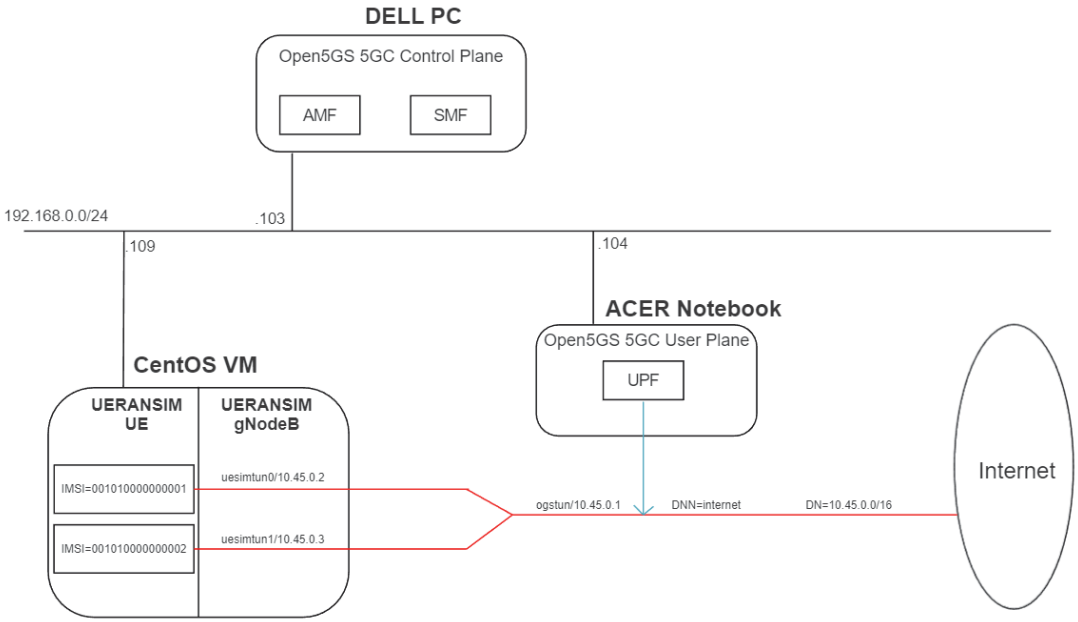

Figure 4.11: Establishment of a PDU session using UERANSIM and Open5GS.

5 Performance Evaluation

Due to the fact that the Open5GS project does not have an integrated monitoring system implemented yet, to check if everything is working properly, the only available tools are the Open5GS NFs log files or the capturing of data traffic through the exploitation of a network protocol analyzer application like Wireshark.

In the following sections, is examined the correct functioning of the whole QoS management operation. Starting from the connection between the simulated New Generation RAN and the 5GC network with the establishment of the PDU session for a UE, to the study of the traffic generated by the MCXPTT application, passing through the 5GC, and the managing of PCC rules, for the established PDU session, using the N5 interface between AF and PCF.

5.1 NG RAN - 5GC connection

Since the 5G network is set up following the CUPS paradigm, first the communication between User plane and Control plane is analyzed by sniffing the traffic on the N4 interface between SMF and UPF.

As shown in Figures 5.1, 5.2 and 5.3, to associate CP and UP, the protocol used over the N4 interface is the Packet Forwarding Control Protocol (PFCP), as specified in [32].

The Control functions manage the packets that are processed and forwarded by the UPF by establishing, modifying and deleting PFCP sessions. The Wireshark traces show the PFCP Association Setup packets between SMF and UPF.

The subsequent Heartbeat packets confirm the correct association and are used by the two NFs to verify if the entity on the other side of the connection is still alive.

```
Open5GS daemon v2.4.9

08/22 15:01:41.809: [app] INFO: Configuration: '/etc/open5gs/smf.yaml' (../lib/app/ogs-init.c:126)
08/22 15:01:41.809: [app] INFO: File Logging: '/var/log/open5gs/smf.log' (../lib/app/ogs-init.c:129)
08/22 15:01:41.863: [gtp] INFO: gtp_server() [127.0.0.4]:2123 (../lib/gtp/path.c:31)
08/22 15:01:41.863: [gtp] INFO: gtp_server() [::1]:2123 (../lib/gtp/path.c:31)
08/22 15:01:41.863: [gtp] INFO: gtp_server() [192.168.0.103]:2152 (../lib/gtp/path.c:31)
08/22 15:01:41.863: [gtp] INFO: gtp_server() [::1]:2152 (../lib/gtp/path.c:31)
08/22 15:01:41.863: [pfcp] INFO: pfcp_server() [192.168.0.103]:8805 (../lib/pfcp/path.c:31)
08/22 15:01:41.863: [pfcp] INFO: pfcp_server() [::1]:8805 (../lib/pfcp/path.c:31)
08/22 15:01:41.863: [pfcp] INFO: ogs_pfcp_connect() [192.168.0.104]:8805 (../lib/pfcp/path.c:62)
08/22 15:01:41.864: [sbi] INFO: nghttp2_server() [127.0.0.4]:7777 (../lib/sbi/nghttp2-server.c:151)
08/22 15:01:41.864: [app] INFO: SMF initialize...done (../src/smf/app.c:31)
08/22 15:01:41.865: [smf] INFO: [91281704-221a-41ed-ace5-6198a7afb8fd] NF registered [Heartbeat:10s] (../src/smf/nf
-sm.c:219)
08/22 15:01:41.865: [diam] INFO: CONNECTED TO 'pcrf.localdomain' (SCTP,soc#15): (../lib/diameter/common/logger.c:10
8)
08/22 15:01:41.866: [smf] INFO: PFCP associated (../src/smf/pfcp-sm.c:174)
```

Figure 5.1: SMF activation and PFCP association with UPF.

```
Open5GS daemon v2.4.8

08/22 14:19:03.392: [app] INFO: Configuration: '/etc/open5gs/upf.yaml' (../lib/app/ogs-init.c:
126)
08/22 14:19:03.392: [app] INFO: File Logging: '/var/log/open5gs/upf.log' (../lib/app/ogs-init.
c:129)
08/22 14:19:03.433: [pfcp] INFO: pfcp_server() [192.168.0.104]:8805 (../lib/pfcp/path.c:30)
08/22 14:19:03.433: [gtp] INFO: gtp_server() [192.168.0.104]:2152 (../lib/gtp/path.c:30)
08/22 14:19:03.442: [app] INFO: UPF initialize...done (../src/upf/app.c:31)
08/22 15:01:33.000: [pfcp] INFO: ogs_pfcp_connect() [192.168.0.103]:8805 (../lib/pfcp/path.c:6
1)
08/22 15:01:33.000: [upf] INFO: PFCP associated (../src/upf/pfcp-sm.c:173)
```

Figure 5.2: UPF activation and PFCP association with SMF.

No.	Time	Source	Destination	Protocol	Length	Info
12619	1014.4925319…	192.168.0.103	192.168.0.104	PFCP	84	PFCP Association Setup Request
12620	1014.4946215…	192.168.0.104	192.168.0.103	PFCP	80	PFCP Association Setup Response
12632	1023.3580903…	192.168.0.103	192.168.0.104	PFCP	84	PFCP Association Setup Request
12633	1023.3598396…	192.168.0.104	192.168.0.103	PFCP	80	PFCP Association Setup Response
12634	1025.4974221…	192.168.0.104	192.168.0.103	PFCP	60	PFCP Heartbeat Request
12635	1025.4978271…	192.168.0.103	192.168.0.104	PFCP	58	PFCP Heartbeat Response
12647	1034.3615204…	192.168.0.103	192.168.0.104	PFCP	58	PFCP Heartbeat Request
12648	1034.3628641…	192.168.0.104	192.168.0.103	PFCP	60	PFCP Heartbeat Response

Figure 5.3: PFCP association over N4 interface.

No.	Time	Source	Destination	Protocol	Length	Info
41	19.532192870	192.168.0.109	192.168.0.103	SCTP	82	INIT
42	19.532275093	192.168.0.103	192.168.0.109	SCTP	306	INIT_ACK
43	19.532432141	192.168.0.109	192.168.0.103	SCTP	278	COOKIE_ECHO
44	19.532466931	192.168.0.103	192.168.0.109	SCTP	50	COOKIE_ACK
45	19.533654440	192.168.0.109	192.168.0.103	NGAP	130	NGSetupRequest
46	19.533687361	192.168.0.103	192.168.0.109	SCTP	62	SACK (Ack=0, Arwnd=102499934)
47	19.533836990	192.168.0.103	192.168.0.109	NGAP	118	NGSetupResponse
48	19.533896900	192.168.0.109	192.168.0.103	SCTP	62	SACK (Ack=0, Arwnd=106442)
79	28.892291375	192.168.0.103	192.168.0.109	SCTP	98	HEARTBEAT
80	28.892745022	192.168.0.109	192.168.0.103	SCTP	98	HEARTBEAT_ACK

Figure 5.4: UERANSIM gNB setup over N2 interface.

Once the 5G network is ready, it is possible to rise up the NG RAN software. Figure 5.4

shows the Stream Control Transmission Protocol (SCTP) packets the UERANSIM gNB and the AMF, in the 5GC, exchange to setup the connection over the N2 interface.

Now it is possible to register the simulated UE to the network. The process starts with the connection between the UE and the NG RAN. Then the gNB communicates with the AMF over the N2 interface in order to register the UE into the network and to establish the PDU session resource.

No.	Time	Source	Destination	Protocol	Length	Info
42	10.964956229	192.168.0.109	192.168.0.103	NGAP/N…	138	InitialUEMessage, Registration request
43	11.021074718	192.168.0.103	192.168.0.109	NGAP/N…	146	SACK (Ack=0, Arwnd=102500000) , DownlinkNASTransport, Authentication request
44	11.021708417	192.168.0.109	192.168.0.103	NGAP/N…	146	SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response
45	11.028993984	192.168.0.103	192.168.0.109	NGAP/N…	126	SACK (Ack=1, Arwnd=102500000) , DownlinkNASTransport, Security mode command
46	11.029519185	192.168.0.109	192.168.0.103	NGAP/N…	186	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport
47	11.046421790	192.168.0.103	192.168.0.109	NGAP/N…	230	SACK (Ack=2, Arwnd=102500000) , InitialContextSetupRequest
48	11.058121822	192.168.0.109	192.168.0.103	NGAP	98	SACK (Ack=2, Arwnd=106496) , InitialContextSetupResponse
49	11.260013701	192.168.0.103	192.168.0.109	SCTP	62	SACK (Ack=3, Arwnd=102500000)
50	11.260610427	192.168.0.109	192.168.0.103	NGAP/N…	238	UplinkNASTransport, UplinkNASTransport
51	11.261300853	192.168.0.103	192.168.0.109	NGAP/N…	142	SACK (Ack=5, Arwnd=102500000) , DownlinkNASTransport
53	11.461675508	192.168.0.109	192.168.0.103	SCTP	62	SACK (Ack=3, Arwnd=106496)
69	16.306101891	192.168.0.103	192.168.0.109	NGAP/N…	242	PDUSessionResourceSetupRequest
70	16.313965084	192.168.0.109	192.168.0.103	NGAP	118	SACK (Ack=4, Arwnd=106496) , PDUSessionResourceSetupResponse
73	16.515931007	192.168.0.103	192.168.0.109	SCTP	62	SACK (Ack=6, Arwnd=102500000)
83	22.016011043	192.168.0.103	192.168.0.109	SCTP	98	HEARTBEAT
84	22.016511320	192.168.0.109	192.168.0.103	SCTP	98	HEARTBEAT_ACK

Figure 5.5: UE registration procedure over N2 interface.

In Figure 5.5 the packets exchanged between the simulated gNB and the AMF are shown.

First the gNB forwards the Initial UE Message with the Registration Request received from the UE. It follows an Identity Request and Response in which the UE sends its Subscription Concealed Identifier (SUCI). After that, the AMF initiates the authentication procedure sending the NAS signalling security messages. Finally, if the UE responds with the correct credentials, the procedure is completed and the UE registration request is accepted.

Figure 5.6 proves the steps previously explained from the AMF perspective. The log shows the connection of the gNB and the UE Registration process. Note that the AMF contacts first the AUSF to obtain the UE authentication vectors and algorithm information. Then the UDM to register the UE profile and finally contacts the PCF to create a policy association and retrieve the UE policy and/or Access and Mobility control policy.

After the correct subscription to the network, the UE has Internet connectivity and a PDU session is established. This process is confirmed by analyzing the SMF and UPF logs, and the packets transmitted over the N4 interface.

Figure 5.7 shows the PFCP messages exchanged between the CP and the UP to establish the PDU Session. SMF and UPF logs, in Figure 5.8 and in Figure 5.9 respectively, confirm the correct creation of the Session and the communication between NFs inside the 5GC to accomplish the process.

```
08/22 15:53:07.987: [amf] INFO: gNB-N2 accepted[192.168.0.109]:48661 in ng-path module (../src/amf/ngap-sctp.c:
114)
08/22 15:53:07.987: [amf] INFO: gNB-N2 accepted[192.168.0.109] in master_sm module (../src/amf/amf-sm.c:661)
08/22 15:53:07.987: [amf] INFO: [Added] Number of gNBs is now 1 (../src/amf/context.c:878)
08/22 15:53:07.987: [amf] INFO: gNB-N2[192.168.0.109] max_num_of_ostreams : 10 (../src/amf/amf-sm.c:700)
08/22 16:00:29.179: [amf] INFO: InitialUEMessage (../src/amf/ngap-handler.c:361)
08/22 16:00:29.180: [amf] INFO: [Added] Number of gNB-UEs is now 1 (../src/amf/context.c:2087)
08/22 16:00:29.180: [amf] INFO:     RAN_UE_NGAP_ID[1] AMF_UE_NGAP_ID[1] TAC[1] CellID[0x10] (../src/amf/ngap-ha
ndler.c:500)
08/22 16:00:29.181: [amf] INFO: [suci-0-001-01-0000-0-0-0000000001] Unknown UE by SUCI (../src/amf/context.c:14
09)
08/22 16:00:29.182: [amf] INFO: [Added] Number of AMF-UEs is now 1 (../src/amf/context.c:1204)
08/22 16:00:29.182: [gmm] INFO: Registration request (../src/amf/gmm-sm.c:135)
08/22 16:00:29.182: [gmm] INFO: [suci-0-001-01-0000-0-0-0000000001]    SUCI (../src/amf/gmm-handler.c:149)
08/22 16:00:29.184: [app] WARNING: Try to discover [AUSF] (../lib/sbi/path.c:115)
08/22 16:00:29.189: [amf] INFO: [ed40287c-2217-41ed-809e-4fb52766c13e] (NF-discover) NF registered (../src/amf/
nnrf-handler.c:315)
08/22 16:00:29.190: [amf] INFO: [ed40287c-2217-41ed-809e-4fb52766c13e] (NF-discover) NF Profile updated (../src
/amf/nnrf-handler.c:357)
08/22 16:00:29.242: [app] WARNING: Try to discover [UDM] (../lib/sbi/path.c:115)
08/22 16:00:29.242: [amf] INFO: [f10e60f4-2217-41ed-863a-85b874541b04] (NF-discover) NF registered (../src/amf/
nnrf-handler.c:315)
08/22 16:00:29.242: [amf] INFO: [f10e60f4-2217-41ed-863a-85b874541b04] (NF-discover) NF Profile updated (../src
/amf/nnrf-handler.c:357)
08/22 16:00:29.248: [app] WARNING: Try to discover [PCF] (../lib/sbi/path.c:115)
08/22 16:00:29.249: [amf] INFO: [f36ebb5a-2217-41ed-862e-ad3d79ba4a75] (NF-discover) NF registered (../src/amf/
nnrf-handler.c:315)
08/22 16:00:29.249: [amf] INFO: [f36ebb5a-2217-41ed-862e-ad3d79ba4a75] (NF-discover) NF Profile updated (../src
/amf/nnrf-handler.c:357)
08/22 16:00:29.472: [gmm] INFO: [imsi-001010000000001] Registration complete (../src/amf/gmm-sm.c:1116)
08/22 16:00:29.472: [amf] INFO: [imsi-001010000000001] Configuration update command (../src/amf/nas-path.c:430)
08/22 16:00:29.472: [gmm] INFO:     UTC [2022-08-22T14:00:29] Timezone[0]/DST[0] (../src/amf/gmm-build.c:535)
08/22 16:00:29.472: [gmm] INFO:     LOCAL [2022-08-22T16:00:29] Timezone[7200]/DST[1] (../src/amf/gmm-build.c:5
40)
08/22 16:00:29.474: [amf] INFO: [Added] Number of AMF-Sessions is now 1 (../src/amf/context.c:2101)
08/22 16:00:29.475: [gmm] INFO: UE SUPI[imsi-001010000000001] DNN[internet] S_NSSAI[SST:1 SD:0xffffff] (../src/
amf/gmm-handler.c:1062)
```

Figure 5.6: AMF log messages for the UE registration.

19	9.022699737	192.168.0.103	192.168.0.104	PFCP	667	PFCP Session Establishment Request
20	9.023825633	192.168.0.104	192.168.0.103	PFCP	158	PFCP Session Establishment Response
21	9.043900537	192.168.0.103	192.168.0.104	PFCP	112	PFCP Session Modification Request
22	9.044221724	192.168.0.104	192.168.0.103	PFCP	63	PFCP Session Modification Response

Figure 5.7: PDU session establishment PFCP packets over N4 interface.

```
08/22 16:00:29.477: [smf] INFO: [Added] Number of SMF-UEs is now 1 (../src/smf/context.c:893)
08/22 16:00:29.477: [smf] INFO: [Added] Number of SMF-Sessions is now 1 (../src/smf/context.c:2972)
08/22 16:00:29.479: [app] WARNING: Try to discover [UDM] (../lib/sbi/path.c:115)
08/22 16:00:29.480: [smf] INFO: [f10e60f4-2217-41ed-863a-85b874541b04] (NF-discover) NF registered (../s
rc/smf/nnrf-handler.c:294)
08/22 16:00:29.480: [smf] INFO: [f10e60f4-2217-41ed-863a-85b874541b04] (NF-discover) NF Profile updated
(../src/smf/nnrf-handler.c:336)
08/22 16:00:29.482: [app] WARNING: Try to discover [PCF] (../lib/sbi/path.c:115)
08/22 16:00:29.482: [smf] INFO: [f36ebb5a-2217-41ed-862e-ad3d79ba4a75] (NF-discover) NF registered (../s
rc/smf/nnrf-handler.c:294)
08/22 16:00:29.482: [smf] INFO: [f36ebb5a-2217-41ed-862e-ad3d79ba4a75] (NF-discover) NF Profile updated
(../src/smf/nnrf-handler.c:336)
08/22 16:00:29.496: [smf] INFO: UE SUPI[imsi-001010000000001] DNN[internet] IPv4[10.45.0.2] IPv6[] (../s
rc/smf/npcf-handler.c:500)
08/22 16:00:34.511: [gtp] INFO: gtp_connect() [192.168.0.104]:2152 (../lib/gtp/path.c:61)
08/22 16:00:34.514: [app] WARNING: Try to discover [AMF] (../lib/sbi/path.c:115)
08/22 16:00:34.515: [smf] INFO: [c8bdb936-2219-41ed-8e64-e94653b5f348] (NF-discover) NF registered (../s
rc/smf/nnrf-handler.c:294)
08/22 16:00:34.515: [smf] INFO: [c8bdb936-2219-41ed-8e64-e94653b5f348] (NF-discover) NF Profile updated
(../src/smf/nnrf-handler.c:336)
```

Figure 5.8: PDU session establishment on SMF.

```
08/22 16:00:34.508: [upf] INFO: [Added] Number of UPF-Sessions is now 1 (../src/upf/context.c:178)
08/22 16:00:34.509: [gtp] INFO: gtp_connect() [192.168.0.103]:2152 (../lib/gtp/path.c:60)
08/22 16:00:34.509: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[internet] PDN-Type[1] IPv4[10.45.0.2] IPv
6[] (../src/upf/context.c:397)
08/22 16:00:34.509: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[internet] PDN-Type[1] IPv4[10.45.0.2] IPv
6[] (../src/upf/context.c:397)
08/22 16:00:34.529: [gtp] INFO: gtp_connect() [192.168.0.109]:2152 (../lib/gtp/path.c:60)
```

Figure 5.9: PDU session establishment on UPF.

5.2 MC communications over the 5G network

With the active PDU session it is possible to simulate a MC communication through the 5G network.

The MCXPTT application gives the possibility to carry out a test that simulates a complete call. It starts with the establishment of the call, then transmits simulated audio packets and ends with the call closing process.

Figure 5.10 shows the traffic captured at the UPF node. In the image are listed the SIP packets intended to initiate the call. Calls are started by means of the methods INVITE together with SDP (Session Description Protocol) which carry the information necessary to allow the endpoints of the calls to exchange audio in form of RTP (Real-Time Transport Protocol) packets.

As it is possible to see, the packets sent by the UE (10.45.0.5) reach the UPF encapsulated in GTP (GPRS Tunnelling Protocol) messages. The GTP for the user plane (GTP-U) protocol supports multiplexing traffic of different PDU Sessions by tunnelling user data over the N3 interface between gNb and UPF. Once the packets reach the UPF, the encapsulation is removed and the messages are forwarded into the data network through the N6 interface. The replies follow the same path but in the opposite direction.

Time	Source	Destination	Protocol	Length	Info
9.951367291	10.45.0.5	192.168.0.110	SIP/SDP/XML	1213	Request: INVITE sip:mcptt-participant.test.org |
9.968358839	192.168.0.110	10.45.0.5	SIP	1061	Status: 100 TRYING |
9.951375843	192.168.0.104	192.168.0.110	SIP/SDP/XML	1227	Request: INVITE sip:mcptt-participant.test.org |
9.968347471	192.168.0.110	192.168.0.104	SIP	1075	Status: 100 TRYING |
9.988264903	192.168.0.110	192.168.0.104	SIP/SDP/XML	2788	Request: INVITE sip:u1@192.168.0.104:48484 |
9.988489114	192.168.0.110	10.45.0.5	GTP <SIP/SD…	136	Request: INVITE sip:u1@192.168.0.104:48484 |
10.167032668	10.45.0.5	192.168.0.110	SIP	1150	Status: 100 TRYING |
10.167043218	192.168.0.104	192.168.0.110	SIP	1164	Status: 100 TRYING |
10.244362535	10.45.0.5	192.168.0.110	GTP <SIP/SD…	232	Status: 200 OK (INVITE) |
10.244529370	192.168.0.104	192.168.0.110	SIP/SDP/XML	188	Status: 200 OK (INVITE) |
10.262986234	192.168.0.110	10.45.0.5	SIP/SDP/XML	1253	Status: 200 OK (INVITE) |

Figure 5.10: SIP packets with INVITE method to start a call.

Figure 5.11 and 5.12 show the traffic captured on the virtual TUN interface created by UERANSIM for the PDU session. In particular Figure 5.11 shows the packets containing audio

information. The payload of these packets is encoded using Adaptive Multi-Rate Wideband (AMR-WB), that is a patented wideband speech audio coding standard.

Figure 5.12 shows the SIP packets intended to close the call. As a matter of fact, the BYE method signals termination of a dialog and ends a call.

Time	Source	Destination	Protocol	Length	Info
14.989932809	10.45.0.2	192.168.0.110	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6264, Time=51791
14.991642329	192.168.0.110	10.45.0.2	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6264, Time=51791
15.021227603	10.45.0.2	192.168.0.110	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6265, Time=52111
15.022370165	192.168.0.110	10.45.0.2	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6265, Time=52111
15.049887632	10.45.0.2	192.168.0.110	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6266, Time=52431
15.051158945	192.168.0.110	10.45.0.2	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6266, Time=52431
15.069920329	10.45.0.2	192.168.0.110	SRTP	129	PT=AMR-WB, SSRC=0x2EAB2710, Seq=6267, Time=52751

Figure 5.11: Audio packets.

Time	Source	Destination	Protocol	Length	Info
15.280182063	10.45.0.2	192.168.0.110	SIP	1142	Request: BYE sip:mcptt-participant.test.org |
15.281496178	192.168.0.110	10.45.0.2	TCP	52	15060 → 36861 [ACK] Seq=27979 Ack=30947 Win=106752 Len=0 TSval=7775410 TSecr=6952447
15.289454581	192.168.0.110	10.45.0.2	SIP	1051	Status: 200 OK (BYE) |
15.289481772	192.168.0.110	10.45.0.2	SIP	1116	Request: BYE sip:dispatcher@192.168.0.104:54382 |
15.291693480	10.45.0.2	192.168.0.110	TCP	52	54382 → 15060 [ACK] Seq=34289 Ack=35911 Win=115840 Len=0 TSval=6952460 TSecr=7775413
15.293651189	10.45.0.2	192.168.0.110	SIP	1222	Status: 200 OK (BYE) |
15.294769539	192.168.0.110	10.45.0.2	TCP	52	15060 → 54382 [ACK] Seq=35911 Ack=35459 Win=115584 Len=0 TSval=7775423 TSecr=6952460

Figure 5.12: SIP packets with BYE to close the call.

5.3 QoS management over N5 interface

At the moment of the UE registration on the network and the establishment of the PDU session, the PCF receives information of the new connection from the AMF, Figure 5.13, and asks to the UDR information about the registered UE. Thus, the PCF updates its database with the policy rules for that session and communicates them to the SMF.

As the session is active, the simulated MC server, that acts as AF, sends the first HTTP request, with the method POST, to create an application session context in the PCF for that PDU session. In this way, the *Npcf_PolicyAuthorization_Create* service operation authorizes the request from the NF service consumer, and optionally communicates with the *Npcf_SMPolicyControl* service to determine and install the policy according to the information provided by the AF.

The new application session context is represented by an URI, and all the future desired policy modifications, for that PDU session, will affect the information stored at that URI.

In Figure 5.14, the HTTP/2 packets sent by the AF are shown, i.e., the simulated MC server, to create the application session context. The body of the request is written in JSON as defined

```
09/01 11:06:31.770: [sbi] DEBUG: STREAM added [3] (../lib/sbi/nghttp2-server.c:1104)
09/01 11:06:31.770: [sbi] DEBUG: [POST] /npcf-am-policy-control/v1/policies (../lib/sbi/nghttp2-server.c:796)
09/01 11:06:31.770: [sbi] DEBUG: RECEIVED: 844 (../lib/sbi/nghttp2-server.c:799)
09/01 11:06:31.770: [sbi] DEBUG: {
        "notificationUri":      "http://127.0.0.5:7777/namf-callback/v1/imsi-001010000000001/am-policy-notify",
        "supi": "imsi-001010000000001",
        "accessType":   "3GPP_ACCESS",
        "pei":  "imeisv-4370816125816151",
        "userLoc":      {
                "nrLocation":   {
                        "tai":  {
                                "plmnId":       {
                                        "mcc":  "001",
                                        "mnc":  "01"
                                },
                                "tac":  "000001"
                        },
                        "ncgi": {
                                "plmnId":       {
                                        "mcc":  "001",
                                        "mnc":  "01"
                                },
                                "nrCellId":     "000000010"
                        },
                        "ueLocationTimestamp":  "2022-09-01T09:06:31.718985Z"
                }
        },
        "timeZone":     "+02:00",
        "servingPlmn":  {
                "mcc":  "001",
                "mnc":  "01"
        },
        "ratType":      "NR",
        "ueAmbr":       {
                "uplink":       "1048576 Kbps",
                "downlink":     "1048576 Kbps"
        },
        "allowedSnssais":       [{
                        "sst":  1
                }],
        "guami":        {
                "plmnId":       {
                        "mcc":  "001",
                        "mnc":  "01"
                },
                "amfId":        "020040"
        },
        "serviceName":  "namf-callback",
        "suppFeat":     "4"
} (../lib/sbi/nghttp2-server.c:800)
```

Figure 5.13: PCF log messages of PDU session information received by AMF.

No.	Time	Source	Destination	Protocol	Length	Info
3824	27.714895424	192.168.0.107	192.168.0.103	HTTP2	80	Magic
3825	27.714895584	192.168.0.107	192.168.0.103	HTTP2	83	SETTINGS[0]
3828	27.715098871	192.168.0.107	192.168.0.103	HTTP2	69	WINDOW_UPDATE[0]
3830	27.715368249	192.168.0.103	192.168.0.107	HTTP2	71	SETTINGS[0]
3831	27.715428408	192.168.0.107	192.168.0.103	HTTP2	145	HEADERS[1]: POST /npcf-policyauthorization/v1/app-sessions
3833	27.720180695	192.168.0.107	192.168.0.103	HTTP2/JSON	553	DATA[1], JavaScript Object Notation (application/json)
3834	27.720182006	192.168.0.107	192.168.0.103	HTTP2	65	SETTINGS[0]
3843	27.793110455	192.168.0.103	192.168.0.107	HTTP2	65	SETTINGS[0]
3861	27.793762619	192.168.0.103	192.168.0.107	HTTP2	176	HEADERS[1]: 201 Created
3862	27.793852892	192.168.0.103	192.168.0.107	HTTP2/JSON	623	DATA[1], JavaScript Object Notation (application/json)

Figure 5.14: HTTP/2 packets over N5 interface to invoke the *Npcf_PolicyAuthorization_Create* service.

by the standard [30], Figure 5.15, and, in addition to creating the application session context, it also requires the installation of some rules.

```
06/30 11:54:40.100: [sbi] DEBUG: STATUS [201] (../lib/sbi/nghttp2-server.c:347)
06/30 11:54:40.100: [sbi] DEBUG: SENDING...: 475 (../lib/sbi/nghttp2-server.c:355)
06/30 11:54:40.100: [sbi] DEBUG: {
        "ascReqData":   {
                "dnn":  "internet",
                "medComponents":        {
                        "0":    {
                                "fStatus":      "ENABLED",
                                "medCompN":     6,
                                "medSubComps":  {
                                        "0":    {
                                                "fNum": 0,
                                                "fDescs":       ["permit out udp from 192.168.0.110 10000 to 10.45.0.2 any", "permit out udp from 10.45.0.2 1-65535 to 192.168.0.110 10000"]
                                        }
                                },
                                "medType":      "AUDIO"
                        }
                },
                "notifUri":     "http://192.168.0.107",
                "supi": "imsi-001010000000001:2",
                "suppFeat":     "0",
                "ueIpv4":       "10.45.0.2"
        }
} (../lib/sbi/nghttp2-server.c:356)
```

Figure 5.15: Body of the HTTP/2 request seen by the PCF log.

No.	Time	Source	Destination	Protocol	Length	Info
740	385.518585952	192.168.0.103	192.168.0.104	PFCP	399	PFCP Session Modification Request
741	385.519199903	192.168.0.104	192.168.0.103	PFCP	86	PFCP Session Modification Response

```
IE Type: Create PDR (1)
IE Length: 192
> PDR ID : 7
> Precedence : 1
v PDI : [Grouped IE]
    IE Type: PDI (2)
    IE Length: 150
  > Source Interface : Core
  > Network Instance : internet
  v SDF Filter :
      IE Type: SDF Filter (23)
      IE Length: 60
    > Flags: 0x01, FD (Flow Description)
      Spare: 0
      Length of Flow Description: 56
      Flow Description: permit out udp from 192.168.0.110 10000 to 10.45.0.2 any
  v SDF Filter :
      IE Type: SDF Filter (23)
      IE Length: 64
    > Flags: 0x01, FD (Flow Description)
      Spare: 0
      Length of Flow Description: 60
      Flow Description: permit out udp from 10.45.0.2 1-65535 to 192.168.0.110 10000
```

Figure 5.16: PFCP packets over N4 interface to assign the new policy rules.

The HTTP request is authorized, and the PCF proceeds to fulfill the desired policies and communicates to the other NFs the new information in order to fix the whole network to support the requested KPIs as described in Chapter 4, Figure 4.1.

In Figure 5.16 the SMF informing the UPF can be seen, over the N4 interface, of the policy changes that need to be applied for that PDU session.

There are other different HTTP requests that the AF can send to the PCF in order to perform QoS management, as described in Section 4.1, Table 4.1.

The Open5gs project supports the CREATE, UPDATE, and DELETE service operations, while SUBSCRIBE and UNSUBSCRIBE are not yet developed. This is because with CREATE and UPDATE it is also possible to cover the SUBSCRIBE and UNSUBSCRIBE func-

tions and therefore their development would be redundant.

Figure 5.17 presents the HTTP/2 packets sent to invoke the UPDATE service operation. The request must be sent to the URL addressing the previously created application session context in the PCF and must present the PATCH method in the header.

The UPDATE service operation updates the policy rules according to the modified service information provided by the authorized AF. In Figure 5.18 the AF is indicating to the PCF that some pre-emption information can be assigned to the PDU considered session.

http2

No.	Time	Source	Destination	Protocol	Length	Info
2281	18.579280199	192.168.0.107	192.168.0.103	HTTP2	80	Magic
2282	18.579280312	192.168.0.107	192.168.0.103	HTTP2	83	SETTINGS[0]
2283	18.579280431	192.168.0.107	192.168.0.103	HTTP2	69	WINDOW_UPDATE[0]
2287	18.579534107	192.168.0.107	192.168.0.103	HTTP2	152	HEADERS[1]: PATCH /npcf-policyauthorization/v1/app-sessions/1
2288	18.579534430	192.168.0.107	192.168.0.103	HTTP2/JSON	526	DATA[1], JavaScript Object Notation (application/json)
2291	18.580100601	192.168.0.103	192.168.0.107	HTTP2	71	SETTINGS[0]
2293	18.580832778	192.168.0.107	192.168.0.103	HTTP2	65	SETTINGS[0]
2300	18.586737125	192.168.0.103	192.168.0.107	HTTP2	65	SETTINGS[0]
2303	18.586849455	192.168.0.103	192.168.0.107	HTTP2	122	HEADERS[1]: 200 OK
2305	18.586893112	192.168.0.103	192.168.0.107	HTTP2/JSON	541	DATA[1], JavaScript Object Notation (application/json)

Figure 5.17: HTTP/2 traffic over N5 interface to invoke the UPDATE service.

There is also the possibility to DELETE a complete application session context stored in the PCF by transmitting an HTTP POST request to the URI representing that resource. Figure 5.19 shows the HTTP/2 packets sent by the AF to completely remove the application session context and all the policies associated to it.

Figure 5.20 presents the PCF log messages triggered by the DELETE service operation. The PCF receives the HTTP request and deletes the application session context with all the rules assigned for that PDU session. Then it contacts the SMF, through the N7 interface, removing all the rules previously associated to the PDU session.

```
07/14 11:05:07.912: [sbi] DEBUG: STATUS [200] (../lib/sbi/nghttp2-server.c:347)
07/14 11:05:07.912: [sbi] DEBUG: SENDING...: 476 (../lib/sbi/nghttp2-server.c:355)
07/14 11:05:07.912: [sbi] DEBUG: {
        "ascReqData":   {
                "afAppId":      "urn:urn-7:3gpp-service.ims.icsi.mcptt",
                "evSubsc":      {
                        "events":       [{
                                        "event":        "NULL",
                                        "notifMethod":  "EVENT_DETECTION"
                                }],
                        "notifUri":     "192.168.0.107"
                },
                "mcpttId":      "sip:dispatcher@test.org",
                "medComponents":        {
                        "0":    {
                                "medCompN":     6,
                                "medType":      "AUDIO",
                                "preemptCap":   {
                                },
                                "preemptVuln":  {
                                },
                                "prioSharingInd":       "ENABLED"
                        }
                },
                "preemptControlInfo":   {
                },
                "resPrio":      "PRIO_1"
        }
} (../lib/sbi/nghttp2-server.c:356)
```

Figure 5.18: PCF log view of the correct reception of the UPDATE service invocation.

No.	Time	Source	Destination	Protocol	Length	Info
98535	5023.601601	192.168.0.107	192.168.0.103	HTTP2	78	Magic
98536	5023.601646	192.168.0.107	192.168.0.103	HTTP2	81	SETTINGS[0]
98537	5023.601674	192.168.0.107	192.168.0.103	HTTP2	67	WINDOW_UPDATE[0]
98538	5023.601903	192.168.0.103	192.168.0.107	HTTP2	69	SETTINGS[0]
98539	5023.602375	192.168.0.107	192.168.0.103	HTTP2	148	HEADERS[1]: POST /npcf-policyauthorization/v1/app-sessions/1/delete
98540	5023.602548	192.168.0.107	192.168.0.103	HTTP2	63	SETTINGS[0]
98541	5023.602613	192.168.0.107	192.168.0.103	HTTP2/JSON	184	DATA[1], JavaScript Object Notation (application/json)
98551	5023.613418	192.168.0.103	192.168.0.107	HTTP2	63	SETTINGS[0]
98552	5023.613519	192.168.0.103	192.168.0.107	HTTP2	101	HEADERS[1]: 204 No Content

Figure 5.19: HTTP/2 traffic over N5 interface to invoke the DELETE service.

```
07/14 11:05:07.912: [sbi] DEBUG: STATUS [200] (../lib/sbi/nghttp2-server.c:347)
07/14 11:05:07.912: [sbi] DEBUG: SENDING...: 476 (../lib/sbi/nghttp2-server.c:355)
07/14 11:05:07.912: [sbi] DEBUG: {
        "ascReqData":   {
                "afAppId":      "urn:urn-7:3gpp-service.ims.icsi.mcptt",
                "evSubsc":      {
                        "events":       [{
                                        "event":        "NULL",
                                        "notifMethod":  "EVENT_DETECTION"
                                }],
                        "notifUri":     "192.168.0.107"
                },
                "mcpttId":      "sip:dispatcher@test.org",
                "medComponents":        {
                        "0":    {
                                "medCompN":     6,
                                "medType":      "AUDIO",
                                "preemptCap":   {
                                },
                                "preemptVuln":  {
                                },
                                "prioSharingInd":       "ENABLED"
                        }
                },
                "preemptControlInfo":   {
                },
                "resPrio":      "PRIO_1"
        }
} (../lib/sbi/nghttp2-server.c:356)
```

Figure 5.20: PCF process to delete the application session context previously created.

6 Conclusion

The entry into the market of the 5G network has forced operators and organizations of the IT sector to ask themselves how to exploit these new technologies to continue providing services with ever greater effectiveness.

This thesis aimed at understanding how QoS management can be applied to MC communications, which require greater guarantees in terms of availability and reliability, exploiting the benefits that the 5G cellular technology brings with it.

Two solutions were considered: the development of a Network Slice dedicated to MC communications and the use of the N5 interface that connects the PCF and the AF.

The first solution, presented in Chapter 3, is based on Network Slicing technology. The idea is to consider a dedicated logical network where MC communications have higher priorities than the other connections present in the network. To achieve this, three scenarios were considered, in which public security forces have to intervene in emergency situations, and it is necessary to organize the various operations using efficient and timely communications.

In the considered scenarios, users adopt smartphones on which the MCXPTT application, developed by Alea S.rl. is installed to make audio and video calls compliant with the MCX standard developed by the 3GPP.

At this point, the performance parameters that the 5G network must provide for MC communications to be guaranteed in such situations have been listed. From these parameters it was therefore possible to identify the KPIs that the hypothesized Network Slice must respect in order for the 5G network to support MC services.

The second solution involves the development of the N5 interface. It allows applications, outside the 5G core network, to install, modify, and/or remove policy rules regarding specific PDU sessions, identified by IP address, SUPI, and other properties, active at that moment in the network.

In the case of MC services, the N5 interface is used by the MC server, located in the SIP

core network, to guarantee optimal QoS levels to users who need to carry out critical communications, by sending HTTP/2 requests to the PCF, the element of the 5GC delegated to the management of policy rules.

To verify the functionality of the Interface and, therefore, the goodness of the developed HTTP requests, it was necessary to recreate the suitable test environment. For this purpose, the following tools were used: a software that implements the 5G network, a UE and gNB simulator to establish PDU sessions that connect to the network, and the MCXPTT application by Alea S.r.l. to generate MC communications to which the desired policy rules will then be applied.

The entire infrastructure is composed of free and open-source software, compliant with the latest ETSI technical specifications, running on common-off-the-shelf hardware. In particular, the Open5gs implementation for the 5GC and the UERANSIM implementation for 5G UE and RAN (gNodeB) were used.

After having configured and connected the various elements together, and having started the PDU session, on which an MC call is carried out, the HTTP requests were sent so that the desired policy rules were accepted and applied, and the effects that these have on the 5G network were analyzed. This was possible thanks to the study of the log files of the different NFs and the analysis of the traffic exchanged by the various network elements.

Comparing the two solutions it is possible to state that both present advantages and disadvantages.

A Network Slice in charge of MC services is certainly an effective and innovative strategy, as it offers service availability and reliability, creating a totally independent logical network with guaranteed resources whenever needed. It also allows the management of QoS through all levels, from radio access to the network, up to the transport layer and the core network. However, the realization of a NS requires many complicated steps, such as: the definition of the algorithms to distribute the resources among the different Network Slices, the development of the scheduler that will have to apply these algorithms, make deals with the network suppliers, manage and control the correct functionality of the NS during its life cycle, etc.

For these reasons, the exploitation of the N5 interface presents an excellent alternative to Network Slicing technology, ensuring effective management of QoS with less effort in terms of complexity and waste of resources.

References

[1] A. Detti, *5G Italy, White eBook, FUnctional Architecture*. CNIT, 2018.

[2] S. Rommer, P. Hedman, M. Olsson, L. Frid, S. Sultana, and C. Mulligan, *5G Core Networks: powering digitalization*. Elsevier Science, 2019.

[3] *Technical Realization of Service Based Architecture; Stage 3*, 3GPP Std., Sept. 2021, tS 29.500.

[4] *Principles and Guidelines for Services Definition; Stage 3*, 3GPP Std., Nov. 2020, tS 29.501.

[5] *System Architecture for the 5G System (5GS)*, 3GPP Std., Oct. 2020, tS 23.501.

[6] Y. Lair and G. Mayer. Mission critical services in 3gpp. [Online]. Available: https://www.3gpp.org/news-events/1875-mc_services#:~:text=Mission%20Critical%20Services%20in%203GPP%20Rel%2D14,MCData

[7] Höyhtyä, Marko, Lähetkangas, Kalle, Suomalainen, Jani, Hoppari, Mika, Kujanpää, Kaisa, T. Ngo, Kien, Kippola, Tero, Heikkilä, Marjo, Posti, Harri, Mäki, Jari, Savunen, Tapio, Hulkkonen, Ari, Kokkinen, and Heikki, "Critical communications over mobile operators' networks: 5g use cases enabled by licensed spectrum sharing, network slicing and qos control," *IEEE Access*, vol. 6, pp. 73 572–73 582, 2018.

[8] *Mission Critical Push to Talk (MCPTT), Stage 1*, 3GPP Std., July 2018, tS 22.179.

[9] *Mission Critical Data Services*, 3GPP Std., July 2018, tS 22.282.

[10] *Mission Critical Video Services*, 3GPP Std., Sept. 2018, tS 22.281.

[11] *Mission Critical Common Requirements*, 3GPP Std., July 2018, tS 22.280.

[12] *SIP: Session Initiation Protocol*, IETF Std., March 1999, rFC 2543.

[13] A. B. Johnston, *SIP: Understanding the Session Initiation Protocol*. Artech House, 2004.

[14] *Policy and charging control architecture*, 3GPP Std., Sept. 2018, tS 23.203.

[15] *Procedures for the 5G System; Stage 2*, 3GPP Std., Nov. 2020, tS 29.502.

[16] *Policy and Charging Control Framework for the 5G System; Stage 2*, 3GPP Std., July 2020, tS 23.503.

[17] *Aspects; Management and orchestration; Concepts, use cases and requirements*, 3GPP Std., Dec. 2019, tS 28.530.

[18] *Service requirements for the 5G system; Stage 1*, 3GPP Std., Sept. 2018, tS 22.261.

[19] C. Giulia, C. Edoardo, and T. Stefano, "Critical communications over mobile operators' networks: 5g use cases requirements and enablers of advanced healthcare services over future cellular systems," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 76–81, 2020.

[20] Ericsson, *5G-powered FRMCS*. Ericsson White Paper, 2022.

[21] *5G, Mobile Communication System for Railways*, 3GPP Std., Nov. 2020, tS 22.289.

[22] *Mission Critical (MC) Video*, 3GPP Std., Apr. 2022, tS 22.281.

[23] *Mission Critical Push to Talk (MCPTT), Stage 1*, 3GPP Std., Nov. 2020, tS 22.179.

[24] J. Pérez-Romero, I. Vilà, O. Sallent, B. Blanco, A. Sanchoyerto, R. Solozábal, and F. Liberal, "Supporting mission critical services through radio access network slicing," *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pp. 1–8, 2019.

[25] M. Volk and J. Sterle, "5g experimentation for public safety: Technologies, facilities and use cases," *IEEE Access*, vol. 9, pp. 41 184–41 217, 2021.

[26] Ericsson. Ericsson trials drone-mounted network. [Online]. Available: https : / / www . ericsson . com / en / news / 2020 / 12 / ericsson-drone-mounted-network-could-support-emergency-response

[27] J. Li, K. K. Nagalapur, E. Stare, S. Dwivedi, S. A. Ashraf, P.-E. Eriksson, U. Engström, W.-H. Lee, and T. Lohmar, "5g new radio for public safety mission critical communications," *IEEE Communications Standards Magazine*, 2021.

[28] R. Schmidt, C.-Y. Chang, and N. Nikaein, "Slice scheduling with qos-guarantee towards 5g," *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, 2019.

[29] *5G System; Policy and Charging Control signalling flows and QoS parameter mapping, Stage 3*, 3GPP Std., May 2022, tS 23.513.

[30] *5G System; Policy Authorization Service, Stage 3*, 3GPP Std., Nov. 2020, tS 29.514.

[31] I. Grigorik, *High Performance Browser Networking*. O'Reilly, 2013.

[32] *Interface between the Control Plane and the User Plane Nodes; Stage 3*, 3GPP Std., Jun. 2022, tS 29.244.