University of Genoa

Polytechnic School

A comparative Analysis for Open-Source Software for 5G Radio Access Network Emulation

"Analisi comparativa di software open-source per emulazione di reti di accesso 5G"

Supervisor:

Professor: Franco **DAVOLI**

Professor: Roberto **BRUSCHI**

Author:

Georges Julien **TAAKAM SADEU**

Co-supervisor:

Dr.ssa: Chiara **LOMBARDO**

Dr: Sergio **MANGIALARDI**

June 2023

Contents

SUMMARY

This thesis provides an overview of some features of the fifth generation (5G) wireless communication systems. The emphasis is on architectural aspects of the access and core networks with a short mention of the beamforming technology, which is the technique used to implement directional signals toward the mobile devices. With the development of 5G speeding up [1], we can see a clearer picture of what the future generation wireless network would be able to achieve, also in term of coverage areas.

The 5G core network aims to be flexible enough to adapt and satisfy the offering of Gbps speeds for smartphone users, as well as low latency for critical services, along with the support of massive quantities of low speed devices in the Internet of Things (IoT). It is also being designed to be more open and modular than its predecessors, allowing the different entities inside the core network to interact with each other without any preconditions and allowing to define procedures for this interaction. This is achieved with the help of new techniques like Network Functions Virtualization (NFV), Network Slicing, and Software Defined Networking (SDN) [2].

The main goal for this master's thesis is to better understand the 5G networking environment, which is a key part of the worldwide digital transformation that stands to impact consumers; for this raison, we configured the UERANSIM 5G simulator to simulate signal transmission from User Equipment (UE) through the radio base station (gNodeB) to the destination. This tool, compared with the srsLTE 4G simulator reveals the advantages, and can be used to analyze the performance of the 5G wireless communication system.

1 CHAPTER I. INTRODUCTION

The Fifth generation (5G) New Radio (NR) air interface is expected to be the foundation of very heterogenous networks serving a wide range of use cases as Ultra Reliable Low Latency Communications (URLLC) in which small data packets must be correctly transmitted and received in a short time with high reliability, massive Machine-Type Communications (mMTC) and enhanced Mobile Broadband (eMBB). In this master's thesis, the focus is on the 5G architecture, by trying to understand how the different functional blocks work, and their mutual interaction to establish communication between devices and ensure a certain performance level, and then to understand how the interfacing takes place at different levels of the architecture.
Before a short description of the 5G architecture, we will briefly examine 4G LTE(Long Term Evolution) the previous technology which allows lower performance and lower speed than the actual 5G. As regards 4G LTE, after an overview of the basic system architecture, we will describe the installation and configuration of the 4G simulator software radio system Long Term Evolution (srsLTE) that will be used to simulate the transmission of signals from User Equipment (UE) through the radio base station(eNB) to the destination. In the end, the result will be compared to that of the 5G simulator UERANSIM to detect the performance, advantages and disadvantages of different technologies or changes. The main goal is to well understand the 5G network, which is a key part of the worldwide digital transformation that stands to impact consumers, public sector organizations and enterprises across every vertical industry. New devices and applications are already emerging on the market to take advantage of 5G's dramatically reduced latency and much higher data speeds [3]. For this master's thesis we will install and configure one of the lastest software versions of the 5G network simulator UERANSIM, which can be used to simulate UEs and 5G Radio Access Network (RAN), to put test calls through our (5GC) [5].
The thesis, will be structured in 6 Chapters: Chapter II 5G Technology, Chapter III srsLTE and UERANSIM, Chapter IV Simulations Environments and Chapter V Performance Evaluation.

2 CHAPTER II. 5G TECHNOLOGY

5G represents the latest innovation in the Internet and telecommunications fields, and especially in the mobile communications sector.
5G (acronym for 5th Generation) indicates the fifth generation of mobile phone technologies, more powerful than fourth generation ones, and allowing much higher performance and speed than the current 4G / IMT Advanced technology. So, 5G has become quite relevant, as it is an enabling technology for new technological challenges worldwide.

2.1 5G Architecture

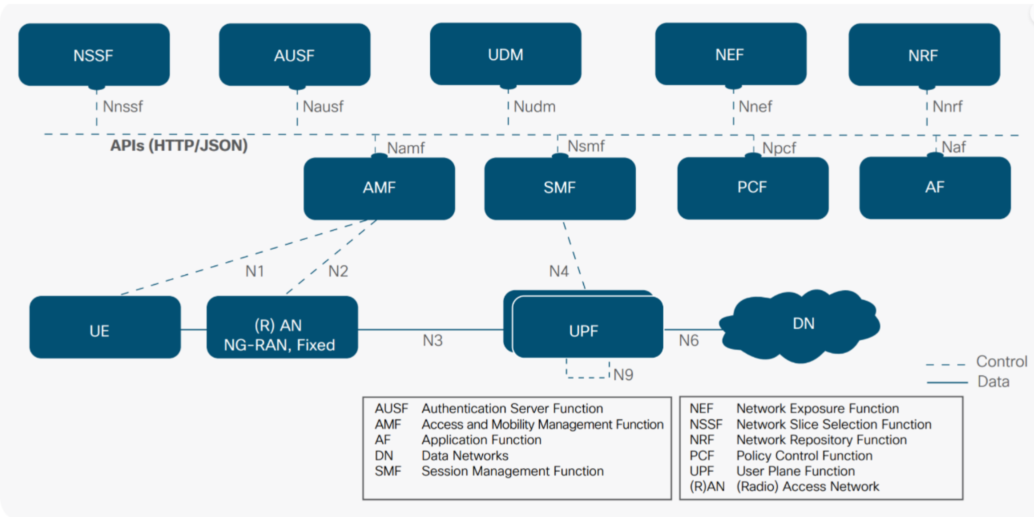


Fig. I.1: Service Based Architecture for 5G System.

The reference 5G architecture is shown in Fig. I.1 (Service Based Architecture, SBA). To describe this architecture, it is important to refer to the 3GPP (3rd Generation Partnership Project), which is defining standards for 5G. 3GPP is a generic term for a number of standards organizations developing protocols for mobile telecommunications. According to the 3GPP the 5G system will have three main components.

1- User Equipment (UE)
UEs are the 5G enabled devices.

2- 5G Radio Access Network (5G-RAN)
It is the network infrastructure commonly used for mobile communications, which is formed by radio base stations.

The RAN connects user equipment to the core network.

3- 5G Core Network (5GC)

It implements various Network Functions, such as session management, authentication, policy control, data storage, etc.

The Core Network Architecture Evolution in 5G will enable, among others, the following services:

- Virtualization and slicing.
- Softwearization / Cloudification.
- Application Programming Interfaces.
- Harmonized protocols (HTTP .....).
- Exposure to 3rd parties.
- Backward and Forward compatibility.

2.2 5G Core Architecture

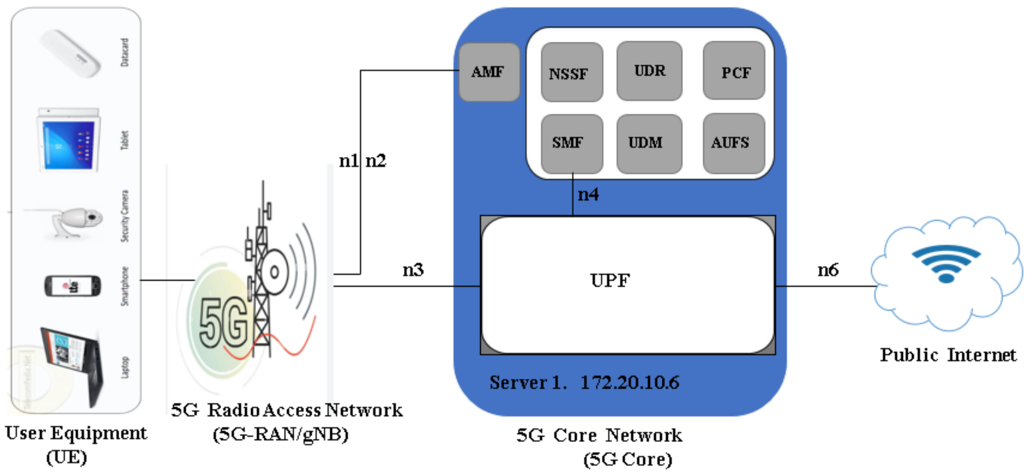


Fig. I.2: UE and 5G-RAN

The 5G core architecture is synthetically depicted in Fig. I.2. Unlike previous cellular networks, the 5G Core network architecture was designed by exploiting the paradigms of Network Function Virtualization (NFV) and Software Defined Networking (SDN). Basically, the 5G Core network adapts a microservices-based design pattern. The different data services and requirements of the 5G Core (5GC), under the general term of Network Functions (NFs) are implemented as microservices.
These NF microservices will be deployed in the same fashion as cloud native applications. The 5G Core System contains a large number of Network

Functions. The main differences with respect to the fourth generation Long Term Evolution (LTE) architecture can be noticed by comparing Fig. I.3 and Fig. I.4.

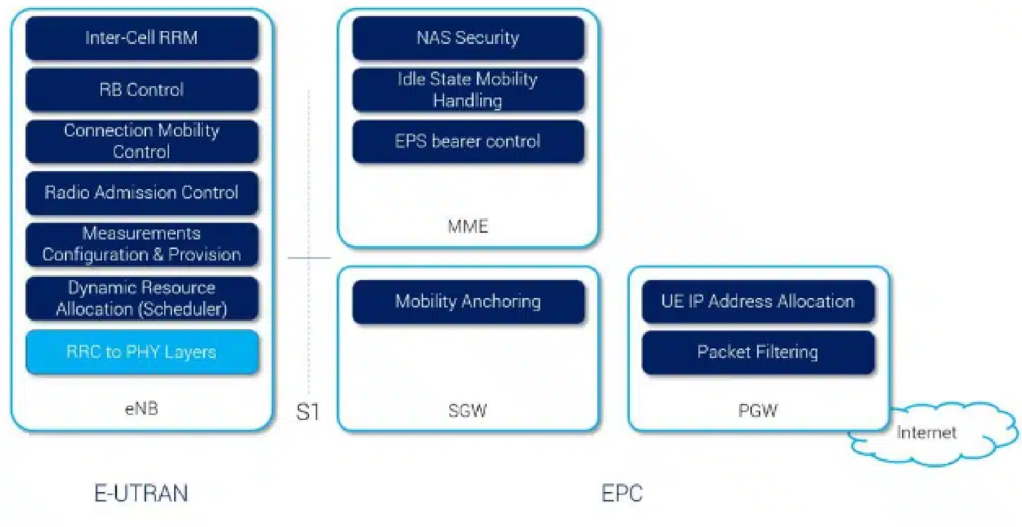


Fig. I.3: Evolved Packet Core (EPS) Functions Split

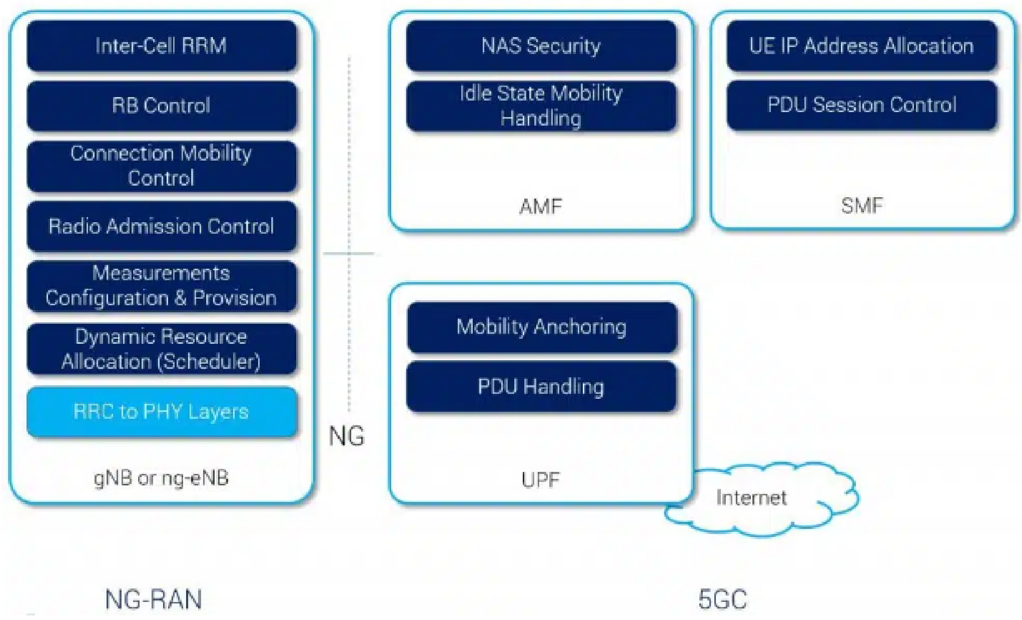


Fig. I.4: 5G System Functions Split

Such differences may be summarized synthetically in three steps as in the following.

Firstly, the nomenclature: in LTE there is a simple pure nomenclature using the "Evolved" term: E-UTRA (radio interface), eNB (base station), E-UTRAN (RAN), EPC (CN), EPS (system); in 5G, in turn, there are many different names with a variation of "5G" and "new/next generation": NR (New Radio – radio interface), gNB or ng-eNB (base station), NG-RAN (RAN), 5GC (CN), 5GS (system).

Secondly, the function split in the CN: LTE still exhibits a certain mix between Control Plane (CP) and User Plane (UP) functions in the different network nodes; in 5G one finds a full CP/UP split, with many CP network functions and the User Plane Function (UPF), doing solely data plane processing.

Thirdly, in 5G some new functionality, not present before, has been introduced. Among others, the new approach to 5GC using the Service Based Architecture (SBA); the concept of network slicing, allowing the coexistence of different virtual networks upon the same hardware infrastructure; a new Quality of Service (QoS) framework.

The Core Network Control Plane splits into Access and Mobility Management Function (AMF) and Session Management Function (SMF) responsibilities. A given device is assigned a single AMF to handle mobility and access roles, but can then have multiple SMFs, each dedicated to a given network slice. The Core Network User Plane is the support for multiple UPFs serving the same device, handled by a single UPF instance and hence avoiding the need for a common Serving Gateway (SGW) used in LTE.

UPF: may be daisy-chained to offer local breakout and may have parallel nodes serving the same APN to assist seamless mobility.

AMF: is the single functionality to manage all UE-related functions. The EPC functionalities of the Mobility Management Entity (MME), SGW and PDN Gateway (PGW) have been reallocated, so that all access and mobility functionalities are performed by the AMF.

AUSF (Authentication Server Function): is the new specification included by the Front End (FE) section and it is dedicated to authenication processing.

SMF: it has the responsibility for the setup of the connectivity for the UE towards Data Networks as well as managing the User Plane for that connectivity.

It collects all the informations related to PDU session management from various network components (e.g, UPF, PCF, UDM) and controls / orchastrates those network components based on request from AMF.

NSSF (Network Slicing Selection Function): supports the following functionality:
- Selecting the set of Network Slice instances serving the UE.
- Determining the Allowed NSSAI(Network Slice Selection Assistance Information) and, if needed, the mapping to the Subscribed S-NSSAIs (Single – Network Slice Selection Assistance Information).
- Determining the Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs.The S-NSSAIs is Used in support of Network Slicing, also used to uniquely identify a Network Slice. The S-NSSAIs contains two components: the SST (Slice/Service Type) and an optional SD (Slice Differentiator).
- Determining the AMF Set to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF (see below).

NEF (Network Exposure Function): it stores/retrieves information as structured data using a standardized interface to the Unified Data Repository.

- Secure provision of information from external applications to the 3GPP network.
- NEF handles masking of network and user sensitive information to external AF's according to the network policy.
- Translates between information exchanged with the AF and information exchanged with the internal network function. For example, it translates between an AF-Service-Identifier and internal 5G Core information such as DNN(Data Network Name), S-NSSAI.

NRF (Network Repository Function): it is the main network function in the service based architecture and plays a key role. All network functions register the services they offer with the NRF using a service registration procedure, and later they use the NRF as a database to discover the services offered by other Networks with service discovery and service authorization procedure. NRF supports the following functionality:
- Supports service discovery function. Receives NF Discovery Requests

from NF instances.
- Maintains the NF profile of available NF instances and their supported services. Differents Network Functions (NF) are connected together via a uniforn interface called a service-based interface. NF can directly access an NF service in another NF without having to pass through another node.

PCF (Policy Control Function): it includes the following functionality:
- determines the resources and services that can be used to support connected devices.
- Supports a unified policy framework to govern network behaviour.
- Provides policy rules to Control Plane function(s) to enforce them.
- Accesses subscription information relevant for policy decisions in a Unified Data Repository (UDR).

UDM (Unified Data Management): is analogous to the Home Subscriber Server in EPC architecture and introduces the concept of User Data Convergence (UDC) that separates the User Data Repository (UDR) storing and managing subscriber information from the front end processing subscriber information. The UDM manages data for access authorization, user registration, and data network profiles. Subscriber data is provided to the session management function (SMF), which allocates IP addresses and manages user sessions on the network.

AF (Aplication Function): is a control plane function within 5G core network, provides application services to the subscriber. Interacts with the 3GPP Core Network in order to provide services, for example to support the following:

- Application influence on traffic routing.
- Accessing Network Exposure Function.
- Interacting with the Policy framework for policy control.

Based on operator deployment, Application Functions considered to be trusted by the operator can be allowed to interact directly with relevant Network Functions.

UDR (Unified Data Repository): it supports the following functionality:

- Storage and retrieval of subscription data by the UDM.
- Storage and retrieval of policy data by the PCF.

- Storage and retrieval of structured data for exposure.

The Unified Data Repository is located in the same PLMN as the NF service consumers storing in and retrieving data from it using Nudr. Nudr is an intra-PLMN interface see Fig. I.5

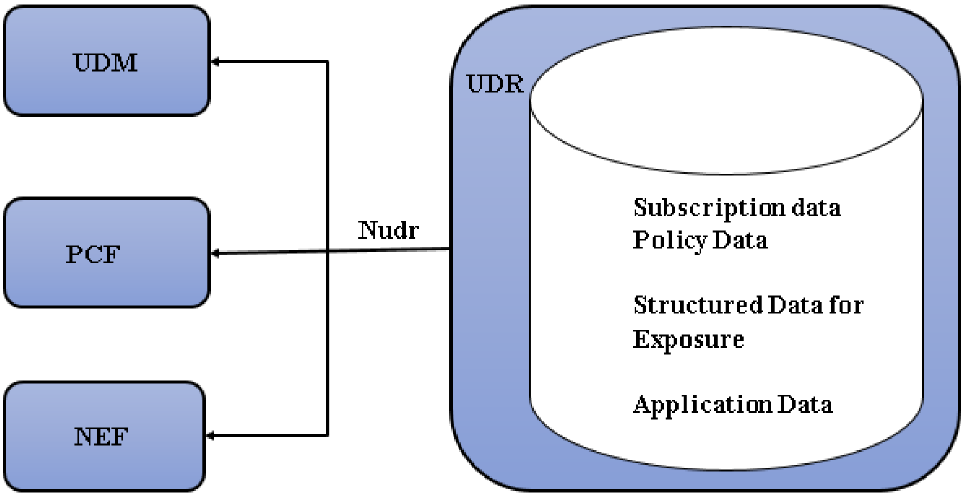


Fig. I.5: Nudr Reference point

The PCF interfaces with the UDR to retrieve subscriber-related policies for User Equipment attach and session establishment. When a UE attaches to the network, AMF requires AM policies of the subscriber from PCF for the UE. Similarly, when a UE makes a PDU session, SMF requires policy rules from PCF. Subscriber attributes are stored in the UDR. PCF communicates with UDR to retrieve these attributes which are used in the evaluation of policies.
PCF invokes the Nudr-DataRepository service to retrieve the AM and SM policy attributes. PCF carries out the discovery of UDR URL through the Nnrf-NFDiscovery service which is the NRF service.

The UDR provisions PCF to retrieve the data stored in the UDR through the Nudr-DataRepository service. The service is also responsible for enabling NF to subscribe and unsubscribe to the data change notifications from UDR. as regards PCF, the Nudr-DataRepository service provides the following retrieve services to access policy control-related subscription information and application-specific information that is stored in the UDR.

- Subscription to notifications from the UDR on changes in the policy control related subscription information.

- Subscription to the UDR for the AF requests targeting a DNN and S-NSSAI or a group of UEs that are iidentified by an Internal Group Identifier.
- Subscription to notifications from the UDR on the update of AF requests targeting a DNN and S-NSSAI or a group of UEs identied by an Internal Group Identifier.

A DNN on a 5G network identifies an external data network and is equivalent to an access point name (APN) on a 4G network.
We remark that, Depending on the construction of the 5G architecture, both UDM software and the UDR can send and store data. In a stateless network, user information is stored in the UDR, but the UDM function retrieves the data, sends it to other network functions, and generally manages it.
Fig. I.6 and Figure. I.7 summarize the call flow of the AM and SM policy association establishment procedures.

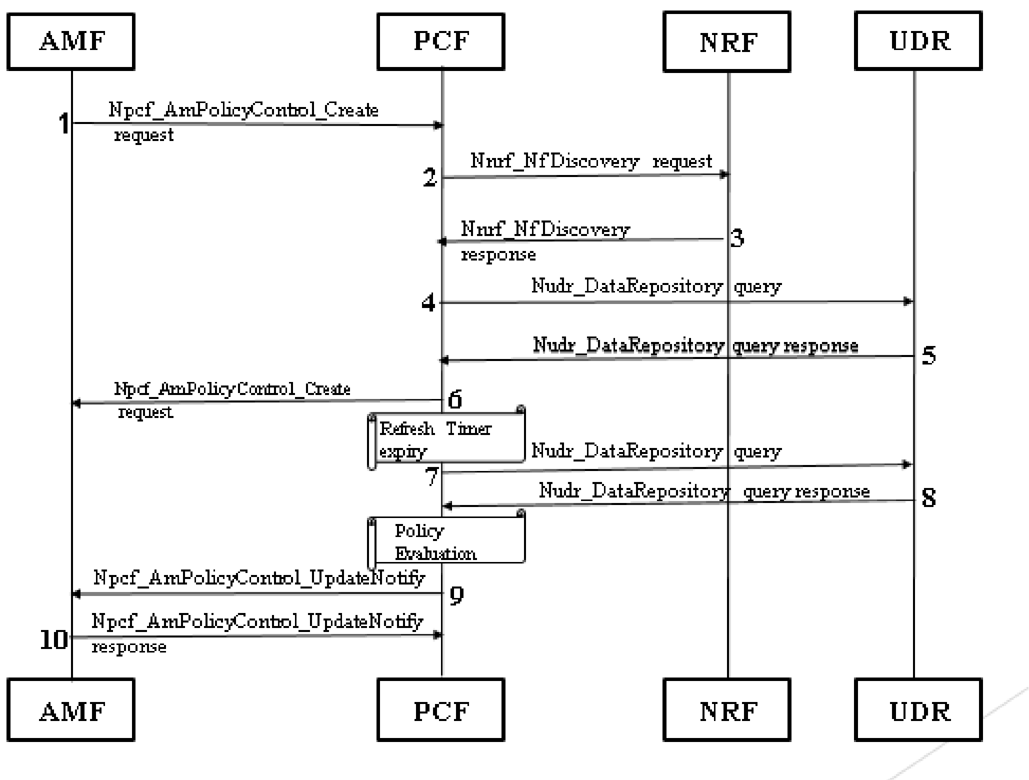


Fig. I.6: AM Policy Subscription

Step	Description
1	The AMF sends a Npcf_AmPolicyControl_Create request to the PCF.
2	If the UDR URL is not configured, the PCF sends the Nnrf_NFDiscovery request is sent to NRF.
3	In response, the NRF sends the Nnrf_NFDiscovery results to the PCF.
4	The PCF sends the Nudr_DataRespository query to the UDR.
5	In response, the UDR sends the repository details to the PCF.
6	The PCF sends the Npcf_AmPolicyControl_Create request to the AMF.
7	The PCF sends the Nudr_DataRepository query to the UDR.
8	The UDR responds to PCF with the repository information.
9	After PCF evaluates the response, if the policy has modified, then the PCF sends the Npcf_AmPolicyControl_UpdateNotify request to the AMF.
10	The AMF sends the Update Notification as a response to the PCF.

Table.I.1: AM Policy Description

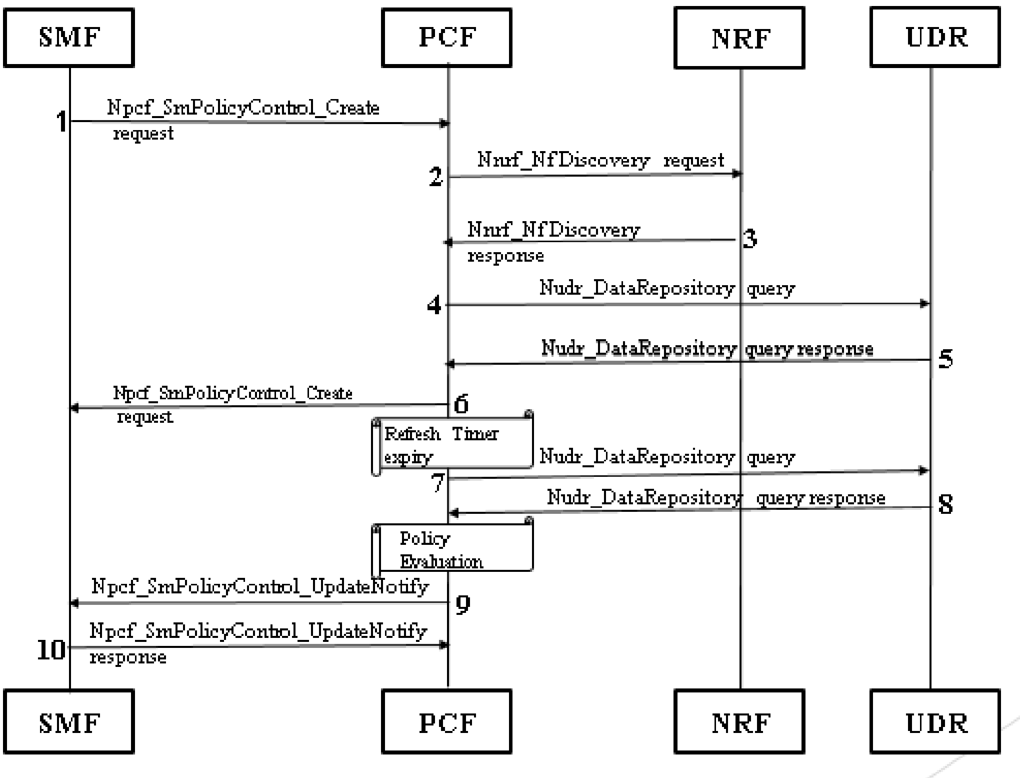


Fig. I.7: SM Policy Subscription

Step	Description
1	The SMF sends a Npcf_SmPolicyControl_Create request to the PCF.
2	If the UDR URL is not configured, the PCF sends the Nnrf_NFDiscovery request to NRF.
3	In response, the NRF sends the Nnrf_NFDiscovery results to the PCF.
4	The PCF sends the Nudr_DataRespository query to the UDR.
5	In response, the UDR sends the repository details to the PCF.
6	The PCF sends the Npcf_SmPolicyControl_Create request to the SMF.
7	The PCF sends the Nudr_DataRepository query to the UDR.
8	The UDR responds to PCF with the repository information.
9	After PCF evaluates the response, if the policy has modified, then the PCF sends the Npcf_SmPolicyControl_UpdateNotify request to the SMF.
10	The SMF sends the Update Notification as a response to the PCF.

Table I.2: SM Policy Description

2.3 5G Dual Connectivity and Architecture Overview

With 5G, the network architecture evolves more and more towards the concept of software defined network, where the nodes and the various functional components of the network are no longer made up of specialized hardware but, simplifying, cloud infrastructures on which programs that replicate run those services that were previously performed by specific machines. In addition to the innumerable paradigm changes and the ability to create increasingly versatile and intelligent networks, this feature allows to separate completely what is the radio access network – essentially, antennas and their equipment plus the users' terminals – from what is the so-called Core Network or 5GC in the nomenclature of the new standard. Among the consequences of this "decoupling" there is also the possibility of using a 5G access network that exploits the characteristics and benefits of the New-Generation Radio or NG radio interface but, coupled to the core network of the LTE standard, the Evolved Packet Core or EPC. 3GPP has defined various ways of implementing the 5G network that allow a gradual roll-out of next-generation services by a telephone operator, the two main ones of which are defined as Non-Stand-Alone and Stand-Alone.

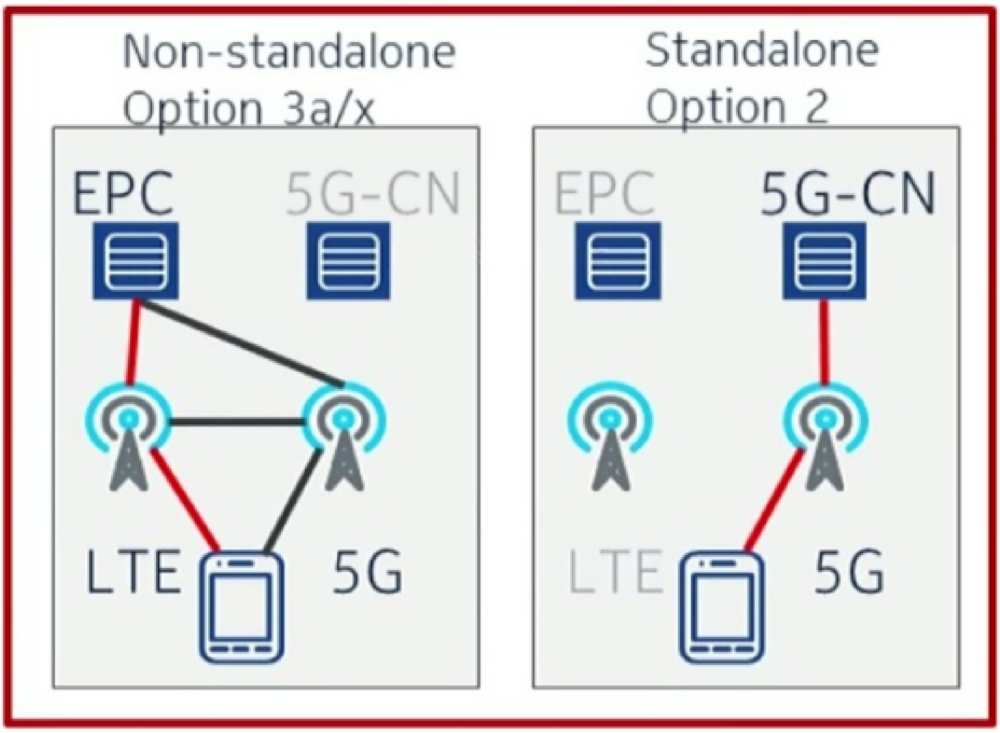


Fig. I.8: 5G Architecture Options

One of the things that will come as a result of NSA (Non-Stand-Alone) architecture on the left-hand side of Fig.I.8 will be the option for Dual Connectivity (DC). In fact, DC was first introduced in LTE as part of 3GPP.
A simple way to understand the difference between Dual Connectivity (DC) and other solutions like Carrier Aggregation (CA) is that, in CA, different carriers are served by the same backhaul (same eNB), while in DC they are served by different backhauls (different eNBs or eNB and gNB).
We will now describe the different connectivity options between NSA and SA.

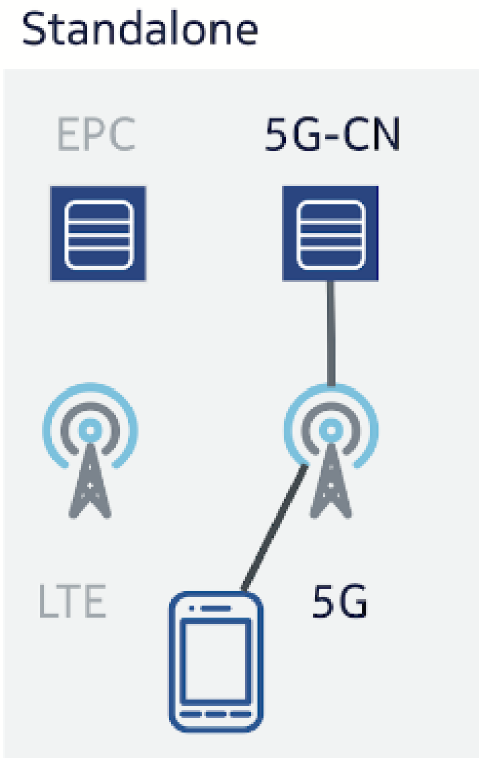


Fig. I.9: 5G SA Modality Option (2)

The Stand-Alone mode is the one that sees the NG-RAN access network convey traffic on the 5G Core Network and essentially represents the arrival point of the roll-out of the new networks.
Currently, the implementation phase of 5G services is ongoing. In Non-Stand-Alone, the new base stations (gNBs) capable of using the new NG radio interface are installed, alongside the traditional LTE or eNB (eNodeB) base stations, but always connected to the LTE EPC network.
More in detail, there are three scenarios regarding Non-Stand-Alone 5G, with defined options 3, 3a and 3x, in which the load distribution between 5G nodes and LTE nodes essentially varies, but in all three cases the smartphone of the user must necessarily support both 5G and 4G. The SBA architecture of the 5G network can guarantee:

- Only option for greenfield 5G operators.
- Full support for new 5G applications and services including:
    Enhanced Mobile Broadband (eMBB).
    Massive Machine-Type Communications (mMTC).
    Ultra-reliable Low Latency Communication (URLLC).

Multiple spectrum portions are needed to provide all the above cases and also to provide ubiquitous 5G coverage.

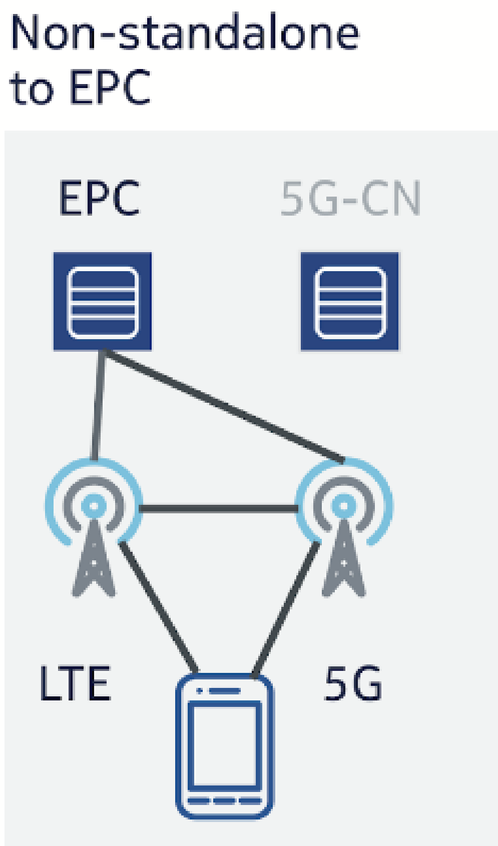


Fig. I.10: 5G NSA Modality Option (3a)

Option 3a provides that the new 5G base stations convey both data and control traffic through the LTE nodes, which are in fact connected to the core network.
This configuration is the easiest to implement but has the bulk defect of conveying a large amount of additional traffic on the LTE base stations.
For 3a, the master is always constituted by the LTE base station, which governs the radio access of the terminals, but the data traffic is directly conveyed by the 5G node to the LTE core network. The advantages are:

- - The traffic on the communication channel control between the two base stations is minimal.

- \- Leverages existing 4G deployments.
- \- Capable of creating 5G hotspots quickly.
- \- No overloading of EPC with 5G signalling.
- \- New 5G application and services creation possible.

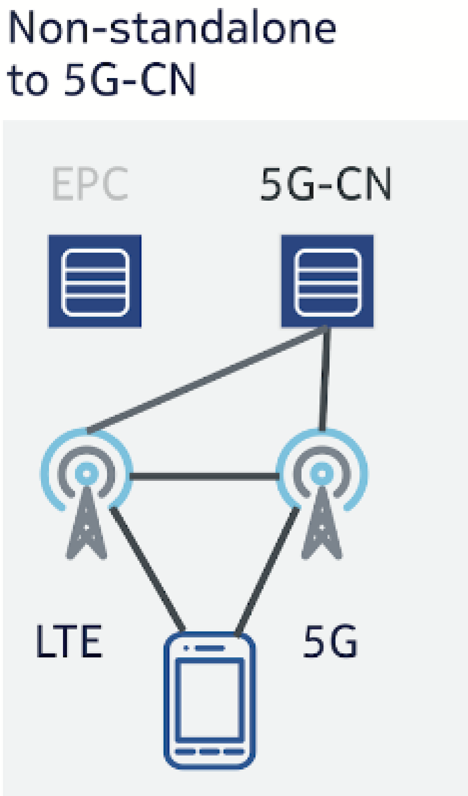


Fig. II.11: 5G NSA Modality Option

The last mode, the Option 3x, the most used one, is in fact a hybrid of the other two and the most versatile, as the 5G antenna can convey the traffic received by the user directly to the core network; in the case of a need to balance the load, it is also possible to use the communication channel between the two nodes.
It is clear that in this first phase of development of 5G networks, in the Non-Stand-Alone mode only the benefits of the new NG radio interface can be enjoyed by the first 5G smartphones that are already on the market, as most of the features provided by the new standard depend on the implementation of the Core Network, which incidentally is the one on which the commercial and political debate is focusing on whether or not to use products developed by Chinese companies.

Among the characteristics of 5G that this first phase will allow to exploit there will certainly be the greater transmission efficiency, therefore essentially greater speed in download and upload, and the reduction of latency, thanks to the use of new modulations, more advanced MIMO (Multi-Input-Multi-Output) techniques, beamforming and the use of the new frequency bands. From this point of view, the objectives of 5G are ambitions: speeds of at least 100 Mbits/s per user in densely populated areas and a maximum capacity of 20 Gbits/s in download, latencies below 1 ms, support for terminals that move up to 500 km/h, ability to manage millions of devices per (macro)-cell.
It must be said that the 5G standard is not yet completely closed: the 3GPP NR Release 15 standard has been finalized, which forms the basis of the specifications of the new generation radio access network; Release 16 has been already closed since the end of 2020 and includes specifications for the automotive and IoT world plus various optimizations. Release 17 functionally "frozen" in 2022, introduces support for frequency bands above 52 GHz and potentially up to 71 GHz.
As regards the CN, the Next Generation Core Network (NGCN) will replace the Evolved Packet Core (EPC).

2.4 Difference between 4G and 5G Network

In this section, we'll discuss how 4G and 5G architectures differ. In a 4G LTE network architecture, the LTE RAN and eNodeB are typically close together, often at the base or near the cell tower running on specialized hardware. L'EPC IN THE 4G LTE is often centralized and further away from the eNodeB [42].

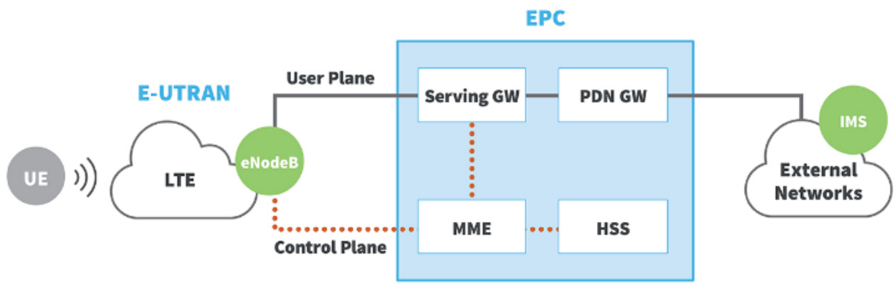


Fig. II.12 4G Architecture

This architecture makes high-speed, low-latency end-to-end communication challenging to impossible.
In the 4G network architecture, User Equipment (UE) like smartphones or

cellular devices, connects over the LTE Radio Access Network (E-UTRAN) to the Evolved Packet Core (EPC) and then further to External Networks, like the Internet. The Evolved NodeB (eNodeB) separates the user data traffic (user plane) from the network's management data traffic (control plane) and feeds both separately into the EPC.
It is important to note that 4G LTE (Long Term Evolution) has a long life ahead; it is a very successful and mature technology and is expected to be in wide use for at least another decade.

According to the 5G NR it is important to see the Fig I.1 in the Chapter I. The 5G NR takes advantage of the drawbacks of 4G to build a very efficient network technology.
Nevertheless, 5G core components running on common hardware is that networks now can be customized through network slicing. Network slicing allows you to have multiple logical "slices" of functionality optimized for specific use-cases, all operating on a single physical core within the 5G network infrastructure.
Thanks to the network slicing technology, a 5G network operator:

- - May offer one slice that is optimized for high bandwidth applications.
- - Another slice that is more optimized for low latency.
- - And a third that is optimized for a massive number of IoT devices.

Depending on this optimization, some of the 5G core functions may not be available at all. For example, if you are only servicing IoT devices, you would not need the voice function that is necessary for mobile phones. And because not every slice must have exactly the same capabilities, the available computing power is used more efficiently.
5G technology offers three principle advantages: Faster data transmission speed, up to multi-Gigabit/s speeds. Greater capacity, fueling a massive amount of IoT devices per square kilometer. Lower latency, down to single-digit milliseconds, which is critically important in applications such as connected vehicles in ITS applications and autonomous vehicles, where near instantaneous response is necessary.

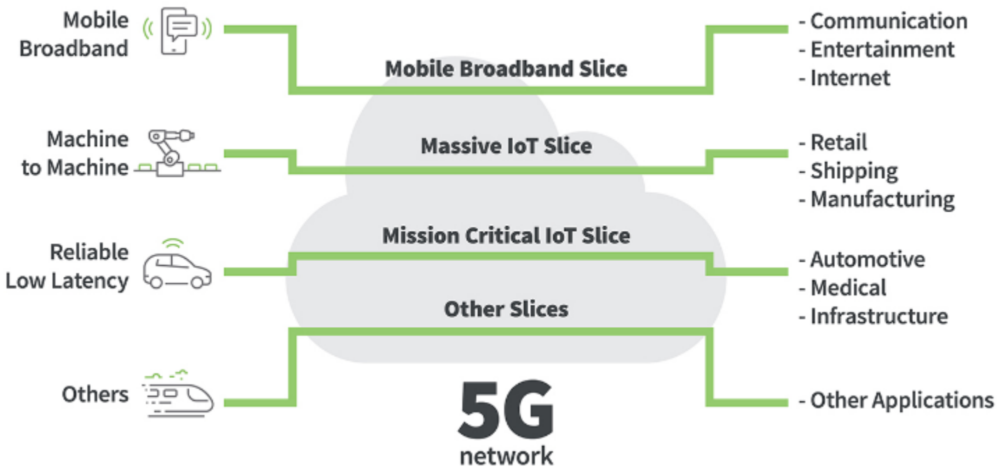


Fig. II.13 5G Network Slicing

Fig.II.13 show the 5G Nerwork Slicing that should be enabled by service providers to build virtual End-to-End networks tailored to application requirements.There are three frequency bands at the core of 5G networks: and these frequencies are shown in the Fig. II.14

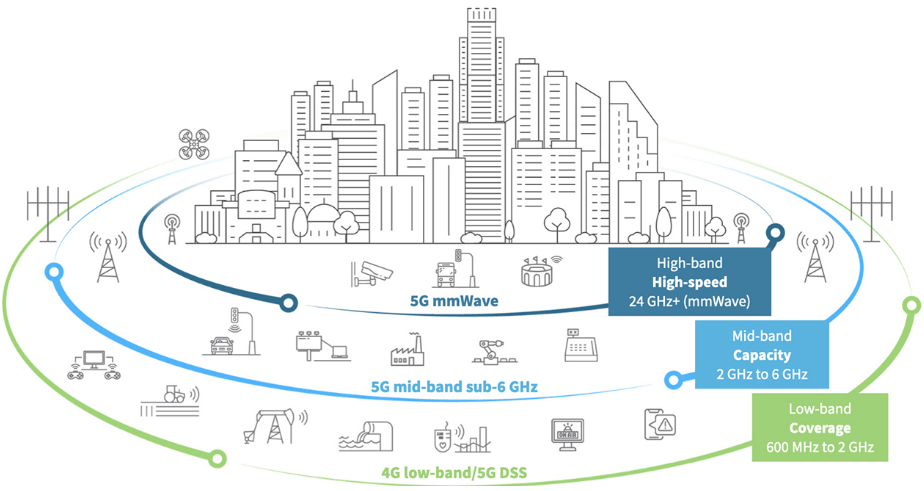


Fig. II.14 5G Design and Planning Considerations

1- 5G high-band (mmWave) delivers the highest frequencies of 5G. These range from 24 GHz to approximately 100 GHz. Because high frequencies cannot easily move through obstacles, high-band 5G is short range by nature. Moreover, mmWave coverage is limited and requires more cellular infrastructure.

2- 5G mid-band operates in the 2-6 GHz range and provides a capacity layer for urban and suburban areas. This frequency band has peak rates in the hundreds of Mbps.

3- 5G low-band operates below 2 GHz and provides a broad coverage. This band uses spectrum that is available and in use today for 4G LTE, essentially providing an LTE 5g architecture for 5G devices that are ready now. Performance of low-band 5G is therefore similar to 4G LTE, and supports use for 5G devices on the market today.

5G networks may implement networking slicing, which allows network administrators to partition parts of the network for specific use cases.[4]
Network slicing adds a new layer of performance management as each slice has specific requirements.
Test agents require complete configuration to provide end-to-end monitoring of individual network slices.
The reliability on the Unified Performance Management(UPM) solutions rather than individual Application Performance Management (APM) and Network Performance Monitoring(NPM) solutions will be necessary as the converged solution will provide IT administrators with a unique control point to monitor an enterprise's diverse network, slices, and applications.
Note that, both of these technologies, APM and NPM are designed to ensure that IT infrastructure runs smoothly and efficiently.
The 5G performance management uses a combination of application and network performance management tools called unified performance management. Since there are multiple connection types, network slices, and application types on a 5G network, a UPM is needed so administrators can use a single panel of dashboard to see and manage the whole network.
The 5G performance management must be more adaptable and flexible than previous forms because the ever-changing demands from the massive amount of data on the network needs to be sorted, filtered, and analyzed.[4]

2.5 5G Core Protocols NGAP (New Generation Application Protocol) over N2 Interface and Procedures

In the 5G SA, the NG interface is designed to interconnect gNB and 5G Core, and is similar to the S1 interface the connects eNB and EPC in 4G LTE. Considering Control and User Plane separation, the specification has defined the NG interface as NG-C and NG-U. NG-C allows signalling between a gNB and an AMF and NG-U allows the transfer of application data between a gNB and a UPF.

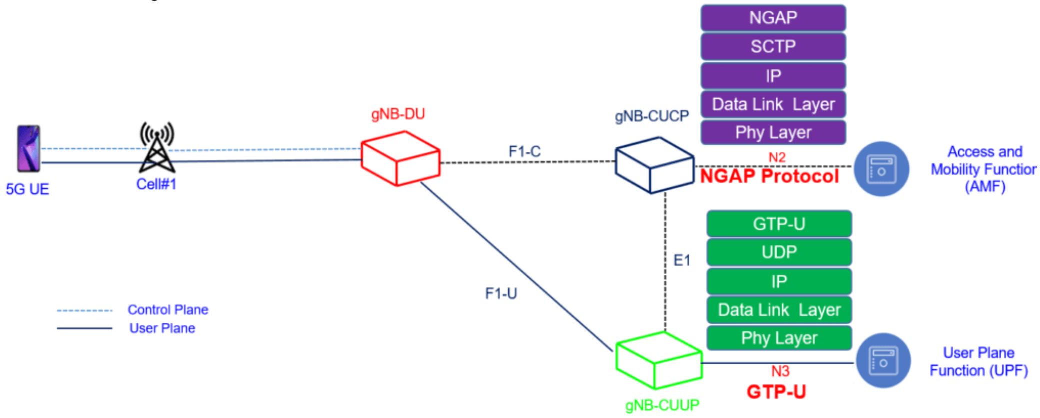


Fig. II.12 NGAP Protocol Pointer

The NGAP Protocol Pointer is derived from the interface name NG with the addition of Application Protocol.

- \- NGAP supports al mechanisms requires to manage the procedures between gNB and AMF.
- \- NGAP also supports transparent transport for NAS procedures that are executed between the UE and AMF.
- \- NGAP does not have any version negotiation.
- \- NGAP is applicable both to 3GPP access and non-3GPP accesses integrated with 5GC.
- \- NGAP relies on a reliable transport mechanism and is designed to run on top of SCTP.
- \- The key difference between NGAP and S1 AP is that S1 AP was designed only for 3GPP access (E-UTRAN) and not non-3GPP accesses.
- \- NGAP is applicable to any access and defined in 3GPP.
- \- N2 interface between gNB and AMF performs management functions.
- \- NGAP supports initial UE Context Setup functionality for establishment of an initial UE context at gNB.
- \- NGAP provides the UE capability information to the AMF during UE capability exchange.
- \- It also supports PDU Session Setup, modification, and release for user plane resources.
- \- Paging over NGAP, providing the functionality to page UE within 5GC.
- \- NGAP allow Trace of actives UEs.
- \- UE location reporting and positioning protocol support.
- \- NGAP supports warning message transmission for emergency services. There are two types of services over NGAP:

1- Non UE-asssociated Service: these NGAP services are related to N2 interface instance between the gNB and AMF and used to establish the NGAP signaling connection between gNB and MF.

2- UE-associated services: these NGAP services are related to a UE and involves signaling related to procedurees where a UE activity is involved. At Registration, PDU Session Establishment, Deregistration.

Types of NGAP Procedures:

i)- Request Response Procedure: in this types of procedures, the initiator gets a response from the receiver of the request.

ii)- No Response Procedures: these elementary procedures without do not expect a response from the receiver.

Some elementary procedures are specifically related to only Non-UE-associated services (e.g., NG Setup Request/Response), while others are related to only UE-associated services (e.g.,PDU Session Establishment).
Some elementary procedures may be using either No UE-associated or UE-associated signaling, depending on the scope and the context; For example, the error indication procedure that uses UE-associated signaling if the error was related to a reception of a UE-associated signaling message, while it uses Non-UE-associated signaling otherwise.

2.6 Network Transformation

Fig.II.13 shows the transformation of networks, moving from today's LTE-Advanced networks to future LTE-Advanced and eventually 5G networks.

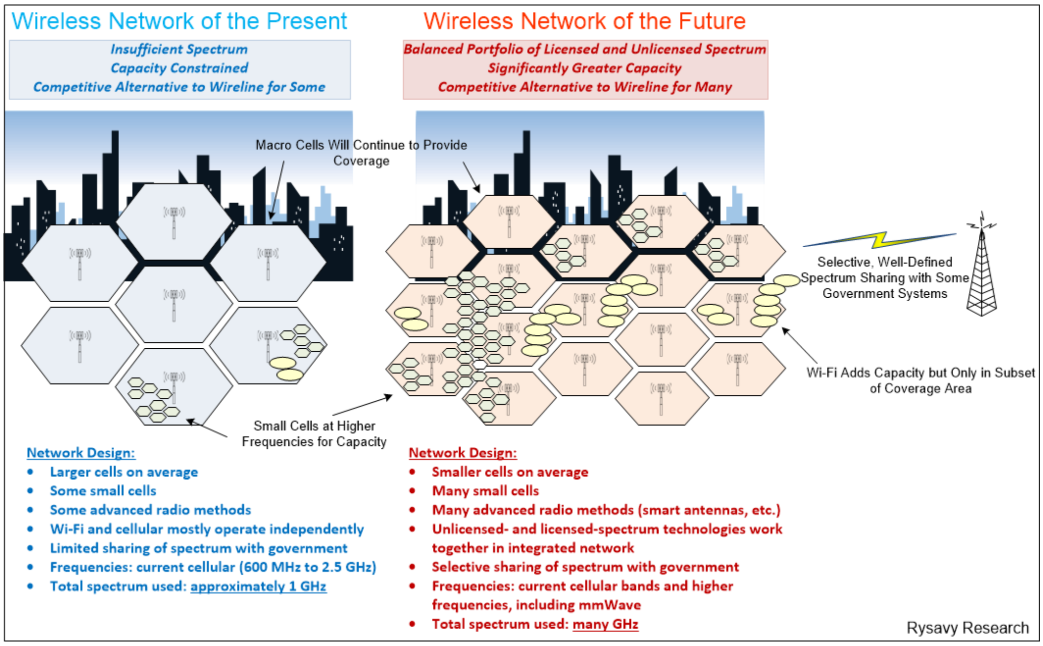


Fig. II.13 View of the Network Transformation [6]

The fundamental decision for 5G is how to best leverage existing technology investments in LTE while exploiting new spectrum and new technology capabilities. 5G design emphasizes ways to combine existing 4G LTE networks with capabilities provided by 5G. One approach likely to be used by many operators is to use LTE in existing frequency bands and the 5G NR in new bands, such as mmWave.

2.7 5G Benefits and Downside

- - Minimal lag when streaming videos and playing games
- - Safer cities with smart, interconnected vehicles
- - Near-instant access to most files online
- - Smaller devices that offload hardware requirements to remote servers
- - New products and applications that require ultrafast speeds
- - Reliable internet in remote areas

The downside to this is that these frequencies experience far more interference from things like trees and buildings, and sometimes even much smaller objects like a person. This means that strategically positioned small cell towers are required to push the network throughout a city.

2.8 Software Defined Networking and Networks

As SDN can mean many things to different people, it is worth having a definition to refer to and understand exactly what software defined networking and networks are.
SDN is a telecommunications network architecture that provides the promise of significant improvements in the network performance.
Using the SDN it's possible to make the network:

- -More Dynamic.
- -Manageable.
- -Cost-effective, and Adaptable.

The key behind software defined networking is that the SDN architectures decouple network control and forwarding functions. This enables the network control to become directly programmable. As a result the underlying network infrastructure can be abstracted from applications and network services.
SDN enables resources to be configured to meet the functions needed at any given time and to ensure that traffic is able to flow in the best manner possible at all times.

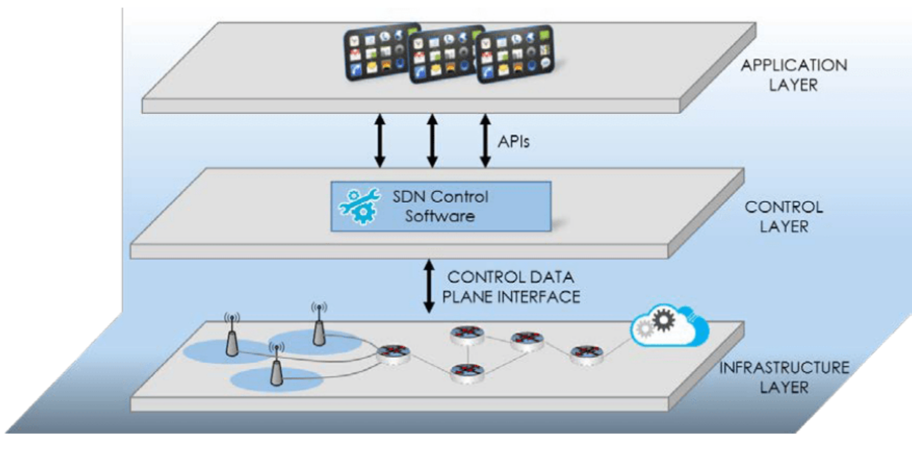


Fig II.14 Software Defined Networking architecture

In SDN Fig II.14, the control operations are centralized in a controller that dictates the network policies. Many controller platforms are open source such as Floodlight [7], OpenDayLight [8], and Beacon [9]. The management of the network can be achieved on different layers (i.e., application, control,

and data plane). For instance, service providers can allocate resources to customers via application layer, configure and modify network policies and logical entities on the control plane, and set up physical network elements on the data plane.
In particular, the challenges and issues that appear of paramount importance in the SDN environment are the following:

1-Scalability: This defines the ability of SDN to, more specifically in the control plane, handle and process an increasing workload. Scalability aims at enlarging the capacity of the SDN by implementing mechanisms such as devolving [10], clustering [11], and high processing [12] to cope with the growing load.
2-Reliability: The SDN is considered reliable when it notifies of delivery failures of the data in real time. In such network, there should be a specified minimum reliability for the delivery of critical data [7]
3-High availability (HA): this is an important aspect of today's services that should be available each time a customer requests a given service or resource. Availability is usually expressed as a percentage of uptime in a given year. Unavailability of services can generally occur owing to network outages or system crashes [13],[14]. Network providers generally deploy backup services to offer HA by implementing redundant server hardware, server Operating System and network components, and so on.
4-Elasticity: is the ability of SDN to dynamically adapt its capacity by scaling up or down the available resources [15], [16] in order to meet the variation and fluctuation of the workload. Generally, elasticity is often focused on the control plane and might be referred to as scalability.
5-Security: SDN security consists of protecting the information from theft or damage to the hardware and the software as well as from disruption of the services [17], [18]. Securing SDN encompasses physical security of the hardware, as well as preventing logical threats that may come from the network or data. SDN vulnerabilities are the entrance door to security attacks being intentional or accidental.
6-Performance: Performance refers to the amount of tasks achieved by SDN components compared with the time/resources (e.g., CPU and RAM) being used [19],[20]. There are many different ways to measure the performance of a network, as each network is different in nature and design. As far as SDN is concerned, the important measures are bandwidth, throughput, latency, and jitter.
7-Resilience: Resilience in SDN is the capability to ensure and maintain an acceptable level of service even in case of a service, network or node failure. When an SDN element is faulty, the network should provide a continuous

operational service with the same performance. In order to increase the resilience of SDN, potential challenges/risks have to be identified and addressed to protect the services [21].
8-Dependability: The dependability of SDN is strongly tied to availability and reliability terms. SDN dependability aims mainly at preventing faults and implementing fault tolerance mechanisms to guarantee service delivery even at a degraded level [22]. In addition to HA and reliability, integrity and maintainability are also two important dependability attributes.

2.9 Network Functions Virtualisation (NFV)

This section describes key NFV features that network operators in the NFV Industry Specification Group (ISG) of ETSI as well as the wider industry are addressing in order to realise 5G use cases. These features include Network Slicing, Cloud-native design principles, End-to-end Service Management, Edge Computing, Cloudification of the Radio Access Network (RAN), Multi-site/domain Services, NFV License Management, Security, Reliability, and Scalability.

NFV aims to transform the way that network operators architect and operate networks and network services by evolving standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage.
Network operators believe NFV is a key technology enabler for 5G. The evolved 5G network will be characterised by agile resilient converged fixed/mobile networks based on NFV and SDN technologies and capable of supporting network functions and applications encompassing different domains, including serving remote areas and inside buildings. This requires integration with existing network systems, efficiently extending the network and backhaul support and implementing end-to-end service management.The breadth of foreseen 5G use cases and environments implies high scalability, ultra-low latency, ability to support a massive number of concurrent sessions and ultra-high reliability and security, while each 5G use case has significantly different characteristics and combinations of these requirements (high scalability, ultra-low latency ultra-high reliability and security,).
To achieve these goals, Network Slicing, Edge Computing, Security, Reliability, and Scalability should be taken into account in the context of virtualisation. Moreover, given that the goal of NFV is to decouple network functions from hardware, and virtualised network functions are designed to run in a generic IT cloud environment, cloud-native design principles and cloud-friendly licensing models are critical matters.

By definition, NFV is an approach to telecommunications networking where the network entities that traditionally used dedicated hardware items are now replaced with computers on which software runs to provide the same functionality.
By running a network based around NFV it is easier to expand and modify the network, providing considerably more flexibility as well as possibility to standardise on much of the hardware as it consists of additional computing power. In this way both Capital Expenditeurs (CapEx) and Operational Expenditeurs (OpEx) can be considerably reduced.

2.10 5G and Virtualization

The major new technological development affecting 5G is network virtualization and the use of application programming interfaces (APIs). Network virtualization refers to implementing the functions of the communications infrastructure in software running on commercial 'off-the-shelf' computing equipment, essentially Ethernet switches linked. This follows the virtualization of data centers. More specifically, 5G will be implemented based on SDN and NFV, mobile edge computing (MEC) and in essence an architecture based on "cloud" computing, linking together a diverse set of resources for transport, routing, storage and processing, including (user) resources at the edge of the network. Moreover, it supports the development of new services through application programming interfaces [23]
Virtualization already started in the fixed network with AT&T being in the lead and Verizon a close follower. In 2013, AT&T described the motivation to move towards NFV as follows: AT&T s network is comprised of a large and increasing variety of proprietary hardware appliances. To launch a new network service often requires adding yet another variety, and finding the space and power to accommodate these boxes is becoming increasingly difficult. This difficulty is compounded by increasing costs of energy, capital investment, and rarity of skills necessary to design, integrate and operate increasingly complex hardware-based appliances. The compelling reasons for applying virtualization are: lower capital expenditures, benefiting from economies of scale in the IT industry; lower operating costs; faster deployment of new services; energy savings; and improved network efficiency.

The European Telecommunications Standards Institute (ETSI) has standardized the framework, including interfaces and reference architectures for virtualization. Fig.II.15 shows the ETSI framework, in which virtualized network functions (VNFs) are the nodes or applications by which operators build services. Other standards and industry groups involved include 3GPP, The Open Network Foundation, OpenStack, Open Daylight, and OPNFV. [24]

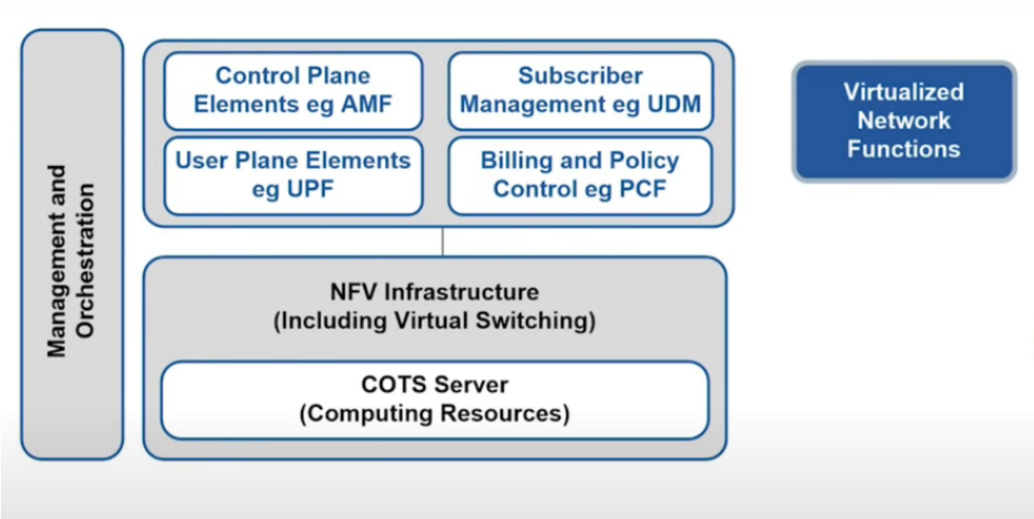


Fig II.15: ETSI network virtualization framework.

Virtualization and the decoupling between Radio Access Technologies (RATs) and the Core Network (CN) functionalities support the principle of network slicing. In that way, the various 5G use cases with different requirements on the radio interface and in terms of data processing in the core network can be combined and supported by one integrated mobile communications network.

2.11 Network Slicing Architecture

From a network operator viewpoint, Network Slicing is a service-oriented network construct providing network-on-demand to concurrent applications. In other words, Network Slicing can be seen as an implementation of the "Network as a Service" paradigm, where a common network is able to provide and expose concurrent, partitioned and self-contained “slices” to support different services in an efficient way and provide the required Quality of Service (QoS). From a standards definition view point, domain-specific standards bodies and open source communities are using “slicing” in contextually different ways.
Not only will 5G networks include a new radio, but thanks to virtualization, these networks will be able to present multiple faces for different use cases using the concept of network slicing. This architecture allows an operator to provide multiple services with different performance characteristics. Each

network slice operates as an independent, virtualized version of the network. For an application, the network slice is the only network it sees. The other slices, to which the customer is not subscribed, are invisible and inaccessible. The advantage of this architecture is that the operator can create slices that are fine-tuned for specific use cases. One slice could target autonomous vehicles, another enhanced mobile broadband, another low-throughput IoT sensors, and so on.
Fig.II.16 shows the network slicing architecture, with devices having access to only the slice or slices for which they have subscriptions. Each slice has radio resources allocated, with specific QoS characteristics. Within the core network, virtualized core network functions support each slice and provide connections to external networks [25]

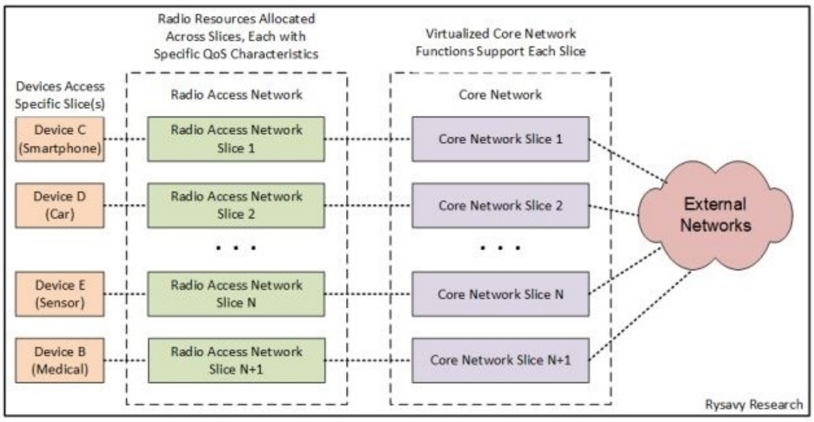


Fig.II.16: Slicing Architecture.

Using SDN and NFV it will be possible to configure the type of network that an individual user will require for the user application. In this way, the same hardware using different software can provide a low latency level for one user, while providing voice communications for another using different software, other users may want other types of network performance and each one can have a slice of the network with the performance needed.

The performance required for the 5G NextGen network has been defined by the NGMN (Next Generation Mobile Network Alliance). The Next Generation Mobile Networks Alliance is a mobile telecommunications association of mobile operators, vendors, manufacturers and research institutes. By using the experience of all parties, it is able to develop the strategies for the next generation mobile networks, like that for 5G.
As conclusion for this subsection, it is important to understand that Network Slicing allows services providers to create multiple logical network over the

same physical infrastructure.
By doing this, the service provider has more flexibility in term of how to provides specific service environments to customers.

2.12 5G Motivation and Requirements

The demand for better mobile broadband experiences is continuously increasing. A huge number of devices require connection to the Internet such as mobile phones, computers, tablets, smart watches, etc. Users of these kind of devices always demand higher data rates. Moreover, several industries are going through a digital transformation. There are emerging concepts for smart vehicles, human machine interaction, sensor network, critical control of remote devices, etc. Communication procedures addressed for these new services are different from the human use case.
Thus, to assure a certain quality of the service, appropriate requirements in terms of reliability, latency, throughput, scalability and energy-efficiency should be met. The current Radio Access Technologies (RATs) are not able to deal with all these requirements. Therefore, 3GPP defined the New Radio (NR) access technology (also known as the 5Th Generation or 5G), a new air interface which is supposed to handle all the capacity and performance requirements of the emerging services.
As already mentioned previously, and as illustrated in Fig. II.17, 5G should be able to deal with several distinct service types, such as massive Machine Type Communication (mMTC), enhanced Mobile Broadband (eMBB) or Ultra-Reliable Low Latency Communications (URLLC). Since this implies a very heterogeneous network, it suggests the need of a high flexibility, so the network can adapt to the different requirements depending on the type of service being requested. The 5G NR frequencies range from low bands below 6GHz to higher bands above 30GHz (millimetre Wave - mmW).

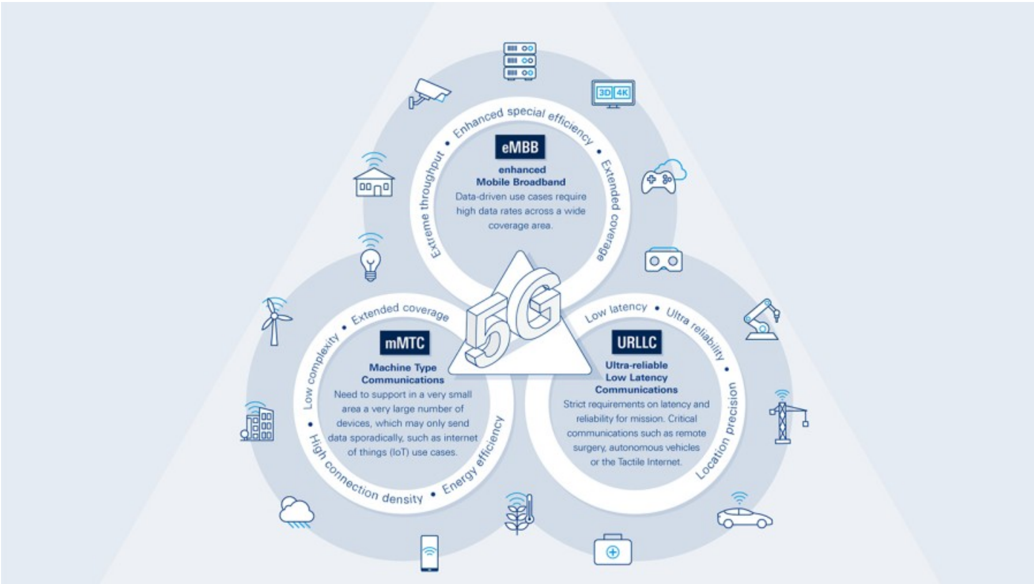


Fig.II.17: 5G Service Types and Requirement

The scope of mMTC services is to provide efficient connectivity for hundreds of devices per square kilometre. These devices usually send short packets and have low delay restrictions. The requirements, therefore, are low cost, low battery consumption and high connection density.Applications of this kind of service include e-Health, transport and logistics, smart agriculture, smart energy network, etc.

eMBB aims to improve consumer experience when accessing multimedia content, services and data and focuses mainly on services with high bandwidth requirements.

URLLC is intended for mission-critical links, which means that it has strict end-to-end latency and high reliability requirements. Some of its applications are vehicle-to-everything communication, drone delivery and smart manufacturing. Further explanation about these services and the requirements for the scenarios where they are used can be found in [6, 27, 28].

2.13 MIMO and Massive MIMO Technology

Multiple Input Multiple Output (MIMO) technology is an integral part of 3GPP E-UTRA long term evolution (LTE). As part of MIMO, beamforming is also used in LTE. The basics of beamforming and the eight MIMO transmission modes are explained in LTE Release 9.
Modern communications networks use MIMO technology to achieve high data

rates. As a special MIMO technique, beamforming also permits targeted illumination of specific areas, making it possible to improve transmission to users at the far reaches of cell coverage. Like other communications standards such as WLAN and WiMAX, LTE also defines beamforming. Beamforming is particularly important for the time division duplexing (TDD) mode in LTE.

MIMO systems are used to improve the robustness of data transmission or to increase data rates.Typically, a MIMO system consists of m transmit antennas and n receive antennas Fig.II.18-(a).

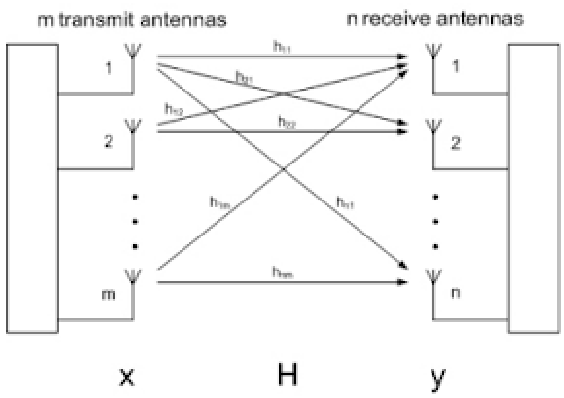


Fig.II.18-(a): MIMO system with m TX and n RX antennas.

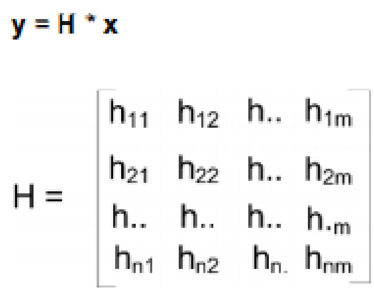


Fig.II.18-(b):Transmission matrix H

Simply stated, the receiver receives the signal y that results when the input signal vector x is multiplied by the transmission matrix H. y = H * x Fig.II.18-(b)

The transmission matrix H contains the channel impulse responses hnm, which reference the channel between the transmit antenna m and the receive antenna n. Many MIMO algorithms are based on the analysis of transmission matrix H characteristics. The rank (of the channel matrix) defines the number of linearly independent rows or columns in H. It indicates how many independent data streams (layers) can be transmitted simultaneously.

MIMO increasing the robustness of data transmission, transmit diversity when the same data is transmitted redundantly over more than one transmit antenna TX diversity. This increases the signal-to-noise ratio. Spacetime codes are used to generate a redundant signal. Alamouti developed the first codes for two antennas [29]. Today, different codes are available for more than two antennas.

MIMO increasing the data rate with spatial multiplexing. Data is divided into separate streams, which are then transmitted simultaneously over the same air interface resources. The transmission includes special sections (also called pilots or reference signals) that are also known to the receiver. The receiver can perform a channel estimation for each transmit antenna's signal. In the closed-loop method, the receiver reports the channel status to the transmitter via a special feedback channel. This enables fast reactions to changing channel conditions, e.g., adaptation of the number of multiplexed streams. When the data rate is to be increased for a single user equipment (UE), this is called Single User MIMO (SU-MIMO). When the individual streams are assigned to various users, this is called Multi User MIMO (MU-MIMO or MASSIVE MIMO is more used in 5G).

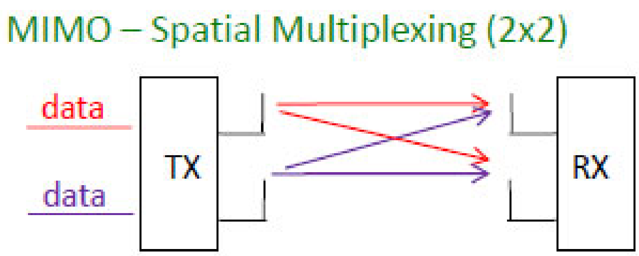


Fig II.19: Illustration of 2x2 MIMO

Fig.II.19 shows an example simplified illustration of 2x2 MIMO (Spatial Multiplexing). Two different data streams are transmitted on two TX antennas and received by two RX antennas, using the same frequency and time, separated only by the use of different reference signals.
One or two transport blocks are transmitted per Transmission Time Interval (TTI). A major change in LTE-Advanced is the introduction of 8x8 MIMO in the Downlink (DL) and 4x4 in the Uplink (UL).
MIMO can be used when the S/N (Signal to Noise ratio) is high, i.e. high quality radio channel. For situations with low SNR, it is better to use other types of multi-antenna techniques to instead improve the SRN, e.g., by means of TX-diversity.

At the physical level, LTE systems can optionally employ multiple transceivers both in correspondence between the radio base station and the user terminal, to improve the robustness of the connection and increase the transmitted data capacity.The techniques used are MIMO and Maximal Ratio Combining (MRC).

The MRC technique is used to improve link reliability under critical propagation conditions when the amplitude of the signal is low and there are multiple paths.
We note that a conventional system equipped with a receiver with multiple antennas is not enough to be able to support MRC / MIMO techniques. In fact, the peculiar characteristic of these systems is that of requiring, in addition to multiple antennas, also multiple transceivers.
Via two or more antenna / transceiver systems, spatially separated between them, and, therefore, characterized by different impulsive responses, the processor performs the equalization of the channel separately on the received signals and then combine them into a single composite signal. Operating in this way, while the received signals are combined coherently, the thermal noise introduced by each transceiver is not correlated determining, in the case of a two-channel MRC receiver, an overall increase SNR of 3dB. To this positive aspect it must obviously be added that relating to the spatial separation of two receivers, which strongly reduces the effects related to selective fading due to multiple paths, improving the overall quality of the received signal.
To obtain this result, the receiver must calculate the impulse response of the channel that characterizes each transmitting antenna. In LTE systems, this result is achieved by transmitting, suitable reference signals from each of the aforesaid antennas and in a sequential way (not overlapping).
Once impulse responses are known, the data can be transmitted also simultaneously on both antennas. The linear combination of the two data streams at two receiving antennas gives rise to a set of two equations with two unknowns that can be solved to derive the two original data streams.

2.13.1 Massive MIMO Technology

Massive MIMO technology is all set to be a core component of the superfast 5G networks that have started rolling out by the end of 2019. While it involves multiple technologies, MIMO can essentially be boiled down to this single principle: a wireless network that allows the transmission and reception of more than one data signal simultaneously over the same radio channel.Standard MIMO networks tend to use two or four antennas. Massive MIMO, on the other hand, is a MIMO system with an especially high number of antennas. There is no set figure for what constitutes a Massive

MIMO set-up, but the description tends to be applied to systems with tens or even hundreds of antennas. For example, Huawei, ZTE, and Facebook have demonstrated Massive MIMO systems with as many as 96 to 128 antennas. The advantages of a MIMO network over a regular one is that it can multiply the capacity of a wireless connection without requiring more spectrum. Reports point to considerable capacity improvements, and could potentially yield as much as a 50-fold increase in the future.

The more antennas the transmitter/receiver is equipped with, the more the possible signal paths and the better the performance in terms of data rate and link reliability.

A Massive MIMO network will also be more responsive to devices transmitting in higher frequency bands, which will improve coverage. In particular, this will have considerable benefits for obtaining a strong signal indoors (though 5G's higher frequencies will have their own issues in this regard).

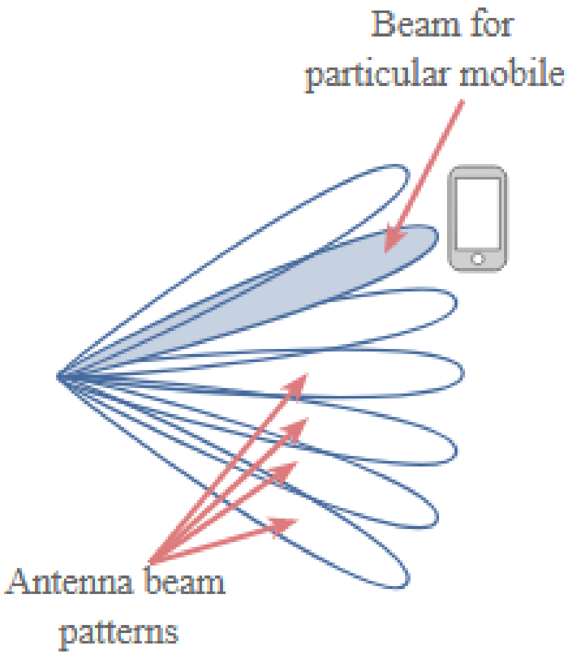


Fig II.20: Concept of antenna beam-forming used with 5G NR.

Beam-forming the technique to direct signals to the different devices.
The greater number of antennas in a Massive MIMO network Fig.II.20 will also make it far more resistant to interference and intentional jamming than current systems that only utilise a handful of antennas.

It should be noted, too, that Massive MIMO networks will utilise beamforming technology, enabling the targeted use of spectrum. Current mobile networks are rather trivial in the way they apportion a single pool of spectrum between all users in the vicinity, which results in a performance bottleneck in densely populated area. With Massive MIMO and beamforming such a process is handled far more smartly and efficiently, so data speeds and latency will be far more uniform across the network.

3 CHAPTER III. srsLTE and UERANSIM

srsLTE and UERANSIM are two open-source program system used to simulate, evaluate and experiment the network traffic between the UE, eNodeB and EPC or UE and gNodeB.
They have some differences that will be mentioned in this chapter. After a brief introduction of srsLTE, its components, features and implementation, we will focus on UERANSIM, since it is the newest open source program system to simulate the 5GC network between UE and gNodeB.

3.1 srsLTE(software radio system Long Term Evolution)

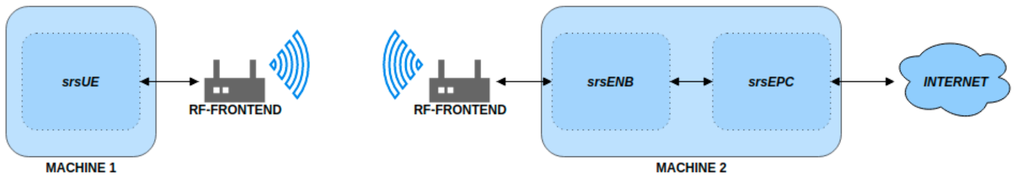


Fig.III.1 Basic srsLTE System Architecture

srsLTE is an open-source LTE software suite. It is developed and maintained by software radio systems, a private limited Ireland-based company [31].
The motivation behind the project was to provide a flexible platform for product development for LTE systems [30]. However, in recent days the implementation has emerged as an alternative option to provide LTE commercial products using Software Defined Radio (SDR) technology [32]. srsLTE offers an open-source implementation of all LTE components, i.e., UE, eNB and EPC, covering the complete protocol stack [30], [31]. The main components of the project are: srsUE, srseNB and srsEPC. The transceiver parts (UE and eNB) are realized using SDR technology; the EPC components are fully implemented on a PC. The specific features of each component are mentioned in subsequent sections. However, there are some common features which are listed below [10]:

- \- Open-source implementation is LTE Release 10 complaint
- \- LTE Bandwidths covered: 1.4MHz, 3MHz, 5MHz, 10MHz, 15MHz and 20MHz
- \- Transmission modes supported:

- single antenna mode
- transmit diversity mode
- Cyclic Delay Diversity (CCD) mode
- closed-loop spatial multiplexing

- \- Frequency-based zero forcing (ZF) equalizer
- \- MMSE (Minimum Mean Square Error) equalizer
- \- Evolved multimedia broadcast and multicast service (eMBMS).

The open-source LTE compliant Linux-based application includes the functionalities of LTE eNodeB, EPC and UE. The software application was initially designed according to release 8 of the LTE standard [30]. However, the current open-source version of the application is LTE release 15 complaint, supporting both Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD) modes [31]. The application has been tested with different SDR platforms like USRP, bladeRF and limeSDR. The implementation is highly modular and can be modified to specific needs. Some functions from the openLTE project have been used in this thesis [31]. For commercial purposes the srs sells the commercial licenses and also the proprietary products based on srsLTE code [30]. In srsLTE all components srsUE, srsEPC and srsENB have detailed configuration files; we will not discuss every single component, as the purpose of this thesis is not the description and simulation of the srsLTE, which is related to 4G technology, but rather to discuss, describe and use UERANSIM, a recent simulator for 5G UE and gNodeB. Notice that, according to the Fig III.1, for the srsLTE simulator srsENB, srsEPC and UE have to be installed in two separate machines (srsENB and srsEPC on the same machine) and srsUE in another one.

3.2 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 base station in basic terms. The project can be used for testing the 5G Core Network and studying the 5G System.

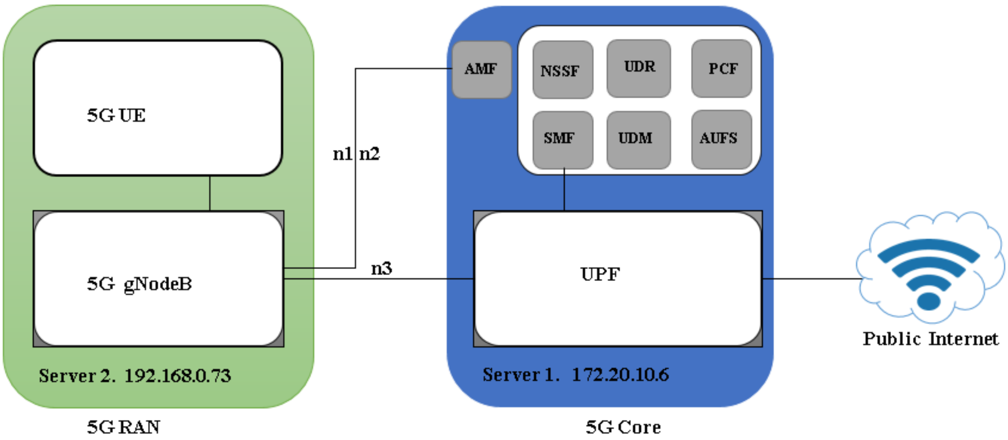


Fig.III.2 5G Core network with gNB/UE simulation with UERANSIM

The purpose of this thesis has been to install the UERANSIM software system and to use it to simulate the network communication between UE and new generation base transceiver station (gNodeB).
The installation, description and simulation procedure will be described in chapter IV.

4 CHAPTER IV. SIMULATIONS

In this chapter we are going to view how the simulation environment looks like, according to the free5GC. At the same time we will show some results of the two simulators.

4.1 srsLTE/srsRAN Simulation Results

Before to go forward in the free5GC mobile network simulator, we have to take a few time to describe with some results, what happen when the previous open-source simulator (srsLTE/srsRAN) was used.

4.2 srsEPC Model

The Fig. IV.1 shows how the epc was initialized. The EPC configurations are stored in two main files epc.conf containing the general configurations for the MME, HSS and GW parameters.

```
Last login: Sun Apr 23 08:12:18 2023 from 192.168.102.238
matilda@srslte-epc:~$ cd ./srsLTE/build
matilda@srslte-epc:~/srsLTE/build$ sudo ./srsepc/src/srsepc
[sudo] password for matilda:

Built in Release mode using commit f02bfe2cf on branch master.


---  Software Radio Systems EPC  ---

Reading configuration file /root/.config/srslte/epc.conf...
HSS Initialized.
MME S11 Initialized
MME GTP-C Initialized
MME Initialized. MCC: 0xf001, MNC: 0xff01
SPGW GTP-U Initialized.
SPGW S11 Initialized.
SP-GW Initialized.
```

Fig. IV.1 5G EPC Initialized Architecture

To inizialize the EPC, it is possibile after moving on the directories */srsLTE/build* and execute this command: sudo *./srsepc/src/srsepc* using the default configuration, this creates a virtual network interface named "srs_ spgw_ sgi" on machine 1 with IP 192.168.0.56. All connected UEs will be assigned an IP in this network.

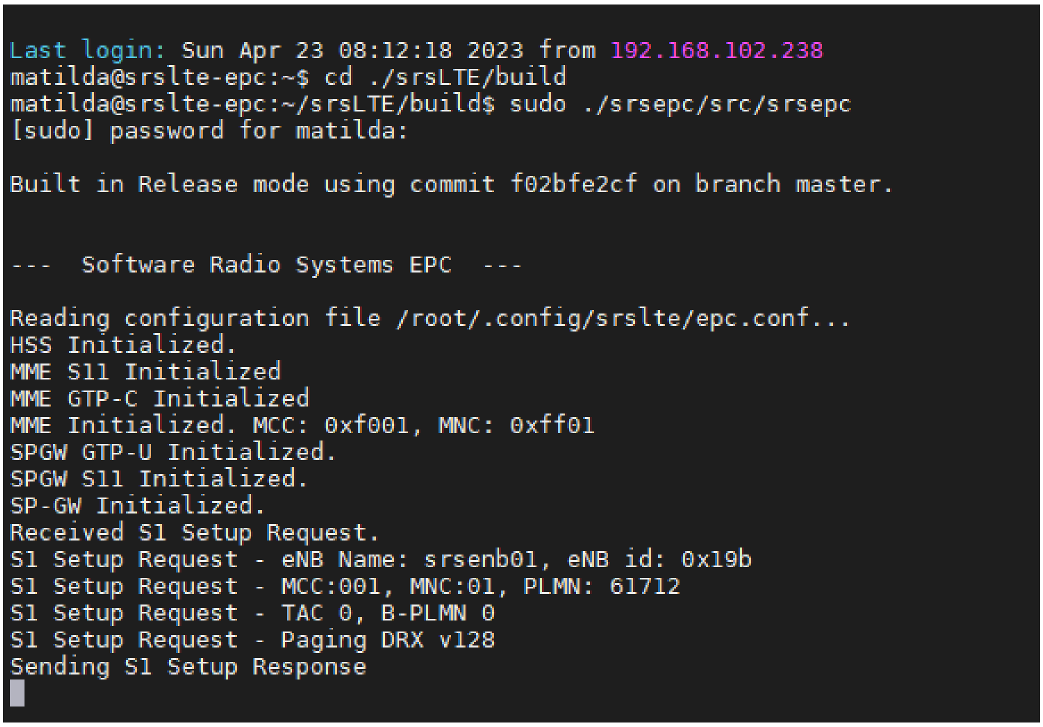
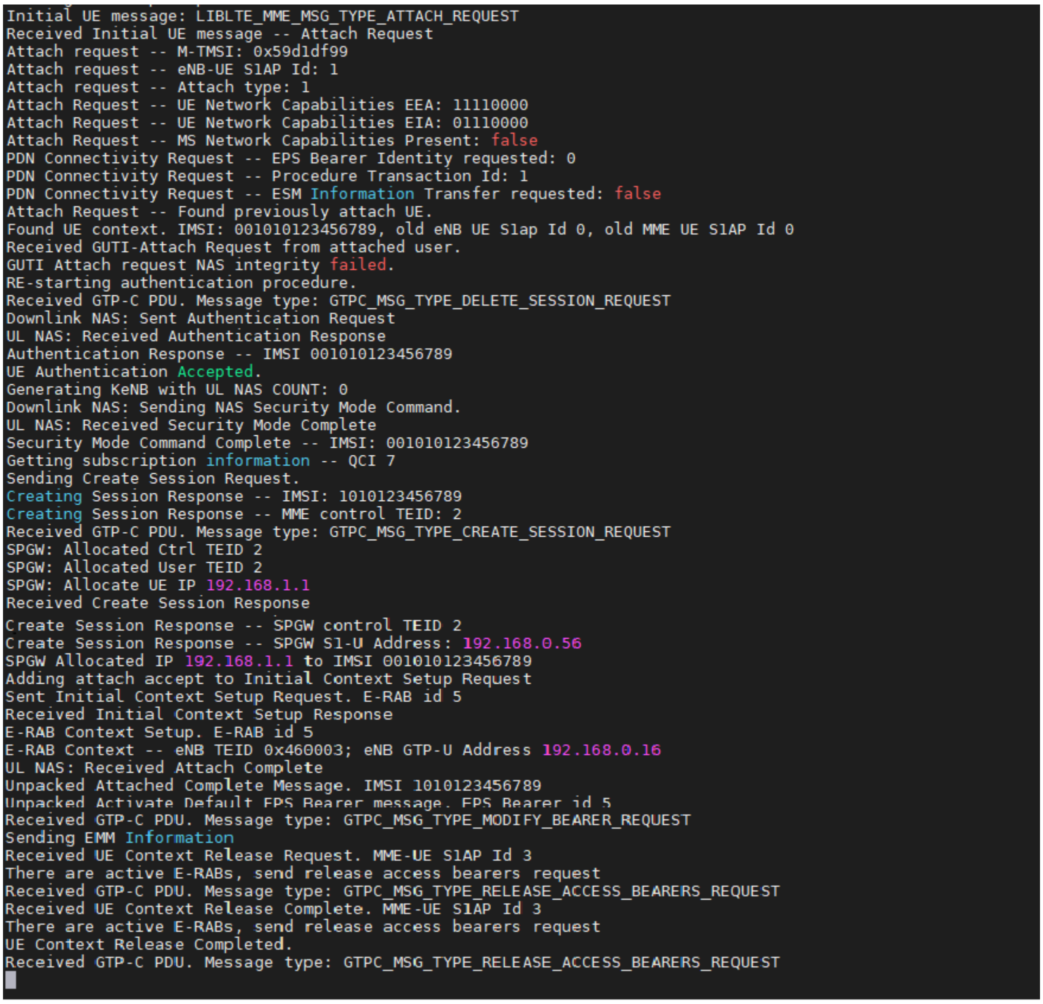


Fig.IV.2 Confirmation of the eNB Connected

The fig. IV.2 above provides a complete detail about the Mobile Country Codes, Mobile Network Codes and unique PLMN (Public Land Mobile Network) after the eNodeB was executed using this command:

"sudo ./srsenb/src/srsenb –rf.device_ name=zmq –rf.device_ args="fail_ on_ disconnect=true,tx_ port=tcp://*:2100,rx_ port=tcp://localhost:2101,id=enb, base_ srate=23.04e6 "

always with sudo privilege. When we see that output, we can be sure that, eNB has successfully connected to the core. It also provides information related eNB id number.



```
Initial UE message: LIBLTE_MME_MSG_TYPE_ATTACH_REQUEST
Received Initial UE message -- Attach Request
Attach request -- M-TMSI: 0x59d1df99
Attach request -- eNB-UE S1AP Id: 1
Attach request -- Attach type: 1
Attach Request -- UE Network Capabilities EEA: 11110000
Attach Request -- UE Network Capabilities EIA: 01110000
Attach Request -- MS Network Capabilities Present: false
PDN Connectivity Request -- EPS Bearer Identity requested: 0
PDN Connectivity Request -- Procedure Transaction Id: 1
PDN Connectivity Request -- ESM Information Transfer requested: false
Attach Request -- Found previously attach UE.
Found UE context. IMSI: 001010123456789, old eNB UE S1ap Id 0, old MME UE S1AP Id 0
Received GUTI-Attach Request from attached user.
GUTI Attach request NAS integrity failed.
RE-starting authentication procedure.
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_DELETE_SESSION_REQUEST
Downlink NAS: Sent Authentication Request
UL NAS: Received Authentication Response
Authentication Response -- IMSI 001010123456789
UE Authentication Accepted.
Generating KeNB with UL NAS COUNT: 0
Downlink NAS: Sending NAS Security Mode Command.
UL NAS: Received Security Mode Complete
Security Mode Command Complete -- IMSI: 001010123456789
Getting subscription information -- QCI 7
Sending Create Session Request.
Creating Session Response -- IMSI: 1010123456789
Creating Session Response -- MME control TEID: 2
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_CREATE_SESSION_REQUEST
SPGW: Allocated Ctrl TEID 2
SPGW: Allocated User TEID 2
SPGW: Allocate UE IP 192.168.1.1
Received Create Session Response
Create Session Response -- SPGW control TEID 2
Create Session Response -- SPGW S1-U Address: 192.168.0.56
SPGW Allocated IP 192.168.1.1 to IMSI 001010123456789
Adding attach accept to Initial Context Setup Request
Sent Initial Context Setup Request. E-RAB id 5
Received Initial Context Setup Response
E-RAB Context Setup. E-RAB id 5
E-RAB Context -- eNB TEID 0x460003; eNB GTP-U Address 192.168.0.16
UL NAS: Received Attach Complete
Unpacked Attached Complete Message. IMSI 1010123456789
Unpacked Activate Default EPS Bearer message. EPS Bearer id 5
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_MODIFY_BEARER_REQUEST
Sending EMM Information
Received UE Context Release Request. MME-UE S1AP Id 3
There are active E-RABs, send release access bearers request
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_RELEASE_ACCESS_BEARERS_REQUEST
Received UE Context Release Complete. MME-UE S1AP Id 3
There are active E-RABs, send release access bearers request
UE Context Release Completed.
Received GTP-C PDU. Message type: GTPC_MSG_TYPE_RELEASE_ACCESS_BEARERS_REQUEST
```

Fig. IV.3 EPC Successful Attach

The Fig.IV.3 gives that readout when the EPC is successeful attach.

4.3 srsENB Model

Once the epc is running, execute "srsenb with no sudo but in the main directory /home/matilda/.config/srslte/enb.conf " command on the other machine but in another Tabulation to start the srseNB. The eNB will start and will connect to the srsepc. The expected srsenb console output is shown in Fig. IV.4

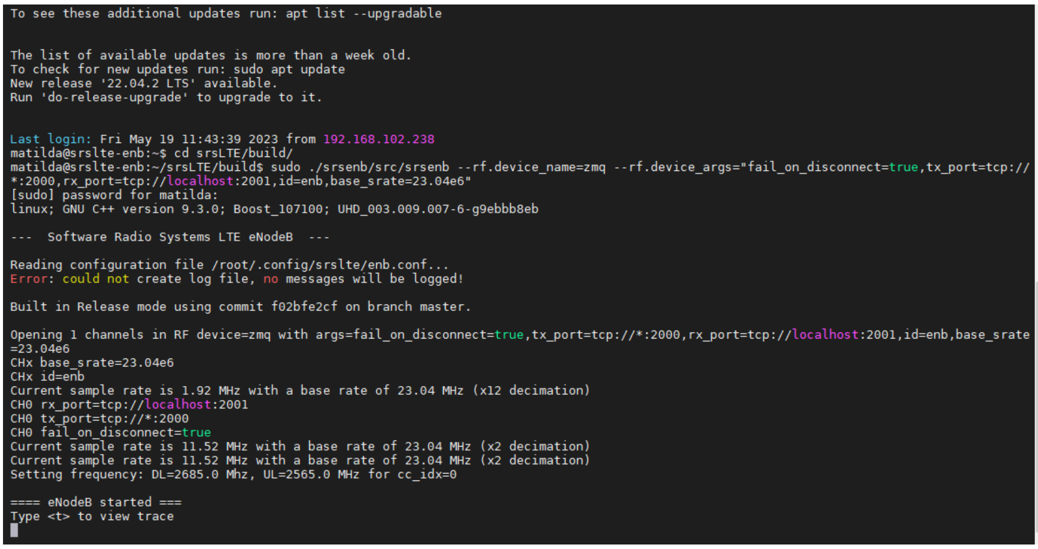


Fig. IV.4 eNB Initialized

The srseNB is the LTE base station, the current open source code include the FDD configuration,Round Robin MAC scheduler, encryption, Channel Quality Indicator (CQI) feedback support and standard S1AP and GTP-U interfaces to the core network. The srseNB can support maximum of 150 Mbps DL in 20 MHz MIMO TM3/TM4 with commercial UEs [33].

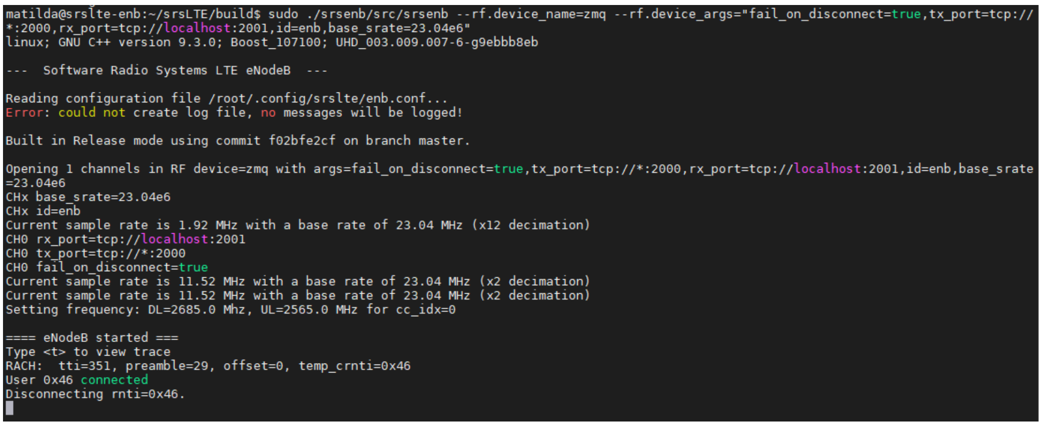
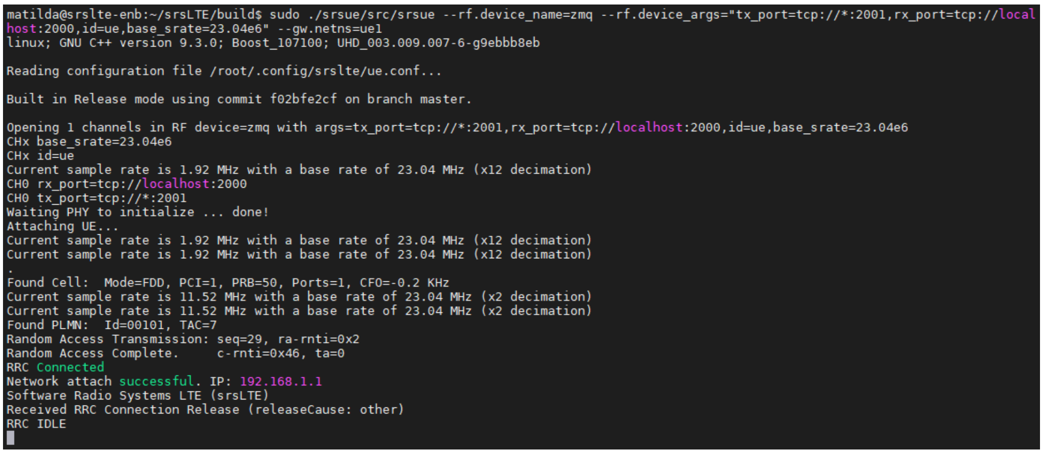


Fig. IV.5 5G srsENB Console with UE Connected

As soon as srsUE successfully attaches to a network a virtual tunnel interface "tun srsue" is created to send and receive data traffic.The next figures shows traffic on our "tun srsue" during the the two modalities (Downlink and

Uplink) testing.

4.4 srsUE Model



```
matilda@srslte-enb:~/srsLTE/build$ sudo ./srsue/src/srsue --rf.device_name=zmq --rf.device_args="tx_port=tcp://*:2001,rx_port=tcp://local
host:2000,id=ue,base_srate=23.04e6" --gw.netns=ue1
linux; GNU C++ version 9.3.0; Boost_107100; UHD_003.009.007-6-g9ebbb8eb

Reading configuration file /root/.config/srslte/ue.conf...

Built in Release mode using commit f02bfe2cf on branch master.

Opening 1 channels in RF device=zmq with args=tx_port=tcp://*:2001,rx_port=tcp://localhost:2000,id=ue,base_srate=23.04e6
CHx base_srate=23.04e6
CHx id=ue
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
CH0 rx_port=tcp://localhost:2000
CH0 tx_port=tcp://*:2001
Waiting PHY to initialize ... done!
Attaching UE...
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
Current sample rate is 1.92 MHz with a base rate of 23.04 MHz (x12 decimation)
.
Found Cell:  Mode=FDD, PCI=1, PRB=50, Ports=1, CFO=-0.2 KHz
Current sample rate is 11.52 MHz with a base rate of 23.04 MHz (x2 decimation)
Current sample rate is 11.52 MHz with a base rate of 23.04 MHz (x2 decimation)
Found PLMN:  Id=00101, TAC=7
Random Access Transmission: seq=29, ra-rnti=0x2
Random Access Complete.     c-rnti=0x46, ta=0
RRC Connected
Network attach successful. IP: 192.168.1.1
Software Radio Systems LTE (srsLTE)
Received RRC Connection Release (releaseCause: other)
RRC IDLE
```

Fig. IV.6 srsENB UE Attach

Using the default configuration, this creates a virtual network interface named "tun_ srsue" on machine 2 with an IP in the network 192.168.0.16. Assuming the UE has been assigned IP 192.168.0.16 (because the UE is run on the same Virtual Machine as eNodeB), you may now exchange IP traffic with system 1 over the LTE link.

The network is now ready for handover to be initiated and tested. To keep the UE from entering idle, you should send traffic between the UE and the eNB. this result is obtained after moving on the $/srsLTE/build$ directories and execute this command:

sudo ./srsue/src/srsue –rf.device_ name=zmq –rf.device_ args="tx_ port= tcp://*:2101,rx_ port=tcp://localhost:2100,id=ue,base_ srate=23.04e6" –gw.netns=ue1

using sudo privilege.

4.5 Overview of free5GC Mobile Network Simulator

The following minimum configuration was set as a condition:

- -The pair of gNodeB and UPF exists in the same location.

• -The UE connected to gNodeB connects to DN managed by UPF in the same location.

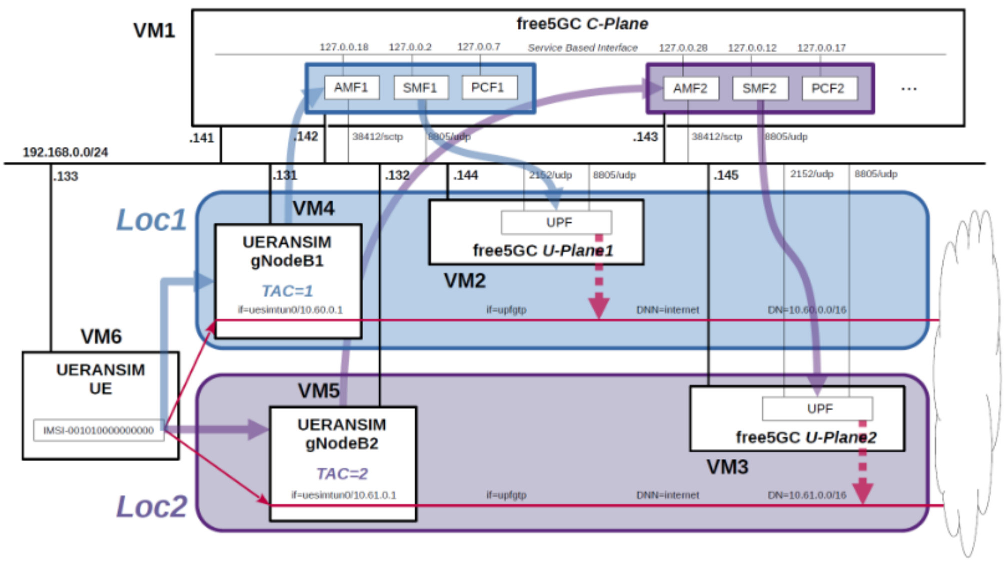


Fig. IV.7 Simulation Environment

In Fig. IV.1, the Tracking Area Code (TAC) is matched to connect gNodeB and AMF, and AMF searches for SMF using the preferred target NF location as one of the parameters. Also, AMF and SMF search for PCF using preferred target NF location as one of the parameters.

Virtual Machine Number	Software and Role	IP Address
VM1	Free5gc C-plane	192.168.0.141/24 192.168.0.142/24 192.168.0.143/24
VM2	Free5gc U-plane 1	192.168.0.144/24
VM3	Free5gc U-plane 2	192.168.0.145/24
VM4	URANSIM RAN (gNodeB1)	192.168.0.131/24
VM5	URANSIM RAN (gNodeB2)	192.168.0.132/24
VM6	UERANSIM UE	192.168.0.133/24

Table IV.1 Virtual Machine and Software Identifiers

In Table IV.1, we describe every Virtual Machine (VM) and every Software (SW) instance with the IPv4 Address of the interface, and the way to interact with others blocks or levels in the system.

Network Function	IP Address	IP Address on SBI
AMF 1	192.168.0.142	127.0.0.18
SMF 1	192.168.0.142	127.0.0.2
PCF 1		127.0.0.7
AMF 2	192.168.0.143	127.0.0.28
SMF 2	192.168.0.143	127.0.0.12
PCF 2		127.0.0.17

Table IV.2 Network Function Interfaces Identifier

Table IV.2 shows the IPv4 Addresses of the Network Functions and the IPv4 Address on the Service Based Interface for the free5GC control plane. Before moving to results, we will show the simple description of our UERAMSIM simulator example shown in Table IV.3.

Virtual Machine Number	Software and Role	IP Address
VM 1	Free5gc C-plane (N2)	192.168.0.125 172.20.10.5
VM 2	UERANSIM gNodeB	192.168.0.73
VM 3	UERANSIM UE	192.168.0.21
VM 4	Free5gc U-plane (N3)	172.20.10.6

Table IV.3 Description of Functions

Table IV.3 describes a very simple configuration that uses free5GC and UERANSIM to select the nearby UPF according to the connected gNodeB.

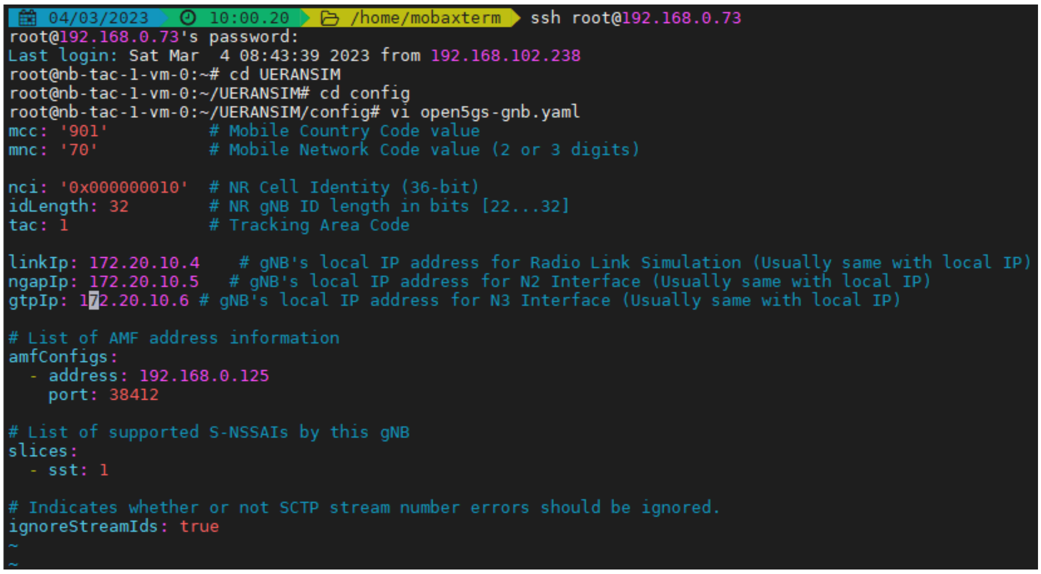


Fig. IV.8 gNodeB Setting Parameters

Fig. IV.8 shows the parameters we set on the appropriate file to obtain the result. To edit these parameters, we can move on the UERANSIM and config directories from Linux OS, which is the Operating System (OS) of the software MobaXterm we used for this thesis. The command vi open5gs-gnb.yaml is executed to access and edit the file. These parameters are set on the VM 2 UERANSIM gNodeB identified with the IPv4 address 192.168.0.73.

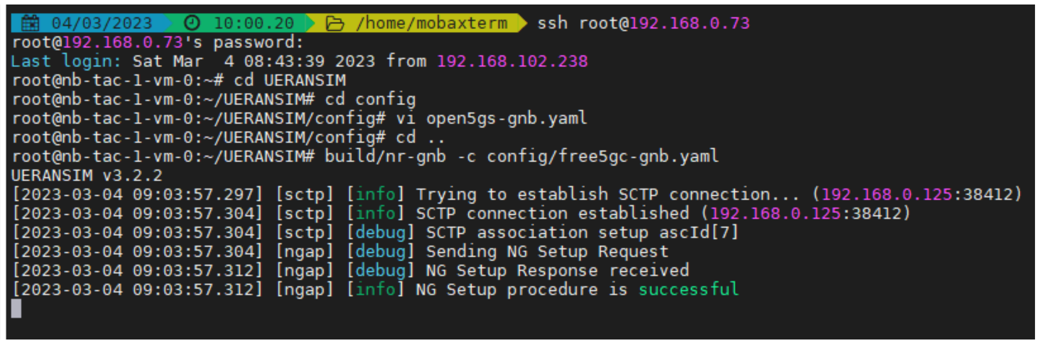
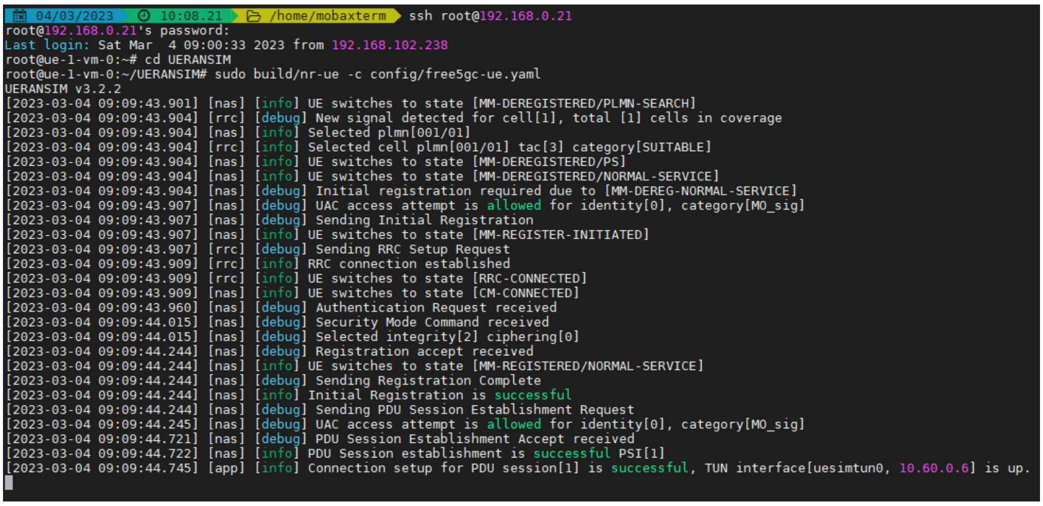


Fig. IV.9 gNodeB Initialization

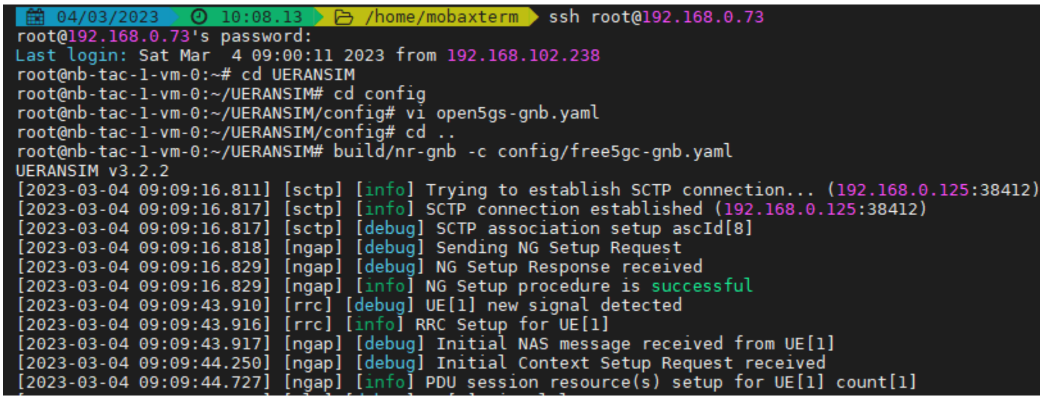
After editing the file, now we can initialize our new generation base station (gNodeB) to receive the signal from the UE. To initialize it, we move back on the UERANSIM directory, execute the command build/nrgnb -c config/free5gc-gnb.yaml and see the successful initialization procedure of the gNodeB. At this moment we can wait for the UE signal to establish the connection between gNodeB and UE.



```
04/03/2023  10:08.21  /home/mobaxterm  ssh root@192.168.0.21
root@192.168.0.21's password:
Last login: Sat Mar  4 09:00:33 2023 from 192.168.102.238
root@ue-1-vm-0:~# cd UERANSIM
root@ue-1-vm-0:~/UERANSIM# sudo build/nr-ue -c config/free5gc-ue.yaml
UERANSIM v3.2.2
[2023-03-04 09:09:43.901] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2023-03-04 09:09:43.904] [rrc] [debug] New signal detected for cell[1], total [1] cells in coverage
[2023-03-04 09:09:43.904] [nas] [info] Selected plmn[001/01]
[2023-03-04 09:09:43.904] [rrc] [info] Selected cell plmn[001/01] tac[3] category[SUITABLE]
[2023-03-04 09:09:43.904] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2023-03-04 09:09:43.904] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2023-03-04 09:09:43.904] [nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2023-03-04 09:09:43.907] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:09:43.907] [nas] [debug] Sending Initial Registration
[2023-03-04 09:09:43.907] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2023-03-04 09:09:43.907] [rrc] [debug] Sending RRC Setup Request
[2023-03-04 09:09:43.909] [rrc] [info] RRC connection established
[2023-03-04 09:09:43.909] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2023-03-04 09:09:43.909] [nas] [info] UE switches to state [CM-CONNECTED]
[2023-03-04 09:09:43.960] [nas] [debug] Authentication Request received
[2023-03-04 09:09:44.015] [nas] [debug] Security Mode Command received
[2023-03-04 09:09:44.015] [nas] [debug] Selected integrity[2] ciphering[0]
[2023-03-04 09:09:44.244] [nas] [debug] Registration accept received
[2023-03-04 09:09:44.244] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2023-03-04 09:09:44.244] [nas] [debug] Sending Registration Complete
[2023-03-04 09:09:44.244] [nas] [info] Initial Registration is successful
[2023-03-04 09:09:44.244] [nas] [debug] Sending PDU Session Establishment Request
[2023-03-04 09:09:44.245] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:09:44.721] [nas] [debug] PDU Session Establishment Accept received
[2023-03-04 09:09:44.722] [nas] [info] PDU Session establishment is successful PSI[1]
[2023-03-04 09:09:44.745] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.60.0.6] is up.
```

Fig. IV.10 UE Launch and Connection

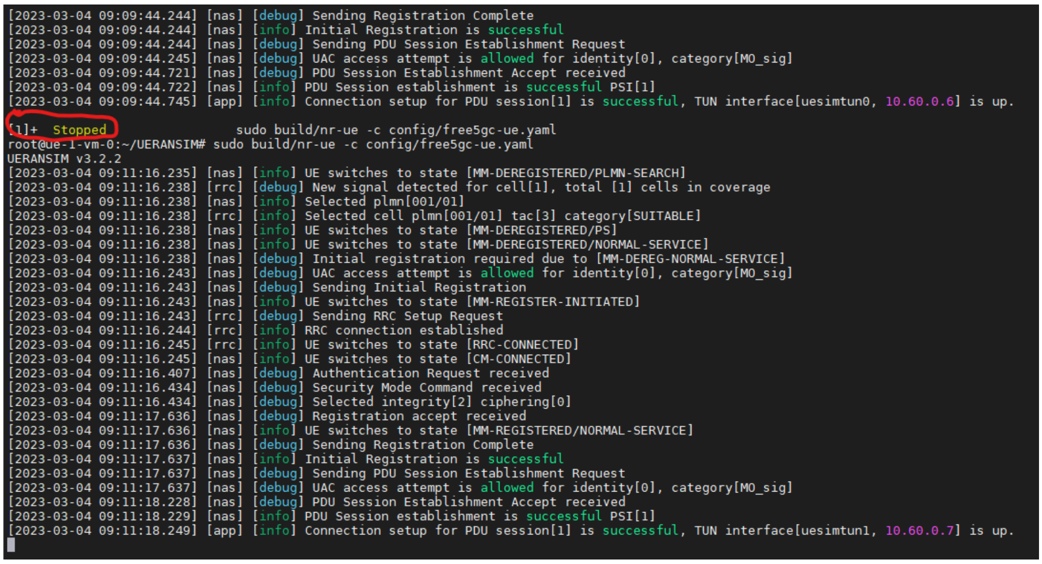
To transmit the signal to establish the connection between UE and gNodeB, it is possible to move on the VM 3 UERANSIM UE, also identified by the IPv4 address 192.168.0.21, and to execute the command
sudo build/nr-ue -c config/free5gc-ue.yaml (on the UERANSIM directory but by using the administrator privilege (sudo)), to access and to emit the signal to the gNodeB and establish connection (Fig. IV.10).



```
04/03/2023  10:08.13  /home/mobaxterm  ssh root@192.168.0.73
root@192.168.0.73's password:
Last login: Sat Mar  4 09:00:11 2023 from 192.168.102.238
root@nb-tac-1-vm-0:~# cd UERANSIM
root@nb-tac-1-vm-0:~/UERANSIM# cd config
root@nb-tac-1-vm-0:~/UERANSIM/config# vi open5gs-gnb.yaml
root@nb-tac-1-vm-0:~/UERANSIM/config# cd ..
root@nb-tac-1-vm-0:~/UERANSIM# build/nr-gnb -c config/free5gc-gnb.yaml
UERANSIM v3.2.2
[2023-03-04 09:09:16.811] [sctp] [info] Trying to establish SCTP connection... (192.168.0.125:38412)
[2023-03-04 09:09:16.817] [sctp] [info] SCTP connection established (192.168.0.125:38412)
[2023-03-04 09:09:16.817] [sctp] [debug] SCTP association setup ascId[8]
[2023-03-04 09:09:16.818] [ngap] [debug] Sending NG Setup Request
[2023-03-04 09:09:16.829] [ngap] [debug] NG Setup Response received
[2023-03-04 09:09:16.829] [ngap] [info] NG Setup procedure is successful
[2023-03-04 09:09:43.910] [rrc] [debug] UE[1] new signal detected
[2023-03-04 09:09:43.916] [rrc] [info] RRC Setup for UE[1]
[2023-03-04 09:09:43.917] [ngap] [debug] Initial NAS message received from UE[1]
[2023-03-04 09:09:44.250] [ngap] [debug] Initial Context Setup Request received
[2023-03-04 09:09:44.727] [ngap] [info] PDU session resource(s) setup for UE[1] count[1]
```

Fig. IV.11 Connection Established Between gNodeB and UE

Fig. V.11 shows the completed connection established between gNodeB and UE according to the preceding step in the VM 2 UERANSIM gNodeB.This occurs after the initialization of UERANSIM UE.
We now show in the next two figures (Fig. IV.12 and Fig. IV.13) what happens in gNodeB and UE when the gNodeB loses the signal.

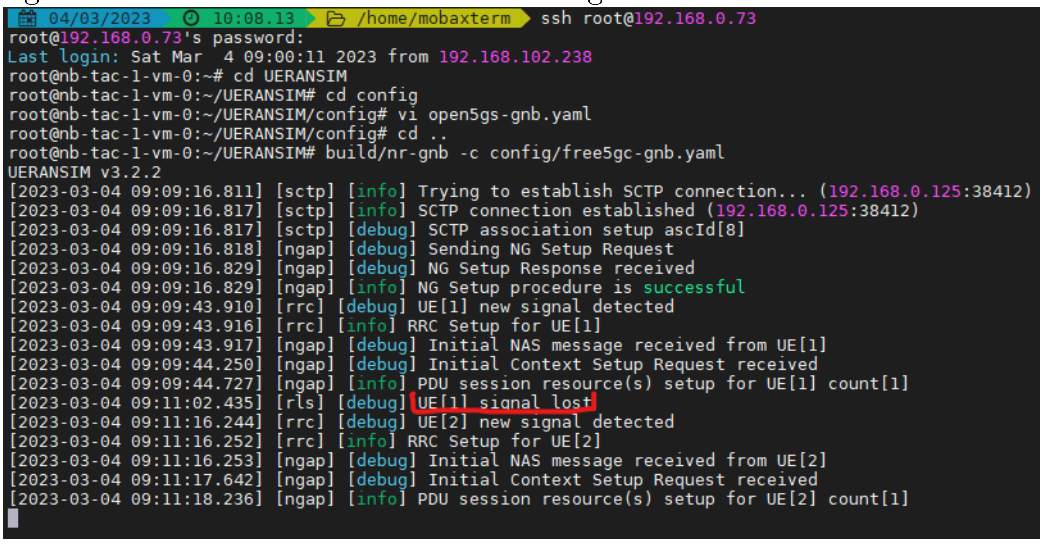


```
[2023-03-04 09:09:44.244] [nas] [debug] Sending Registration Complete
[2023-03-04 09:09:44.244] [nas] [info] Initial Registration is successful
[2023-03-04 09:09:44.244] [nas] [debug] Sending PDU Session Establishment Request
[2023-03-04 09:09:44.245] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:09:44.721] [nas] [debug] PDU Session Establishment Accept received
[2023-03-04 09:09:44.722] [nas] [info] PDU Session establishment is successful PSI[1]
[2023-03-04 09:09:44.745] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun0, 10.60.0.6] is up.

[1]+  Stopped                 sudo build/nr-ue -c config/free5gc-ue.yaml
root@ue-1-vm-0:~/UERANSIM# sudo build/nr-ue -c config/free5gc-ue.yaml
UERANSIM v3.2.2
[2023-03-04 09:11:16.235] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2023-03-04 09:11:16.238] [rrc] [debug] New signal detected for cell[1], total [1] cells in coverage
[2023-03-04 09:11:16.238] [nas] [info] Selected plmn[001/01]
[2023-03-04 09:11:16.238] [rrc] [info] Selected cell plmn[001/01] tac[3] category[SUITABLE]
[2023-03-04 09:11:16.238] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2023-03-04 09:11:16.238] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2023-03-04 09:11:16.238] [nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2023-03-04 09:11:16.243] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:11:16.243] [nas] [debug] Sending Initial Registration
[2023-03-04 09:11:16.243] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2023-03-04 09:11:16.243] [rrc] [debug] Sending RRC Setup Request
[2023-03-04 09:11:16.244] [rrc] [info] RRC connection established
[2023-03-04 09:11:16.245] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2023-03-04 09:11:16.245] [nas] [info] UE switches to state [CM-CONNECTED]
[2023-03-04 09:11:16.407] [nas] [debug] Authentication Request received
[2023-03-04 09:11:16.434] [nas] [debug] Security Mode Command received
[2023-03-04 09:11:16.434] [nas] [debug] Selected integrity[2] ciphering[0]
[2023-03-04 09:11:17.636] [nas] [debug] Registration accept received
[2023-03-04 09:11:17.636] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2023-03-04 09:11:17.636] [nas] [debug] Sending Registration Complete
[2023-03-04 09:11:17.637] [nas] [info] Initial Registration is successful
[2023-03-04 09:11:17.637] [nas] [debug] Sending PDU Session Establishment Request
[2023-03-04 09:11:17.637] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:11:18.228] [nas] [debug] PDU Session Establishment Accept received
[2023-03-04 09:11:18.229] [nas] [info] PDU Session establishment is successful PSI[1]
[2023-03-04 09:11:18.249] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun1, 10.60.0.7] is up.
```

Fig. IV.12 UE Signal Loss

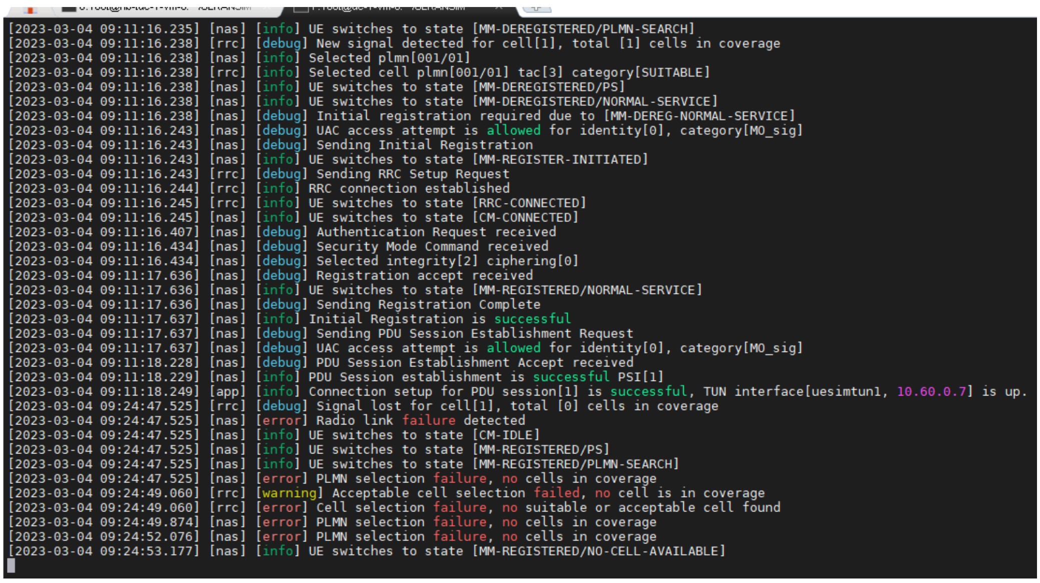
Fig. IV.12 shows what happens in the UE when it stops transmitting the signal and at the same time the new UE signal is transmitted.



```
04/03/2023  10:08.13  /home/mobaxterm  ssh root@192.168.0.73
root@192.168.0.73's password:
Last login: Sat Mar  4 09:00:11 2023 from 192.168.102.238
root@nb-tac-1-vm-0:~# cd UERANSIM
root@nb-tac-1-vm-0:~/UERANSIM# cd config
root@nb-tac-1-vm-0:~/UERANSIM/config# vi open5gs-gnb.yaml
root@nb-tac-1-vm-0:~/UERANSIM/config# cd ..
root@nb-tac-1-vm-0:~/UERANSIM# build/nr-gnb -c config/free5gc-gnb.yaml
UERANSIM v3.2.2
[2023-03-04 09:09:16.811] [sctp] [info] Trying to establish SCTP connection... (192.168.0.125:38412)
[2023-03-04 09:09:16.817] [sctp] [info] SCTP connection established (192.168.0.125:38412)
[2023-03-04 09:09:16.817] [sctp] [debug] SCTP association setup ascId[8]
[2023-03-04 09:09:16.818] [ngap] [debug] Sending NG Setup Request
[2023-03-04 09:09:16.829] [ngap] [debug] NG Setup Response received
[2023-03-04 09:09:16.829] [ngap] [info] NG Setup procedure is successful
[2023-03-04 09:09:43.910] [rrc] [debug] UE[1] new signal detected
[2023-03-04 09:09:43.916] [rrc] [info] RRC Setup for UE[1]
[2023-03-04 09:09:43.917] [ngap] [debug] Initial NAS message received from UE[1]
[2023-03-04 09:09:44.250] [ngap] [debug] Initial Context Setup Request received
[2023-03-04 09:09:44.727] [ngap] [info] PDU session resource(s) setup for UE[1] count[1]
[2023-03-04 09:11:02.435] [rls] [debug] UE[1] signal lost
[2023-03-04 09:11:16.244] [rrc] [debug] UE[2] new signal detected
[2023-03-04 09:11:16.252] [rrc] [info] RRC Setup for UE[2]
[2023-03-04 09:11:16.253] [ngap] [debug] Initial NAS message received from UE[2]
[2023-03-04 09:11:17.642] [ngap] [debug] Initial Context Setup Request received
[2023-03-04 09:11:18.236] [ngap] [info] PDU session resource(s) setup for UE[2] count[1]
```

Fig. IV.13 Signal loss and new detection in gNodeB

Fig. IV.13 identifies in red what happen in the Base Station when the UE loses the signal and at the same time the new UE signal occurred. Then the gNodeB establishes the new connection with the UE, and the signal can be transmitted to the receiver.



```
[2023-03-04 09:11:16.235] [nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[2023-03-04 09:11:16.238] [rrc] [debug] New signal detected for cell[1], total [1] cells in coverage
[2023-03-04 09:11:16.238] [nas] [info] Selected plmn[001/01]
[2023-03-04 09:11:16.238] [rrc] [info] Selected cell plmn[001/01] tac[3] category[SUITABLE]
[2023-03-04 09:11:16.238] [nas] [info] UE switches to state [MM-DEREGISTERED/PS]
[2023-03-04 09:11:16.238] [nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[2023-03-04 09:11:16.238] [nas] [debug] Initial registration required due to [MM-DEREG-NORMAL-SERVICE]
[2023-03-04 09:11:16.243] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:11:16.243] [nas] [debug] Sending Initial Registration
[2023-03-04 09:11:16.243] [nas] [info] UE switches to state [MM-REGISTER-INITIATED]
[2023-03-04 09:11:16.243] [rrc] [debug] Sending RRC Setup Request
[2023-03-04 09:11:16.244] [rrc] [info] RRC connection established
[2023-03-04 09:11:16.245] [rrc] [info] UE switches to state [RRC-CONNECTED]
[2023-03-04 09:11:16.245] [nas] [info] UE switches to state [CM-CONNECTED]
[2023-03-04 09:11:16.407] [nas] [debug] Authentication Request received
[2023-03-04 09:11:16.434] [nas] [debug] Security Mode Command received
[2023-03-04 09:11:16.434] [nas] [debug] Selected integrity[2] ciphering[0]
[2023-03-04 09:11:17.636] [nas] [debug] Registration accept received
[2023-03-04 09:11:17.636] [nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[2023-03-04 09:11:17.636] [nas] [debug] Sending Registration Complete
[2023-03-04 09:11:17.637] [nas] [info] Initial Registration is successful
[2023-03-04 09:11:17.637] [nas] [debug] Sending PDU Session Establishment Request
[2023-03-04 09:11:17.637] [nas] [debug] UAC access attempt is allowed for identity[0], category[MO_sig]
[2023-03-04 09:11:18.228] [nas] [debug] PDU Session Establishment Accept received
[2023-03-04 09:11:18.229] [nas] [info] PDU Session establishment is successful PSI[1]
[2023-03-04 09:11:18.249] [app] [info] Connection setup for PDU session[1] is successful, TUN interface[uesimtun1, 10.60.0.7] is up.
[2023-03-04 09:24:47.525] [rrc] [debug] Signal lost for cell[1], total [0] cells in coverage
[2023-03-04 09:24:47.525] [nas] [error] Radio link failure detected
[2023-03-04 09:24:47.525] [nas] [info] UE switches to state [CM-IDLE]
[2023-03-04 09:24:47.525] [nas] [info] UE switches to state [MM-REGISTERED/PS]
[2023-03-04 09:24:47.525] [nas] [info] UE switches to state [MM-REGISTERED/PLMN-SEARCH]
[2023-03-04 09:24:47.525] [nas] [error] PLMN selection failure, no cells in coverage
[2023-03-04 09:24:49.060] [rrc] [warning] Acceptable cell selection failed, no cell is in coverage
[2023-03-04 09:24:49.060] [rrc] [error] Cell selection failure, no suitable or acceptable cell found
[2023-03-04 09:24:49.874] [nas] [error] PLMN selection failure, no cells in coverage
[2023-03-04 09:24:52.076] [nas] [error] PLMN selection failure, no cells in coverage
[2023-03-04 09:24:53.177] [nas] [info] UE switches to state [MM-REGISTERED/NO-CELL-AVAILABLE]
```

Fig. IV.14 UE state after gNodeB stops Initialization

Fig. IV.14 shows what happens at the UE when the gNodeB stops or no initialization occurs.

5 CHAPTER V. PERFORMANCES EVALUATIONS

In this chapter, we will show some result which describe well our simulator and help us to more evaluate the performance of the simulator, according to the payload transmission as a time function.

5.1 A- UERANSIM Evaluation

Time (ms)	**0.05**	**0.1**	**0.2**	**0.05**	**0.1**	**0.2**	**0.05**	**0.1**	**0.2**	**0.05**	**0.1**	**0.2**
Payload (byte)	**64**	**64**	**64**	**512**	**512**	**512**	**1024**	**1024**	**1024**	**2048**	**2048**	**2048**
Avg RTT without 5G (ms)	**10.5**	**10.2**	**11.3**	**10.7**	**10.2**	**10.4**	**10.2**	**10.7**	**10.6**	**11.4**	**11.3**	**11.7**
Avg RTT (ms)	**7.8**	**7.9**	**7.9**	**8.0**	**7.9**	**8.1**	**8.0**	**8.4**	**8.3**	**8.3**	**8.4**	**8.4**
Average Difference (ms)	**2.7**	**2.3**	**3.4**	**2.7**	**2.3**	**2.3**	**2.2**	**2.3**	**2.3**	**3.1**	**3.9**	**3.3**

Table V.1 References values of UERANSIM get to the fixed time interval

Table V.1 shows the references values of UERANSIM get to the fixed time interval in which, we get the differents rows averages from which, we compute the average difference such as described in the same the table. These two commands:

i)- sudo ping -c 1000 -i .1 -U -s 56 1.1.1.1
ii)- sudo ping -c 1000 -i .1 -U -s 56 -I uesimtun0 1.1.1.1

help us after execute it on our UERANSIM simulator to obtain these averages. With the first command, we can catch the Round Trip Time (RTT) Average without mobile radio system for example passing through the normal ethernet interfaces, this mean without use of the "uesimtun0". And the second one is used to catch the normal Average using the mobile radio system when we include the (-I ueransim) parameter.
From these commands, it is possible to set the values of the differents parameters we need. For example, for the time, we can modify this variable (-i.1), for the Payload it is possible to vary (-s 56) and at the end modify the numbers of the packet we can generate by using (-c 1000).

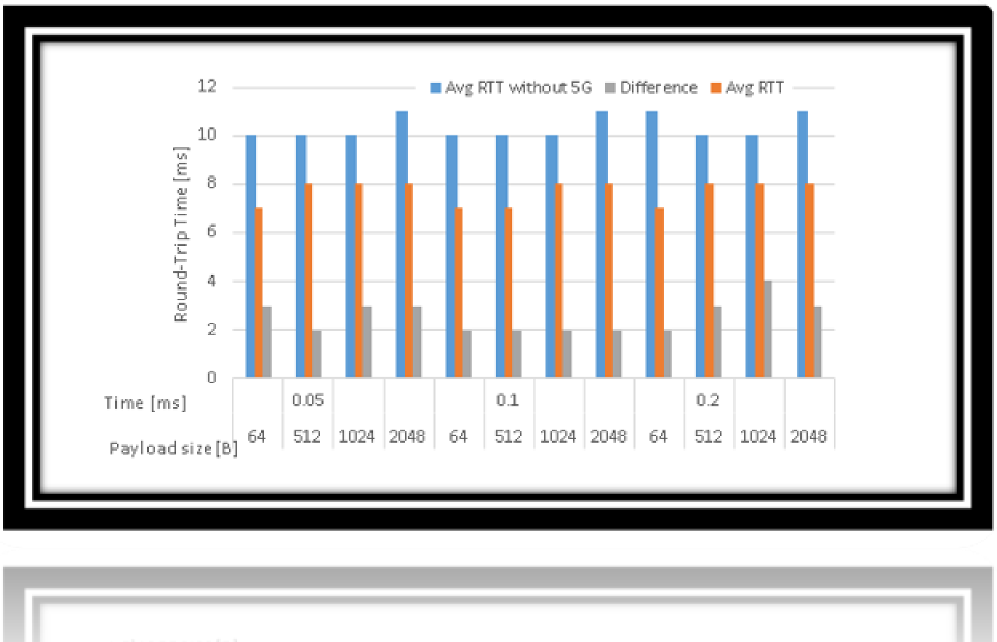


Fig. V.1 UERANSIM Payload Statistics

Fig. V.1 shows the 5G packets Statistics referring to the above table, this figure highlights the averages of the Payload at the fixed time intervall and Allows us to clearly see the good performance of 5G technology in terms of the latency.

5.2 B- srsLTE/srsRAN Evaluation

Time (ms)	0.05	0.1	0.2	0.05	0.1	0.2	0.05	0.1	0.2	0.05	0.1	0.2
Payload (byte)	64	64	64	512	512	512	1024	1024	1024	2048	2048	2048
Avg RTT without 4G (ms)	10.5	10.2	11.3	10.7	10.2	10.4	10.2	10.7	10.6	11.4	11.3	11.7
Avg RTT (ms)	80.6	52.0	35.6	70.2	64.4	46.6	41.1	50.7	51.5	90.0	49.5	61.8
Average Difference (ms	70.1	42.0	24.4	60.0	54.2	36.2	31.0	40	41.0	79.0	38.2	50.0

Table V.2 References values of srsLTE get to the fixed time interval

Table V.2 shows the references values of srsLTE get to the fixed time interval where we obtain the average by executing this command:

i)- sudo ip netns exec ue1 sudo ping -c 1000 -i .1 -U -s 56 -I tun_ srsue 1.1.1.1

on srsUE Virtual Machine. As in the UERANSIM case, it is also possible to

get the differents Payload with the Time in (ms) by varing the values of (-s 56) for il payload and (-i.1) for the time.
Note that, the Round Trip Time Average in this case is the same as in the UERANSIM case because, these depend only on the Virtual Machines (VM) and not on the 4/5G software and the VM's are identical.
It also too important to understand that, using the default configuration of the srsLTE, this creates a virtual network interface named "tun_ srsue" on machine 2 with an IP in the network 192.168.0.16. Assuming the UE has been assigned IP 192.168.1.1, in this example and we may now exchange IP traffic with system over the LTE link.

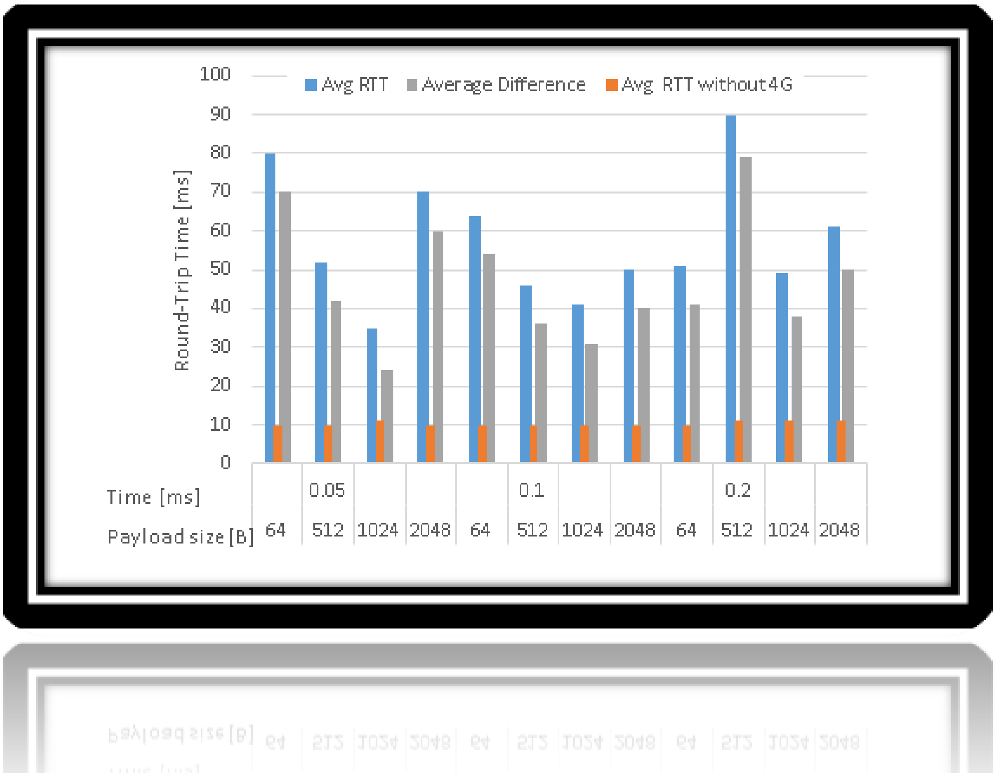


Fig. V.2 srsLTE Payload Statistics

The Fig. V.2 depicts the statistic diagram of the payload such as describe on the table below. Now, we can compare the both figures to detect and conclude according to the 5G performances.
In order to understand what is one of the main diffrence between these two software system (UERANSIM and srsLTE), we use the same Payload value in byte and the same Time interval in ms (millisecond) to draw the diagram above that the average was obtained by executing the above (i) command.

6 CHAPTER VI. CONCLUSION

5G networks are a key part of the worldwide digital transformation that stands to impact consumers, public sector organizations and enterprises across every vertical industry.
Around the world today, the demand for better mobile broadband experiences is continuously increasing. A huge number of devices require connection to the Internet such as mobile phones, computers, tablets, smart watches, etc. Users of these kinds of devices always demand higher data rates. Moreover, several industries are going through a digital transformation. There are emerging concepts for smart vehicles, human machine interaction, sensor networks, critical control of remote devices, etc. Communication procedures addressed for these new services are different from the human use case.
In order to better understand the 5G networking environment and analyze the performance of the 5G wireless communication system, in this thesis I have compared the performance of two open-source program system used to simulate, evaluate and experiment the network traffic between the UE, eNodeB and EPC or UE and gNodeB, namely, srsLTE and UERANSIM. For both system, we made as the packets varied the transmission and notice that, the performances in terms of the latency in packet transmission were better for 5G then 4G. A simulator for both software environments has been deployed and tested under different traffic conditions. The results of this experiment is shown in the Chapter V where we describe as well the different averages of the packets depending on time to reveal the best performances of the systems that are in use today in our daily life.

7 REFERENCES

[1] Read about the key technologies creating all the buzz around 5G in our blog post: 5G Trends

[2] The evolution to 5G and the progress so far has been discussed in the following post: 3GPP Release-15: Further LTE Enhancements and 5G Normative Work Kick-off

[3] Harald Remmert, CTO, Cellular Solutions, Digi International March 19, 2021

[4] https://nickvsnetworking.com/my-first-5g-core-open5gs-and-ueransim/

[5] https://www.sdxcentral.com/5g/definitions/key-elements-5g-network/

[6] Sources: Patel et al. (2014); 5G Infrastructure Association (2015). See for small scale application and experimentation with virtual networks for instance the PhD by Strijkers (2014). For information on SDN in general, see Göransson and Black (2014) and Stallings (2016).

[7] Floodlight controller, Floodlight documentation, for developers, architecture. $from : http : //www.projectfloodlight.org/floodlight$

[8] OpenDaylight: a Linux Foundation Collaborative Project, 2014. [On line]. Retrieved from: http://www.opendaylight.org.

[9] Erickson D. The Beacon OpenFlow controller. Pro-ceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking.ACM, 2013

[10] Yu M, Rexford J, Freedman MJ, Wang J. Scalableflow-based networking with DIFANE. SIGCOMM Computer Communication Review 2010.

[11] Tootoonchian A, Ganjali Y. HyperFlow: a distributed control plane for OpenFlow. Proceedings of the 2010Internet Network Management Conference on Re-search on Enterprise Networking. USENIX

[12] Cai Z. Maestro: achieving scalability and coordina-tion in centralized network control plane, Ph.D. dis-sertation, Rice Univ.

Houston, TX, USA, 2011.

[13] Rimal BP, Jukan A, Katsaros D, Goeleven Y. Archi-tectural requirements for cloud computing systems:an enterprise cloud approach. Journal of Grid Com-puting 2011.

[14] Armbrust M, a view of cloud computing. Communication of the ACM ACM 2010.

[15] Dixit A,Hao F, Mukherjee S, Lakshman T, Kompella R. Towards an elastic distributed SDN controller. In Proceedings of the Second ACM SIGCOMM Work-shop on Hot Topics in Software Defined Networking, service. Hot SDN 13. ACM: New York, NY, USA, 2013.

[16] Dixit A, Hao F, Mukherjee S, Lakshman TV,Kompella R. ElastiCon: an elastic distributed SDN controller. Proceedings of the Tenth ACM/IEEE Sym-posium on Architectures for Networking and Commu-nications Systems. ACM, 2014.

[17] Scott-Hayward S, O'Callaghan G,Sezer S. SDN secu-rity: a survey, IEEE SDN for Future Networks andServices (SDN4FNS), 2013.

[18] Kloeti R. OpenFlow: a security analysis. April 2013.

[19] $https://www.usenix.org/system/files/conference$ $/hot-ice12/hotice12-final33_0.pdf$. and Cbench (Controller Bench)

[20] Jarschel M, Lehrieder F, Magyari Z, Pries R. A flexible OpenFlow-controller benchmark. Proc. EWSDN,2012.

[21] Tipper D. Resilient network design: challenges andfuture directions. Telecommunication Systems 2014.

[22] Avižienis A, Laprie JC, Randell B, Landwehr C. Ba-sic concepts and taxonomy of dependable and secure computing, Dependable and Secure Computing,IEEE Transactions on. IEEE, 2004.

[23] J. C. Ikuno, M. Wrulich, and M. Rupp, "TCP Performance and modeling of LTE H-ARQ," in proceedings of the International ITG Workshop on Smart Antennas (WSA 2009), Berlin, Germany, 2009.

[24] Sources: Patel et al. (2014); 5G Infrastructure Association (2015). See for small scale application and experimentation with virtual networks for instance the PhD by Strijkers (2014). For information on SDN in general, see Göransson and Black (2014) and Stallings (2016).

[25] Source: 4G Americas (2014).

[26] For more details, see 5G Americas, Network Slicing for 5G Networks and Services, November 2016. Available at:http://www.5gamericas.org /files/3214 /7975/0104/5$G_{A}mericas_{N}etwork_{S}licing_{1}1.21_{F}inal.pdf$.

[27] R. Kloeti, “OpenFlow: a security analysis,” Proceedings of the 21st IEEE International Conference on Network Protocols (ICNP), April 2013.

[28] Magnus Olsson, et. al., SAE and the Evolved Packet Core-Driving the Mobile broadband Revolution, AP, 2009.

[29] www.rfwireless-world.com/Articles/ difference-between-TDD-and-FDD.html https://learning.oreilly.com/library/view/evolved-packet-system/978047072 3661/chap03-sec033.html(downlink-uplink) www.rfwireless-world.com/Articles/ difference-between-SC-FDMA-and OFDMA.html

[30] S. Alamouti, "A simple transmit diversity technique for wireless communications," IEEE J. Sel. Areas Commun., vol. 16, no. 8, pp. 1451-1458, 1998.

[31] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D Sutton, Pablo Serrano, Cristina Cano, and Doug J Leith. "srsLTE: an open-source platform for LTE evolution and experimentation". In: Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization. ACM. 2016, pp. 25–32.

[32] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano and Douglas J. Leith. srsLTE. https://github .com/srsLTE/srsLTE, Last accessed on 2019-08-20. 2019.

[33] Software Radio Systems. SRSLte1. https://www.softwareradiosystems. com/products/srslte, Last accessed on 2019-08-20. 2019.

[34] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D. Sutton, Pablo Serrano, Cristina Cano and Douglas J. Leith. srsLTE. https://github

.com/srsLTE/srsLTE, Last accessed on 2019-08-20. 2019.

[35] http://tenettech.net/SDR/product-category/usrp-bus-series/

[36]https://www.free5gc.org/installations/stage-3-sim-install/

[37] http://www.digi.com/blog/post/5g-network-architecture

8 APPENDIX A

8.1 Installation Steps

These softwares need to be installed on the Ubuntu Operating System Virtual Machine.
For Ubuntu 16.04 version operating system there is need of installing some of the dependencies libraries for srsLTE software by running this command:

```
sudo apt-get install cmake libfftw3-dev libmbedtls-dev libboost-program
-options-dev libconfig++-dev libsctp-dev.
```

But from the Ubuntu 20.04 version to the actual 23.04 version of April 2023, that dependencies package is now replaced with libmbedtls-dev. So you need to install libmbedtls-dev package by using:[36]

```
sudo apt-get update
sudo apt-get install libmbedtls-dev
```

8.2 Install srsLTE/srsRAN

Now let us clone the srsLTE or srsRAN and build using the commands mention below:

```
cd
git clone https://github.com/srsLTE/srsLTE.git
cd srsLTE
mkdir build
cd build
cmake ../
make
make test
sudo make install
srslte_ install_ configs.sh user
```

By default, all the applications in srsLTE/srsRAN will search for the config files in the user's home directory (/.config/srsLTE) upon startup[34]. So you need to install using the commands sudo make install and also using install config.sh.

8.3 Install UERANSIM

To download UERANSIM

cd
git clone https://github.com/aligungr/UERANSIM
cd UERANSIM
git checkout v3.1.0

Update and upgrade ueransim VM first:

sudo apt update
sudo apt upgrade

Install required tools:

sudo apt install make
sudo apt install g++
sudo apt install libsctp-dev lksctp-tools
sudo apt install iproute2
sudo snap install cmake –classic

Build UERANSIM

cd /UERANSIM
make

Setting free5GC and UERANSIM Parameters
In free5gc VM, we need to edit three files:

- - /free5gc/config/amfcfg.yaml
- - /free5gc/config/smfcfg.yaml
- - /free5gc/config/upfcfg.yaml

First SSH into free5gc VM, and change /free5gc/config/amfcfg.yaml

cd /free5gc
nano config/amfcfg.yaml

It is possible to replace ngapIpList IP from 127.0.0.1 to 192.168.X.X, namely by edit:

- - /free5gc/config/smfcfg.yaml

nano config/smfcfg.yaml

and finally, in the same way, edit:

- - /free5gc/config/upfcfg.yaml

8.4 Setting UERANSIM

In the UERANSIM VM, there are two files related to free5gc:

- - /UERANSIM/config/free5gc-gnb.yaml
- - /UERANSIM/config/free5gc-ue.yaml

The second file is for UE, which we don't have to change if the data inside is consistent with the (default) registration data we set using WebConsole as the following.

Install free5GC WebConsole:
free5GC provides a simple web tool WebConsole to help creating and managing UE registrations to be used by various 5G network functions (NF). To build WebConsole we need Node.js and Yarn.
First SSH into free5gc (192.168.X.X), and remove obsolete tools that may exists:

```
sudo apt remove cmdtest
sudo apt remove yarn
```

Then install Node.js and Yarn using:

```
curl -sS https://dl.yarnpkg.com/debian/pubkey.gpg | sudo apt-key add -
echo "deb https://dl.yarnpkg.com/debian/ stable main" | sudo tee
/etc/apt/sources.list.d/yarn.list
sudo apt-get update
sudo apt-get install -y nodejs yarn
```

To build WebConsole

```
cd /free5gc
make webconsole
```

Notice that, the WebConsole has to be installed after the above Build UERANSIM and after "make".

curl: is a command line tool that enables data exchange between a device and a server through a terminal.

9 ACKNOWLEDGMENTS

To achieve this goal has not been easy but God surrounded me friends and people who have helped me realize this dream and I have to thank them with all my heart.
Firstly I have to say a big thank you to my parents, brothers and thier wives, sisters and husbands and my biggest family for their support and prayers:

Mr: SADEU Vincent	Mrs: SADEU Yveline Marthe
Mr: TETANUTOU Albert Robert	Mrs: Tetanutou Justine
Mr: WAMBO SADEU Eric	Mrs: WAMBO Pascaline P
Mrs: MEJOGO SADEU Rachelle	Mr: ESSONO Laurent
Mrs: KAMGUEM SADEU Christine	Mrs: KENGNE Yvonne
Mrs: TEUPO SADEU Doris	Mrs: MOKAM SADEU J
Mr: TSINKAM SADEU Emmanuel	Mrs: MAKOUWE Marie A

Secondly, a big thank you to all the teachers I met during this stage. A particular thanks to my Supervisor e Co-supervisor.

Supervisor:	Co-supervisor:
Professor: Franco DAVOLI	Dr.ssa: Chiara LOMBARDO
Professor: Roberto BRUSCHI	Dr: Sergio MANGIALARDI

I will always be grateful for what each of you has made in my life and I must never forget you, thank you so much.
Thirdly, I thank my dears friends and people who allowed me to keep hope until the end of this step:
Dr: Guillaume Thierry SOH KOMDJEU
Dr.ssa: Arlette MBOULA MBEMO
Dr: Pharan DJIMAFO
Dr: Benoit NKOULI FOUDA
Dr: Barnabe BINGANA NDJOMO
Dr.ssa: Giulia Nina NOTEWO
Dr: Patrick NGUENANG
Dr: Gerard Dumas LEUKEFACK
Dr: Pascaline NGO MOUA
Dr: Eric TANETSI
Dr: Francis MANBOU FOKA
Dr: Federic TAKOUDJOU

I will always be grateful to you, thank you so much.