La République algérienne démocratique et populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

UNIVERSITÉ AMAR TELIDJI LAGHOUAT

FACULTE DE TECHNOLOGIE

DEPARTEMENT D'ÉLECTRONIQUE

MEMOIRE DE MASTER

DOMAINE : Sciences et technologie
FILIERE : Télécommunications
OPTION : Réseaux et Télécommunications

Thème

5G Mobility Management

Présenté par
Bengana Mustapha Charaf Eddine

Le jury de soutenance :

Nom et prénom	Grade	Qualité
Mr.Lahcen Merah	Dr	Président
Mr Omar Sami Oubbati	Dr	Examinatrice
Mr Saadi Ramdani	MAA	Encadreur

Promotion: 2019-2020

Dedication

This thesis dedicated to:

To whom I prefer, and why not; She sacrificed for me and spared no effort to always make me happy

To my beloved mother.

We walk in the paths of life, and it remains who controls our minds in every way we walk with the kind face and the good deeds.

To my dear father.

who encouraged me throughout my university career,

To my dear sister,

who stood next to me and helped me with all their possessions, in many levels

To my friends, and everyone

Acknowledgments

First and foremost, I thank Almighty God for guiding me all the time and when. Which gave me health and wellness to accomplish this Thesis

I would like to thank my family for all their support and encouragement to me

A big thank you to my supervisor, Mr. Saadi Ramdani, for guiding me all the time and for supporting me on all my paths as I work on the Thesis, I am very grateful for the time that he spent helping me

Finally, a special thanks to Omar Ait Aissa, Recioui Mouadh, Elabed Soufiane and every friend who contributed to my encouragement all this time

Abstract:

The fifth-generation mobile network that will replace 4G cellular technology with higher multi-Gbps peak data speeds up to 10 Gbps, ultra-low latency less than a millisecond. It also promises to accelerate the development and widespread adoption of many of the emerging innovations currently limited to the periphery Public awareness, such as the Internet of Things (IoT), smart cities, and self-driving vehicles. In this work we did a study on next-generation mobility management that has always been challenging in all previous generations to bring in seamless connectivity and reduce dropped packets that were a problem in the fourth generation. We will use the open source software NS3 to simulate the next generation and see the impact of the handover on the next generation and what awaits mobility management as challenges.

Résumé:

Le réseau mobile de cinquième génération qui remplacera la technologie cellulaire 4G par des vitesses de données de multi-Gbps plus élevées jusqu'à 10 Gbps, ultra faible latence inférieure à une milliseconde. Il promet également d'accélérer le développement et l'adoption généralisée de nombreuses innovations émergentes actuellement limitées à la périphérie de la sensibilisation du public, comme l'Internet des objets (IoT), les villes intelligentes et les véhicules autonomes. Dans ce travail, nous avons fait une étude sur la gestion de la mobilité de la prochaine génération cela a toujours été un défi dans toutes les générations précédentes d'apporter une connectivité transparente et de réduire les paquets abandonnés qui ont été un problème dans la quatrième génération. Nous utiliserons le logiciel open source NS3 pour simuler la prochaine génération et voir l'impact du handover sur la prochaine génération et ce qui attend la gestion de la mobilité comme des défis.

ملخص:

شبكة الجيل الخامس من الهاتف المحمول التي ستحل محل تقنية الجيل الرابع الخلوية بسرعة بيانات فائقة متعددة تصل إلى 10 جيجابت في الثانية، زمن وصول منخفض للغاية أقل من ميلي ثانية. كما يعد بتسريع تطوير العديد من الابتكارات الناشئة واعتمادها على نطاق واسع، وهي تقتصر حالياً على الوعي العام المحيطي، مثل إنترنت الأشياء ، والمدن الذكية، والمركبات ذاتية القيادة. في هذا العمل قمنا بدراسة حول الجيل التالي من إدارة التنقل التي كانت دائما تحديا في جميع الأجيال السابقة لجلب اتصال سلس والحد من الحزم المسقطة التي كانت مشكلة في الجيل الرابع. سوف نستخدم برنامج مفتوح المصدر NS3 لمحاكاة الجيل القادم ونرى تأثير التسليم على الجيل القادم وما ينتظر إدارة التنقل كتحديات.

Table of Contents

TABLE OF CONTENTS

TABLE OF CONTENTS

List of Figures

LIST OF FIGURES

List of Tables

List of Abbreviations

1G: First Generation

2G: Second Generation

3G: Third Generation

3GPP: 3rd Generation Partnership Project

4G: Fourth Generation

5G: Fifth Generation

A

AMPS: Advanced Mobile Phone System

AP: Access Point

AR: Augmented Reality

AS: Access Stratum

AuC: Authentication Center

B

BPSK: Binary phase-shift keying

BSC: Base Station Controller

BSS: Base Station Sub-system

BTS: Base Transceiver Station

C

CDMA: Code Division Multiple Access

C-RNTI: Cell Radio Network Temporary

CSG: Closed Subscriber Group

CSI: Channel State Information

D

DASs: Distributive Antenna Structures

DRB: Digital Radio Broadcasting

E

EDGE: Enhanced Data GSM Evolution

EIR: Equipment Identity Register

EMBB: Enhanced Mobile Broadband

ENodeB: Evolved Base Stations

E-UTRAN: The Evolved UMTS Terrestrial Radio Access Network

EPC: The Evolved Packet Core

ETWS: Earthquake and Tsunami Warning System

G

GERAN: GSM EDGE Radio Access Network

GGSN: Gateway GPRS Support Node

GNB: Next Generation NodeB

GPRS: General Packet Radio Service

GSM: Global System for Mobile correspondence

GTP: GPRS Tunneling Protocol

LIST OF ABBREVIATIONS

GUTI: Globally Unique Temporary Identifier

H

HARQ: Hybrid Automatic Repeat Request

HD: High-Definition

HFN: Hyper Frame Number

HLR: Home Location Register

HSDPA: High Speed Downlink Packet access

HSUPA: High Speed Uplink Packet Access

HSPA+: High Speed Packet Access plus

HSS: Home Subscriber Server

HTTP: Hypertext Transfer Protocol

I

ICT: Information Communications Technology

IEEE: Institute of Electrical and Electronics Engineers

IMSI: International Mobile Subscriber Identity

IMEI: International Mobile Equipment Identity

IMT: International Mobile Telecommunications

IoT: Internet of Things

IP: Internet Protocol

IPv6: Internet Protocol Version 6

ITU-R: International Telecommunication Union-Radiocommunication Sector

L

LOS: Line Of Sight

LTE: Long Term Evolution

M

MAC: Media Access Control

MIMO: Multiple Input Multiple Output

MME: Mobility Management Entity

MN: Mobile Node

MS: Mobile Station

MSC: Mobile Switching Centre

MU-MIMO: Multi-User MIMO

N

NAS: Non-Access Stratum

O

OFDM: Orthogonal Frequency-Division Multiplexing

P

PBGT: Power Budget

PCEF: Policy Control Enforcement Function

PCRF: Control and Charging Rules Function

PDU: Protocol Data Unit

PDCP: Packet Data Convergence Protocol

PLMN: Public land mobile network

POTS: Plain Old Telephone Service

PDN: Packet Data Network

Q

QAM: Quadrature Amplitude Modulation

QoS: Quality of Service

QPSK: Quadrature Phase Shift Keying

R

RAT: Radio Access Technology

RF: Radio Frequency

RNC: Radio Network Controller

RRC: Radio Resource Control

RRM: Radio Resource Management

Identity

RSRP: Reference Signal Receive Power

S

SDAP: Service Data Adaptation Protocol

SDMA: Space-Division Multiple Access

SDU: Service Data Unit

S-GW: serving gateway

SGSN: Serving GPRS Support Node

SINR: Signal-to-Interference-Noise Ratio

SMS: Short Message System.

SSB: Synchronization Signal Block

T

TA: Tracking Areas

TACS: Total Access Communication System

TCP: Transmission Control Protocol

TDD: Time Division Duplexing

TNL: Tunnel

U

UE: The User Equipment

UMTS: Universal Mobile Terrestrial/Telecommunication Systems

USIM: Universal Subscriber Identity Module

UTRAN: Universal Terrestrial Access Network

V

V2x: Vehicle-To-Everything

VLR: Visitor Location Register

LIST OF ABBREVIATIONS

VNFs: Virtual Network Functions

W

Wi-Fi: Wireless Fidelity

WiMAX: Worldwide Interoperability for Microwave Access

WLAN: Wireless Local Area Network

X

XDSL: Digital Subscriber Line

XML: Extensible Markup Language

General Introduction

Over the years, the telecommunications sector has witnessed a tremendous development, starting from the first generation to the second and the third and the fourth generation, where every generation comes with improvement and development from the previous generation.

The need for tremendous speeds and unique experience led us to the fifth generation, which represents a huge leap in the speed of the mobile device, and includes This speed is both the rate of data that users can download to their device, and the response speed between sending and receiving information. This technology aims to increase the data speed to 10-100 times twice the current speed of 4G networks. It is expected that the download rates for users will reach more than one gigabyte per second, which is much faster than tens of megabytes per second.

One of the importance function in the wireless networks is the mobility management which track all the users on the network and deliver to them a best quality for the general uses , with two function has the location and the handover management , it's been developed after every generation Right up to the fifth generation which makes us ask the question , how it's been developed and how it's going to work with the technologies offer by the 5G ? , that is the aim of our work.

By using a program to simulate all about it ,we going to answer that question , the platform we use the LTE EPC and for the radio access has a custom mmwave Mac and Physique layer and its going to gives us an idea of the mobility management(both the location and the handover management). By using a program to simulate all about it ,we going to answer that question , the platform we use the LTE EPC and for the radio access has a custom mmwave Mac and Physique layer and it's going to gives us an idea of the mobility management(both the location and the handover management).

this work divided into 4 chapters: first chapter cover the different generations of the wireless networks. The second chapter explain everything about the mobility management. For the third chapter cover all about the 5 generation and the mobility management in it. finely in the last chapter we going to use the simulation to extract the results and discuss about it

Chapter I:

Different generations of mobile networks

I.1. Introduction

Through the years mobile wireless networking technology has evolved. Globally, there are multiple generations of wireless networking technologies that exist, the newest is the wireless network of the 5th generation.

Before the rise of 4G LTE, the 3G (third generations) remote system has been a functioning player in the industry. The 4G arrange came at a period when the 3G innovation has begun demonstrating restrictions in zones like range portion, data transfer capacity accessibility, and absence of consistent interconnectivity across heterogeneous systems. The 4G innovation has accompanied improved remote abilities, higher system speeds contrasted with 3G and visual advances. The 4G innovation is one that stands apart dependent on its capacity, for example, worldwide wandering, getting to the web whenever from anyplace and more extensive help for sight and sound administrations.

But still before going to talk about the 5th generation we need to ask some questions:

What are the limitations of the 4G generation in term of mobility management in IP networks? and what is the issue and challenges that waits for the next generation(5th)?

I.2. Evolution of Mobile Wireless Technologies

I.2.1 First generation mobile communication system (1G)

The 1G (first generation) arrange was completely simple cell frameworks and was a circuit exchanged based innovation which came into tasks in the mid-1980s. The norms for the 1G cell arrange included Advanced Mobile Phone System (AMPS) and Total Access Communication System (TACS). It was explicitly implied for voice and instant messages. The system had constrained inclusion territory, limit issues, low quality of transmissions, security and wasteful usage of the accessible range.[1]

I.2.2 Second generation mobile communication system (2G)

The second generation presented another computerized innovation for remote transmission otherwise called Global System for Mobile correspondence (GSM). GSM innovation turned into the base standard for additional advancement in remote measures later. This standard was equipped

for supporting up to 14.4 to 64kbps (greatest) information rate which is adequate for SMS and email administrations. Code Division Multiple Access (CDMA) framework created by Qualcomm additionally presented and executed in the mid-1990s. CDMA has a greater number of highlights than GSM as far as otherworldly productivity, number of clients and information rate.

So as to help higher information rate, General Packet Radio Service (GPRS) was presented and effectively conveyed. GPRS was equipped for information rate up to 171kbps.

EDGE – Enhanced Data GSM Evolution additionally created to improve information rate for GSM systems. EDGE was fit to help up to 384kbps.

Another mainstream innovation CDMA2000 was likewise acquainted with help higher information rate for CDMA systems.

I.2.3 Third generation communication system(3G)

The third generation began with the presentation of UMTS – Universal Mobile Terrestrial/Telecommunication Systems. UMTS has the speed rate of 384kbps and it bolster video requiring the first time for the mobile phones. After the presentation of the communication for mobile system 3G, advanced cells got mainstream over the globe. Explicit applications were produced for cell phones which handles sight and sound visit, email, video calling, games and social insurance.

So as to upgrade information rate in existing 3G systems, another two innovation enhancements are acquainted with organize. HSDPA – High Speed Downlink Packet access and HSUPA – High Speed Uplink Packet Access, created and sent to the 3G systems. 3.5G system can bolster up to 2mbps.

3.75 framework is an improved rendition of 3G coordinate with HSPA+ High Speed Packet Access plus. Later this framework will advance into all the more impressive 3.9G framework known as LTE (Long Term Evolution).

I.2.4 Fourth generation communication system(4G)

The fourth generation systems are improved variant of 3G systems created by IEEE, offers higher speed rate and able to deal with further developed mixed media administrations. LTE and LTE advanced wireless innovation utilized in fourth generation frameworks. Besides, it has similarity with past form in this way simpler organization and update of LTE and LTE advanced systems are conceivable.

Concurrent transmission of voice and information is conceivable with LTE framework which fundamentally improve speed rate. All serving including voice administrations are transmitted by the IP packets. Complex modulation plans and bearer conglomeration is utilized to duplicate uplink/downlink limit.

Wireless transmission advancements (ex: WiMAX) are acquainted in 4G framework with improve speed rate and system execution.

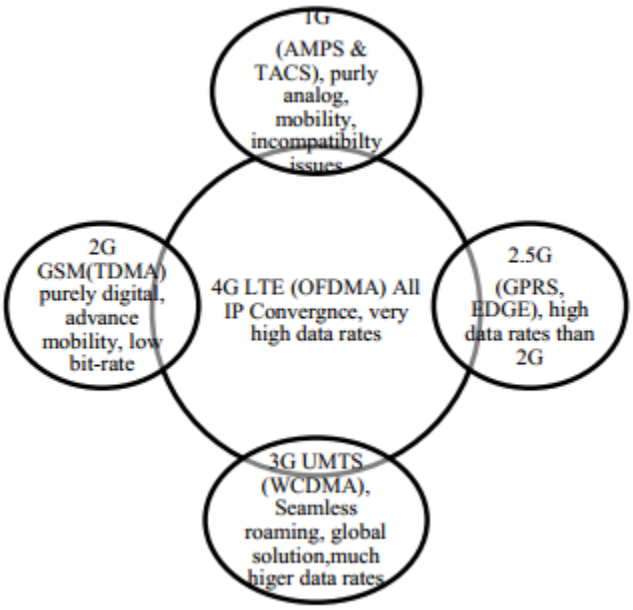

Figure I.1: Wireless technology evolution [1]

I.2.5 Fifth generation communication system(5G)

5G will utilize trend setting innovations to send ultra-quick web and media experience for clients. Current LTE advanced systems will change into supercharged 5G organizes in future. So as to

accomplish higher speed rate, 5G innovation will utilize millimeter waves and spectrum range for information transmission. Complex modulation procedure has been created to help monstrous information rate for Internet of Things.[2]

I.3. Different architecture of mobile wireless networks

I.3.1 The architecture of the 1G

The first generation of 1G cellular system mainly used standards following:

- AMPS (Advanced Mobile Phone System) launched in the United States, is a network analog based on FDMA (Frequency Division Multiple Access) technology
- NMT (Nordic Mobile Telephone) was mainly designed in the Nordic countries and used in other parts of the planet.
- TACS (Total Access Communications System), which is based on AMPS technology, has been widely used in Britain.

This first generation of cellular networks using analog technology was replaced with the appearance of a more efficient second generation using a digital technology.

I.3.2 The architecture of the 2G

I.3.2.1 GSM network architecture

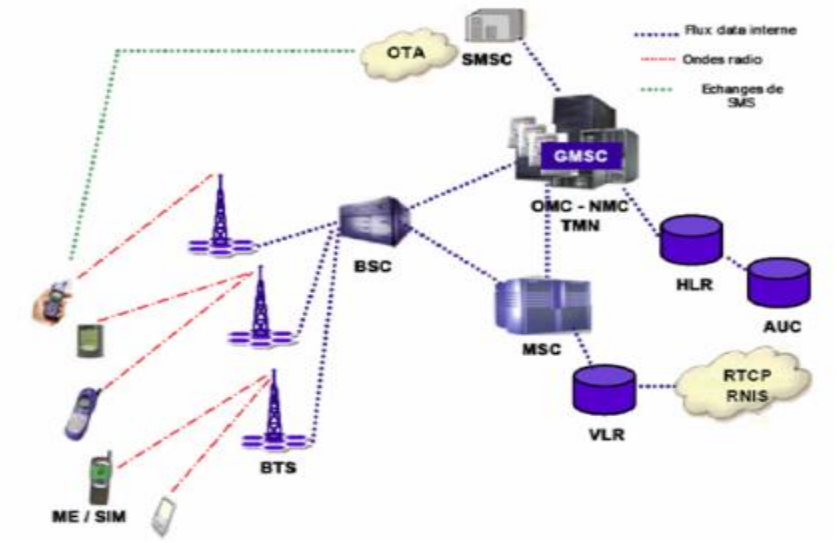

Figure I.2: GSM network architecture [3]

a) Base station (BTS-Base Transceiver Station): Ensures reception incoming and outgoing calls from mobile equipment.

b) The BSC-Base Station Controller: Ensures the control of base stations.

c) Mobile service switches (MSC-Mobile Switching Center): Ensures the switching in the network

d) HLR-Home Location Register: Database ensuring the storage of information on the identity and location of subscribers.

e) Authenticity Center (AuC-Authentication Center): Authenticates network terminals.

f) Register of visitor subscribers (VLR-Visitor Location Register): Database ensuring the storage of information on the identity and location of network visitors.

I.3.2.2 GPRS network architecture

A GPRS network is primarily an IP network. The network therefore consists of IP routers. The introduction of mobility also requires the clarification of two new entities:

- The service node - the SGSN.
- The gateway node - the GGSN.
- A third entity - the BG plays an additional security role.

The GPRS network adds a certain number of "modules" to the GSM network without changing the existing network. Thus, all the modules of the GSM architecture are kept.

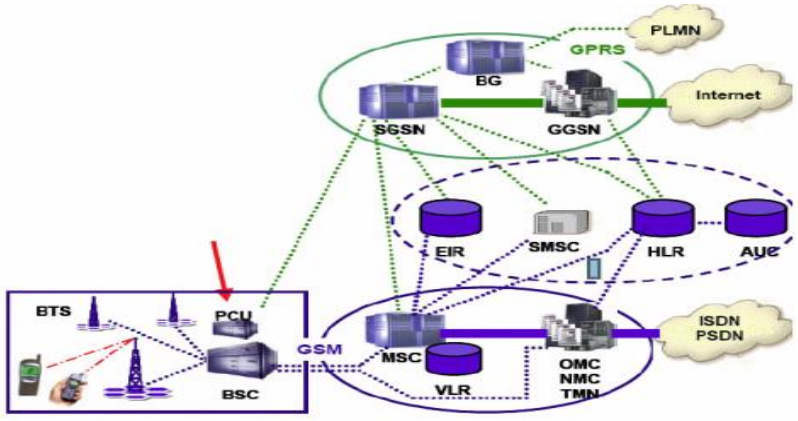

Figure I.3: GPRS network architecture[3]

I.3.2.2 EDGE network architecture

EDGE uses a different modulation from the modulation used by GSM, which implies a modification of base stations and mobile terminals. It thus makes it possible to multiply by a factor of 3 the data throughput with reduced coverage. In the EDGE theoretically achieves data rates of up to 384 kbit / s for fixed stations (pedestrians and slow vehicles) and up to 144 kbit / s for mobile stations (fast vehicles).

EDGE is an extension of the GPRS network. Only the radio subsystem is significantly amended.

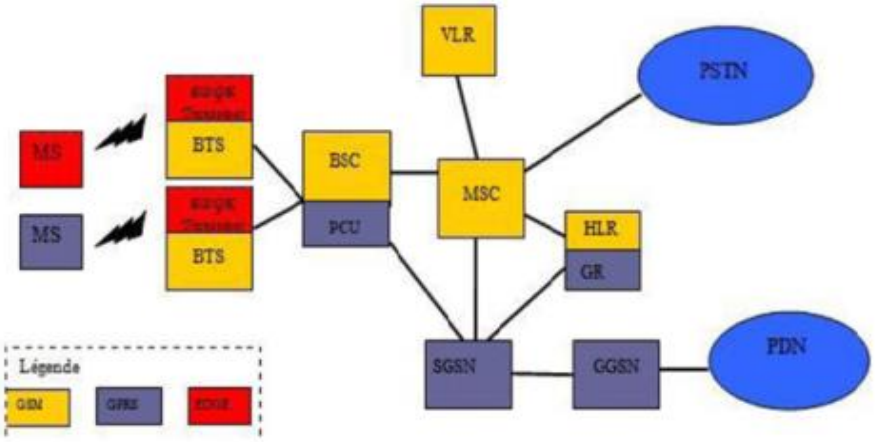

Figure I.4: EDGE network architecture

The deployment of EDGE requires:

- Updating the BSC and BTS.
- The addition of a transceiver (EDGE Transceiver) at the BTS level, capable of support 8-PSK modulation.[4]

I.3.3 The architecture of the 3G

The UMTS network comes to combine with the already existing networks GSM and GPRS bring respective functionalities of Voice and Data; the UMTS network then brings the Multimedia functionalities.

The founding idea of the 3G system is to integrate all second-generation networks around the world into a single network and to add multimedia capabilities (broadband for data).

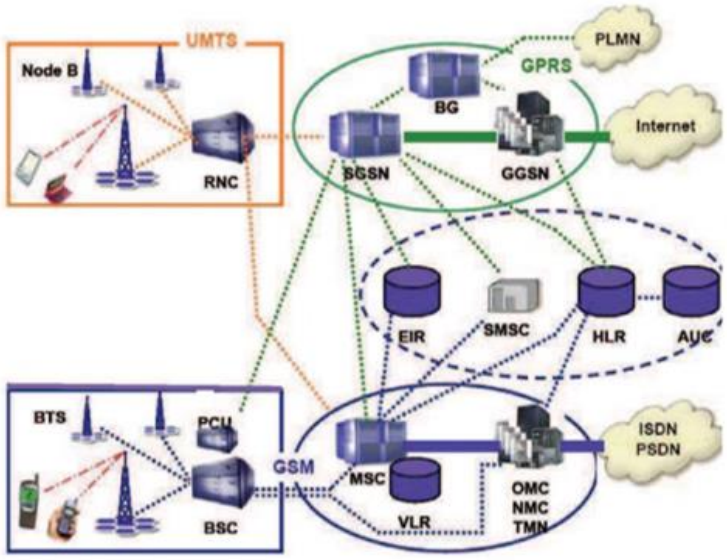

Figure I.5: 3G network architecture

a) "Node B" Node B is a set of base stations (BS) and site controllers which are also responsible for managing macro-diversity (1 mobile ↔ several B nodes). Each base station manages a cell. Several cells can therefore depend on the same Node B, but each cell supports only one duplexing mode: FDD (Frequency Division Duplex) or TDD (Time Division Duplex).

"Nodes B" manage the physical layer of the radio interface. "Node B" governs channel coding, interleaving, bit rate adaptation and spreading.

b) RNC The RNC is a Node B controller and is still here the equivalent of the BSC in the GSM network.

The RNC controls and manages the radio resources by using the RRC protocol (Radio Resource Control) to define procedures and communication between mobiles (through Nodes B) and the network.

The RNC interfaces with the network for packet and circuit mode transmissions. The RNC is directly connected to a Node B, it then manages:

- Load and congestion control (saturation) of the different Node B
- Admission control and code allocation for new radio links (entry of a mobile in the area of managed cells, etc.)

c) The USIM card The USIM card ensures terminal security and confidentiality of communications.

Public key encryption algorithms are used. There are a number of possibilities for 3G USIM cards (longer encryption keys, protection of subscriber and terminal identity data and others).

d) Mobile IT and telecommunications technologies come together through the integration of operating systems and applications on UMTS terminals. The

terminals will adapt to different networks and must be able to operate in four environments:

- In a rural area (Pico cell)
- In a building (micro cell)
- In urban spaces (macro cell)
- With a satellite [3]

I.3.4 The architecture of the LTE

The significant level system of LTE architecture is contained of three principle segments:

- The User Equipment (UE).
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
- The Evolved Packet Core (EPC).

The advanced packet center speaks with the packet information arranges in the outside world, for example, the web, private corporate systems or the IP media subsystem. The interfaces between the various pieces of the framework are signified Uu, S1 and SGi as demonstrated as follows:

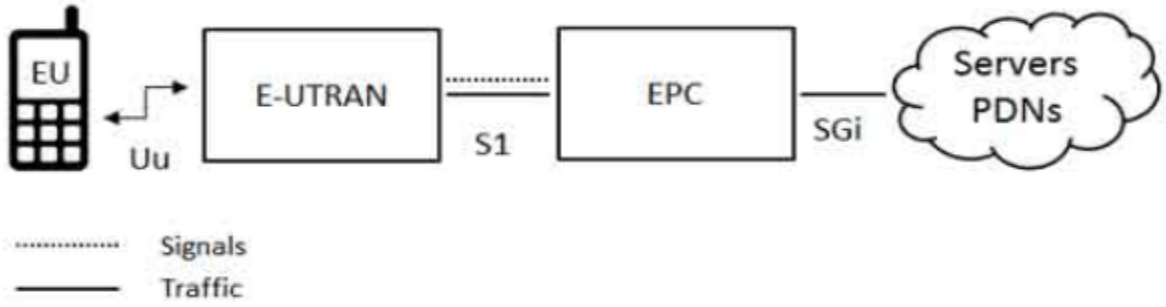

Figure I.6: Different Interfaces [21]

I.3.4.1 The User Equipment (UE)

The interior design of the client hardware for LTE is indistinguishable from the one utilized by UMTS and GSM which is really a Mobile Equipment (ME). The portable gear included the accompanying significant modules:

- **Mobile Termination (MT):** This handles all the correspondence capacities.
- **Terminal Equipment (TE):** This ends the information streams.
- **General Integrated Circuit Card (UICC):** also called the SIM card for LTE types of gear. It runs an application known as the Universal Subscriber Identity Module (USIM).

A USIM stores client explicit information fundamentally the same as 3G SIM card. This keeps data about the client's telephone number, home system personality and security keys and so forth.

I.3.4.2 The E-UTRAN

The design of developed UMTS Terrestrial Radio Access Network (E-UTRAN) has been represented beneath:

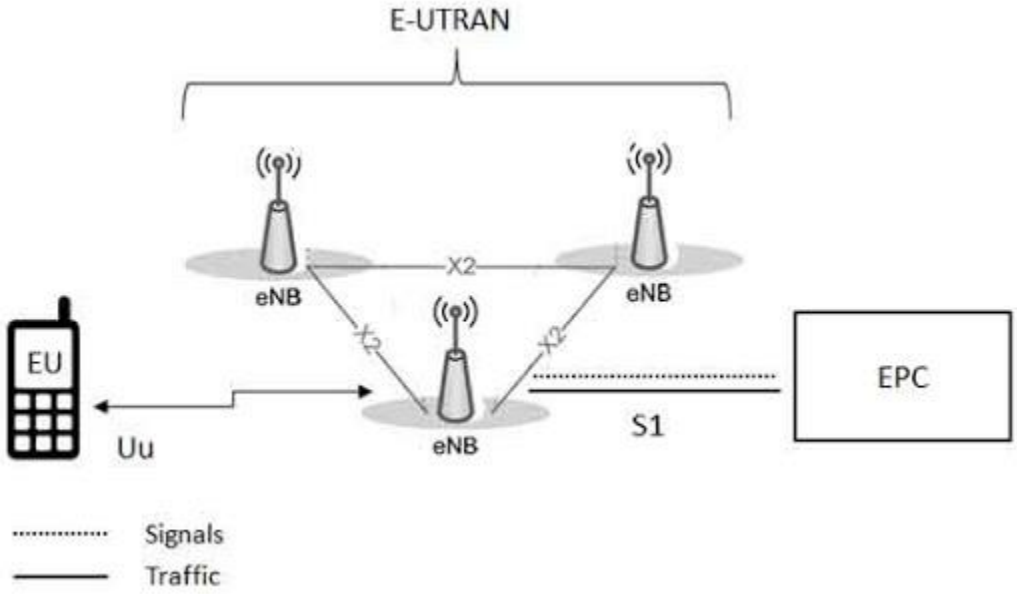

Figure I.7: The access network [21]

The E-UTRAN handles the radio correspondences between the cell phone and the developed packet core and simply has one segment, the evolved base stations, called eNodeB or eNB. Each

eNB is a base station that controls the mobiles in at least one cells. The base station that is speaking with a cell phone is known as its serving eNB.

LTE Mobile connect with only each base station and one cell in turn and there are following two primary capacities upheld by eNB:

- The eNB sends and gets radio transmissions to all the mobiles utilizing the simple and advanced sign handling elements of the LTE air interface.
- The eNB controls the low-level activity of every one of its mobiles, by sending them flagging messages, for example, handover orders.

Every eNB associates with the EPC by methods for the S1 interface and it can likewise be associated with close by base stations by the X2 interface, which is basically utilized for flagging and bundle sending during handover.

I.3.4.3 The Evolved Packet Core (EPC)

The engineering of Evolved Packet Core (EPC) has been represented beneath. There are scarcely any more segments which have not been appeared in the outline to keep it straightforward. These parts resemble the Earthquake and Tsunami Warning System (ETWS), the Equipment Identity Register (EIR) and Policy Control and Charging Rules Function (PCRF).

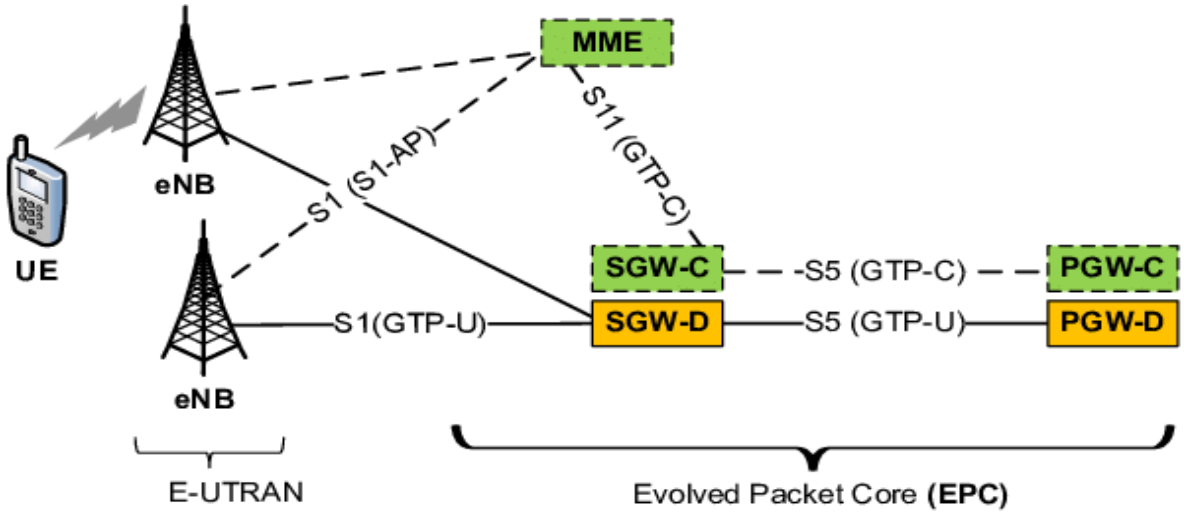

Figure I.8: The core network [21]

The following is a concise depiction of every one of the segments appeared in the above design:

- The Home Subscriber Server (HSS) part has been conveyed forward from UMTS and GSM and is a focal database that contains data pretty much all the system administrator's supporters.
- The Packet Data Network (PDN) Gateway (P-GW) speaks with the outside world. Packet data network PDN, utilizing SGi interface. Every PDN is distinguished by an access point name (APN). The PDN entryway has a similar job as the GPRS bolster hub (GGSN) and the serving GPRS bolster hub (SGSN) with UMTS and GSM.
- The serving gateway (S-GW) goes about as a router, and advances information between the base station and the PDN portal.
- The mobility management entity (MME) controls the elevated level activity of the portable by methods for flagging messages and Home Subscriber Server (HSS).
- The Policy Control and Charging Rules Function (PCRF) is a part which isn't appeared in the above chart yet it is liable for approach control dynamic, just as for controlling the stream based charging functionalities in the Policy Control Enforcement Function (PCEF), which dwells in the P-GW.

The interface between the serving and PDN doors is known as S5/S8. This has two marginally various usage, in particular S5 if the two gadgets are in a similar system, and S8 in the event that they are in various systems.[5]

I.4. Security and Mobility Issues in 4G LTE Network

I.4.1 Security Issues

Security conspires in remote correspondence have advanced in accordance with the development of remote advances. The various advancements have had their security frameworks developing from one phase to a more significant level. In 1G remote, it was feasible for interlopers or an outsider to increase false access to the system. 2G GSM had an improved security framework over 1G yet with a powerless improved security validation calculation. The ace security key could be unveiled by having a million associations with a SIM card.

In 3G remote system an upgraded procedure of a two-way validation instrument was received. Common verification was accomplished by the cell phone and system. For more grounded security, 128-piece encryption and honesty keys were used. Security was additionally improved

by acquainting a few components with guarantee freshness of the figure keys. It was shown by Horncand and Howard, (2000) that if a security key is undermined, the harm is restricted for that time of legitimacy of the key coming about to short instead of enduring impact.

Critical advances have been made to improve security issues from 1G through to 4G LTE remote systems. The 4G framework is an IP-based foundation and has an open nature. It has improved security component contrasted with 3G. A nitty gritty report in Seddigh et al, (2010) demonstrated that 4G utilizes transitory identifiers simply like the 3G yet further deliberation was utilized to limit the open door for interlopers to take identifiers contrasted with 3G.

By plan and method of activity the 4G systems is intended to cover a more extensive land region in which there are diverse working systems with their particular security plans. It is normal that the 4G will offer consistent support of these heterogeneous systems. Nonetheless, the heterogeneity of these remote systems leads to difficulties in security and protection. Vulnerabilities at either the physical or MAC (different access control) layers of the system might be ascribed to the difficulties introduced by these heterogeneous systems.

In another report, Barbeau (2005) referenced impedance and scrambling assaults as the two key vulnerabilities at the physical layer. Obstruction can result to correspondence framework disappointment because of a high SNR (signal-to-noise ratio) brought about by meddling signs in the type of white Gaussian Noise (WGN) and multicarrier (limited band signal), that are intentionally embedded into the framework. Scrambling is a progressively troublesome type of assault to actualize. This is on the grounds that a specific or some portion of the casings is the objective. To be fruitful, the aggressor must be learned and advanced to have the option to distinguish specific casings and schedule vacancies.

Verification, encryption and trustworthiness assurance are key security issues in 4G LTE with techniques recorded as:

- Freshness – The confirmation vector which is at the core of the validation methodology is destined to be new. i.e. not recently used. This is accomplished by means of the grouping numbers traded in the messages that fill in as contribution to the figuring and uprightness calculations.

- Security calculations - The calculations utilized in the HE (home environment) and USIM to process the validation vectors are generally one-way scientific capacities, where the yield is gotten with a given arrangement of information sources, utilizing a pre-characterized calculation. In this way, as clarify in Sankaran (2009), it is very mind boggling for an aggressor to attempt to get the data sources utilizing the outputs.

The security prerequisites of 4G heterogeneous systems have been characterized as having two levels. The primary level is on versatile hardware and the second is on Operator systems. Versatile gear prerequisites incorporate securing the gadget's trustworthiness, protection and classification, controlling access to information, and forestalling the portable hardware being taken or traded off and the information being manhandled or utilized as an assault device.

Besides, the encryption and cryptography strategies being utilized for 3G systems are not proper for 4G organizes as new gadgets, for example, advanced cells and opposite end-client gear (UE) and administrations are presented without precedent for 4G systems .Right now UE can likewise turn into a wellspring of malignant assaults .The utilization of the 3G's Authentication and Key Agreement (AKA) to a 4G correspondence engineering was examined by Aiash, Mapp, Lasebae and Phan, (2010) utilizing X.805 standard. Their investigation demonstrated numerous dangers to the system's security.

This demonstrated the present security dangers in 3G and other new dangers were inborn to 4G innovation. The movement to 4G which is a heterogeneous system, brings about receptiveness to cell assaults as well as web-based assaults.[8]

I.4.2 Mobility Issues

Mobility management is the essential innovation used to consequently bolster mobile terminals making the most of their administrations while at the same time wandering uninhibitedly without the interruption of interchanges. Mobility management was expressed by Payaswini and Manjaiah (2013), as extremely vital in 4G-Networks which is a heterogeneous system and progressively complex to deal with. This can occur in various layers of the OSI (open framework interconnection) model including system layer. These layers were given in Akyildiz, McNair, Ho, Uzunalioglu and Wang (1999) as layer-3 (L3), connect layer-2 (L2) and cross-layer (L3 + L2). The L2 mobility alludes to the situation where the Mobile Node (MN) wanders among various

access hubs while the purpose of connection to IP organize continues as before. The L3 portability includes the difference in IP addresses.

Portability remote system alludes to the MN staying associated as it changes same system area or between various systems. It is an instance of remain associated while on the move. Poor portability the board influences the nature of administration (QoS). It is an instance of encountering a disengagement as development advances between areas or systems.

Network issue was recognized in Tripathi, Kumar and Manrya (2014) to be either due to activating or handover issues. Activating happens when various types of occasions trigger portability activities prompting a few clashes. Handover or Handoff the board is a procedure by which a MN keeps its association dynamic when it moves from one passage to another. The procedure as appeared in Figure I.8 spotlights generally on the control of the difference in a versatile hub's passage during dynamic information transmission .4G systems are both multi-area and multi-innovation which present various difficulties on the grounds that the various advances included were planned with various degree of handover techniques.[6]

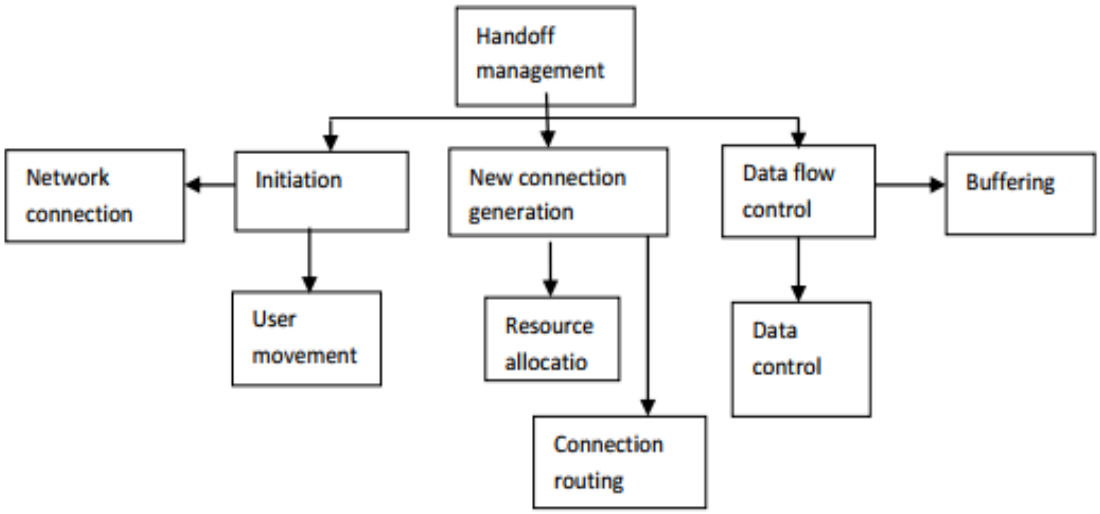

Figure I.9: Handoff management process

There are two degrees of handoff which are vertical and Horizontal handoffs. Horizontal handoff manages intrasystem handoffs while vertical handoff manages intersystem handoffs. The two degrees of handoff are bolstered by 4G framework.

Intrasystem handoffs are when MN moves between two distinct cells or passages inside a similar system. Right now, issues are bound to a similar system. Vertical handoff happens when more than one system is included, for example, when MN relocates from one system to an alternate system. Payaswini and Manjaiah, (2013), reasoned that it is hard to understand the vertical handoff among various remote correspondence frameworks while meeting suitable degree of QoS. This is on the grounds that drag out handoff time will result to loss of parcels or separations. The impact of handoff delay in 4G remote system was likewise featured in Rakesh, (2016) where it was communicated as a help challenge. They expressed that the client may encounter a drop in QoS which will influence the administration execution.

Terminal versatility which permits portable clients to unreservedly meander across topographical

limits of remote systems are likewise a part of portability challenge in 4G. Terminal versatility can be in type of area or handoff the executives. Not at all like the area the board which includes QoS issues, for example, verification data, data with respect to unique and new cells, the handoff the executives guarantee correspondence is continuous when the terminal wanders from a neighborhood system to a visited organize. The versatile Ipv6 address changes as the portable terminal leaves one system to another thus causes an expansion in framework load, high handover dormancy and bundle misfortunes. This outcome to framework corrupts and the QoS execution is influenced.

In the structure of handoff, the executive's strategies, the accompanying difficulties were recorded in:

- Reduction of both flagging and force overheads.
- QoS ensures during the handoff procedure – extraordinary low intra and intersystem handoff dormancy, which incorporates flagging message handling time, assets and courses arrangement delay, position change time, constrained interruption to client traffic, close to zero handoff disappointment and parcel misfortune rate.
- Efficient utilization of system assets.[7]

I.5. Conclusion

Mobile remote correspondences innovation has developed from 1G through 4G and step by step moving toward 5G to keep pace with the consistently expanding data transmission requests.

Security methods are set up to shield the present portable correspondence frameworks, anyway harder security systems are as yet fundamental for future systems. The 5G innovation will have a high information rate contrasted with 4G (LTE) and is required to be a blend of 2G, 3G and 4G (LTE) with more noteworthy inclusion and high unwavering quality. It is additionally expected to have a superior QoS than 4G because of an improved decrease in start to finish dormancy.

Subsequently, improved mobility management and harder security instruments are required which will be an enhancement for 4G frameworks. As another system, 5G will encounter new utilize cases and in this way will probably be presented to new types of dangers. Such dangers could be checked by having improved and strong inherent security systems.

The idea of security computerization ought to be considered. This will permit the system to act self-adaptive and self-healing utilizing canny security controls. These could be given on the foundation of SDN. The SDN empowered arrangement is equipped for not just giving a re-configurable system the executives stage, yet in addition rearranges confirmation handover in achieving decreased idleness. With the execution of VNT, fitting adaptability will be given in the determination of security for the distinctive system cuts in this way having a system with improved adaptability security choice instrument when contrasted with existing innovations.

Chapter II:

Mobility Management

II.1. Introduction

The start of wireless networks (1 and 2 generations) depend on circuit exchanged foundation, on non-IP based framework. These systems bolster voice and low information rate administrations, for example, short message administration (SMS).

Be that as it may, the air interface innovations of such systems are insufficient to help high information rate administrations, for example, media, gushing administrations, document move, and gaming.

Mobility management assumes a huge job in the current and the future wireless mobile networks in adequately conveying administrations to the portable clients moving. Mobility management is the fundamental innovation that supports meandering clients with mobile terminals to make the most of their administrations in progress through remote systems. From the perspective of usefulness, Mobility management empowers correspondence systems to Locate meandering terminals so as to convey information bundles, for example work for static situation, and keep up associations with terminals moving into new zones, for example work for dynamic situation.

II.2. Mobility Management Models of GSM/UMTS/LTE Systems

The mobility management organize reference model sums up the portability the executive's capacities, substances at a theoretical level. Based on this reference model, the mobility management elements and relating capacities in GSM/UMTS/LTE are characterized and condensed in Table II.1.

The mobility management elements of cell framework could be gathered generally in: radio access-related mobility management, location management, handover control.

The radio access-related mobility management work incorporates those capacities explicit at the radio interface and inside the radio system. In view of whether there is radio association among MS and the radio access arrange or not, those capacities could be additionally partitioned into mobility management in connected mode furthermore, idle mode. For MS in associated mode, handover system identified with radio layer (e.g., handover choice, readiness, and executions) and comparing information sending. For MS entering the idle model, the phone determination or

reselection ought to be performed by MS. The radio system likewise needs to booking and transmission of paging messages got from center network.

The location management alludes to those capacities primarily identified with center system and non-radio access layer, for MSs have no associations with arrange, i.e., idle mode. The enrollment, area refreshing, and reachability the board are three most significant capacities inside location management. Enlistment is the initial step performed by the MS after it is fueled on, during which the appropriate PLMN is chosen, and the MS got verified and approved by the system.

The motivation behind area refreshing is to keep the system refreshed where generally the MS found and keep the MS enlisted also. Where the MS is found is stopped an enormous enrolled territory contains numerous cells, where this zone is meant as area region, Routing Area and loads of tracking areas (TAs). The reachability management work is for the most part used to discover or "come to" the MS out of idle mode, if there is an ending call or information for it. The paging messages sent to every cell of MS's registered region are utilized to advise the MS that there is ending occasions for it. Such plan of over three capacities is an exchange off of expenses between sending those paging messages and area refreshing motioning, since per cell granularity area refreshing expends a lot of system assets. [9]

Table II.1 Entities, functions in GSM/UMTS/LTE networks based on mobility management network reference model

Network reference model	**GSM/GPRS**	**UMTS**	**LTE**	**Mobility management functions**
Access points	BSS, BSC	Node B, RNC, home Node B	eNode B, home eNode B	Radio access-related mobility management
Domain mobile controller	MSC, SGSN and GGSN	MSC, SGSN and GGSN	MME, SGW and PGW	Handover control, including gateway and user plane anchor functions
Location server	VLR, and HLR	VLR and HLR	MME, HSS	Location management
Registration server	HLR, AuC	HLR, AuC	HSS, AuC	User subscription data management.

The handover control is the procedure by which a correspondence is kept up while moving the versatile in the cell organize. This support is conceivable gratitude to the difference in the radio

channel utilized. The new divert can be in a similar cell, we talk then of an intracellular handover, or towards another cell, it is the intercellular handover.

The target of the handover is to keep up an adequate nature of correspondence between the versatile and the system through a difference in recurrence or cell. The handover permits in addition to other things to:

- Allow clients to move around during a call.
- Minimize interferences
- Optimize the utilization of radio assets.
- Balance the traffic load between cells.
- Reducing the vitality utilization of mobiles

The activating of the handover is connected to specific criteria called trigger pointers. Among them:

- The quality of the got signal. The base station consistently quantifies the quality of the sign got by the command post station, yet in addition tunes in to the base stations of neighboring cells; this is called handover helped by the system
- The separation. At the point when the versatile sees that it is a long way from its base station, and by accepting a more grounded signal from another phone, it advises its present base station; it is handover helped by portable

The present base station at that point chooses to hand over to the neighboring base station and actualizes the handover system.[10]

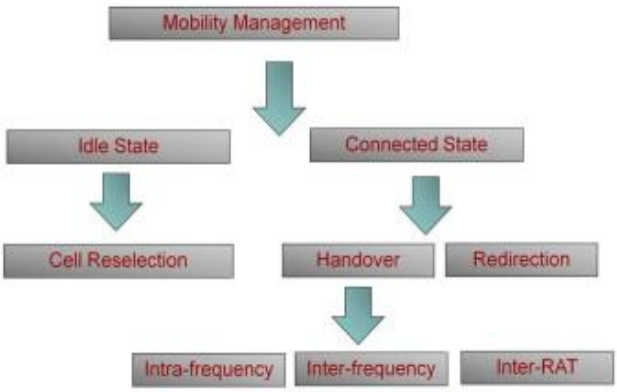

Figure II.1: Mobility Management [21]

II.3. Mobility Management in the Idle Mode

If there are no statistics to be dispatched or received, the MS would leave active mode, and goes into the idle mode, i.e., there no connections between MS and the community on account that such connections have been released.

When a MS powers on, it additionally enters into the idle mode firstly. Within the idle mode, the PLMN selection, phone selection, and reselection, region registration, and the supports for manual CSG phone decision are four principal duties from UE point of view Figure II.2.

Those 4 duties are all coordinate strategies between NAS and AS layer. For PLMN selection, the NAS selects a PLMN either routinely with the aid of making use of information saved on the SIM card associated to PLMN selection, e.g., a listing of precedence ordered entries, each contains a PLMN and one or extra radio get right of entry to technologies , or based totally on user's manual enter. Then, NAS requests the AS to choose a mobile that belongs to this selected PLMN. The NAS can additionally manage in which RAT(s) the mobile decision ought to be performed, through indicating those RAT(s) associated with the chosen PLMN to the AS layer. If such information is no longer provided, the phone choice is performed within the RAT(s) that the UE supported.

By detecting and synchronizing to a broadcast channel, the UE finds one or extra "PLMN identity" from the gadget information. Then, AS layer searches and selects an appropriate mobile if the idle-mode measurements end result of a mobile phone meets the mobile resolution criteria, e.g., for LTE, the measured cell acquires degree cost and nice fee meet that they are each greater than zero.

Once a suitable telephone is found, the UE chooses this cellphone to furnish reachable services, and further, the UE tunes to this cell's manipulate channel. This deciding on is recognized as "camping on the cell".

When camped on a cell, the UE is capable to acquire machine facts from the PLMN, e.g., registration vicinity facts such as monitoring vicinity identity of this mobile and transfers to linked if it has registered with the PLMN, receiving "paging" messages sent on manipulate channel.

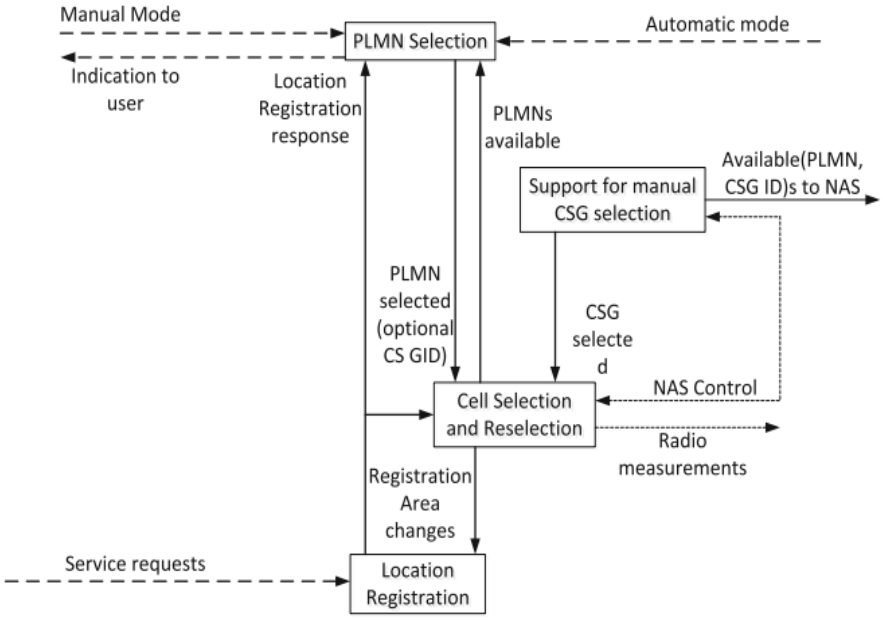

Figure II.2: Overall idle-mode process [10]

The location registration is the next technique if UE camped on an appropriate phone after it powered on. The UE registers its presence, by skill of a NAS registration technique to the selected PLMN. After a successful registration, the selected PLMN will become the registered PLMN, and the registration place where this process befell grew to become the registered registration vicinity of this UE. When camped on a cell, the UE shall normally search for a better phone according to the cellphone reselection criteria. Priorities between one-of-a-kind radio frequencies or RATs may be provided to the UE by using machine facts or dedicated signaling, and priorities-related standards may also be considered moreover in cellphone reselection process.

By placing suitable priorities, load balancing amongst exclusive frequencies/RATs ought to be completed at the radio layer. Thus, the reselected better phone might also belong to another

frequency/RAT which is extraordinary from that of present day camped mobile phone. Depending on UE's mobility state, some parameters are scaled to make the reselection extra reasonable. For example, both in high-mobility or medium-mobility state, the hysteresis price is adjusted hence for averting "ping-pong" reselections as much as possible.

The mobility nation is determined on how many times the reselection that UE performs two during a fixed period, as a substitute than its authentic mobility speed.

When UE is leaving linked mode, the Redirected Carrier Frequency perhaps gives by community to UE, and it is used to redirect the UE to an E-UTRA; or an inter-RAT carrier frequency is to be used with the aid of cellphone determination method upon leaving the RRC_CONNECTED.

The NAS is knowledgeable if the telephone (re)selection effects in changes in the received device records relevant for NAS in contrast to in the past gadget statistics which is stored locally, e.g., if the registration place is changed, which may trigger NAS to provoke the Location Registration procedures. Since having been registered, the UE initiates place update or routing place update, or tracking location update manner accordingly, which depends on the RAT of the reselected mobile phone and the provider, to replace its presence to its registered PLMN.

The CSG mobile is a mobile phone that broadcasting a particular CSG identification and only grant get right of entry to users belongs to the CSG identified with the aid of the same identification if such CSG cells function in close mode. Normally, a cellphone operated with the aid of domestic eNodeB acts as a CSG cell, for a precise group of users. CSG cells are candidate cells as properly as different non-CSG cells for regular mobile decision and reselection process, if the UE has the permission to get right of entry to such CSG cells. The manual CSG mobile phone decision approves the quit user to pick a CSG and an associated PLMN. The AS first scans and affords available CSG cells' CSG identities and associated PLMNs to NAS, then such identities would be displayed to user. Based on user's choice of a CSG, NAS requests AS to select a telephone belonging to this CSG.[11]

II.4. Mobility Management in the Connected Mode

II.4.1 The Handover

II.4.1.1 Handover Types

There are different kinds of handovers, which can be classified in various ways.

- Horizontal (i.e. intra-technology) handover – Handover between the same access technologies
- Vertical (i.e. inter-technology) handover – Handover between the different access technologies

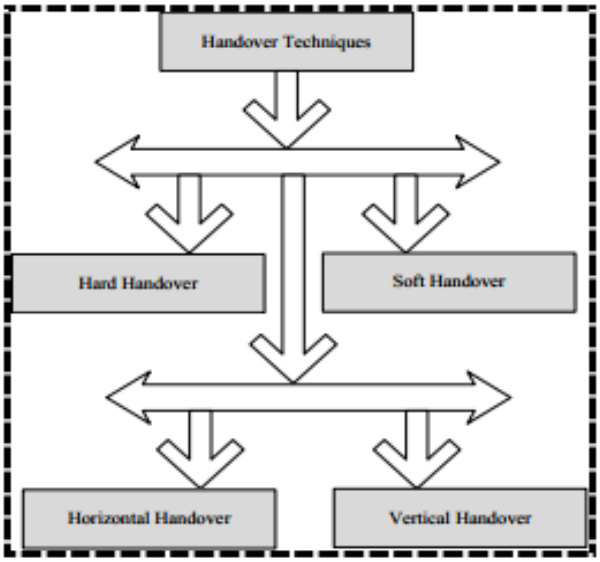

Figure II.3: Classification of Handover [21]

Handovers can be additionally divided into L2 and L3 handovers based on the protocol layers worried in the handover process. In a L2 handover the IP settings do not exchange at some point of the handover, consequently only link technological know-how-based handover techniques are needed. When IP subnet modifications due to AP change, also IP reconfiguration is wished. For instance, Mobile IPv6 can be utilized for the L3 handover.

Hard and Soft handover refer to whether or not the mobile node loses connection to the network for the duration of handoff or not, respectively.

- Hard handover – During a difficult handover there is a period of time when the cell node has no connection to the community at all. When making the handover, the node disconnects from its old link and reconnects at the new one. It can take place in a case when the mobile node has e.g. solely a single network interface. Usually a node can now not be

related to a couple of hyperlinks or Access Points at the identical time by means of the equal community interface.

- Soft handover – When the cellular node makes a handover except at any time being definitely offline, then we talk about smooth handovers. To operate this, it is very probably that more than one community interfaces have to be existing at the cell node.

During handover, packet loss is likely to manifest and one of the essential dreams of mobility management protocols is to decrease this packet loss. In make-before-break handover the cellular node is aware of before that it will soon come upon a tough handover, consequently it might also perform some steps earlier than breaking the connection at the old link. Otherwise, at the new link the cellular node would need to perform too many steps earlier than it can set up a working IP configuration, which would end result in lengthy delays and huge packet loss. The latter sort of handover is known as break-before-make. The intention is to provide seamless handover, the place top layers ride minimal disruption.[12]

II.4.1.2 Handover Control Within CS Domain

In Figure II.4, an inter-MSC handover technique with GERAN is shown, which takes place inside CS domain. When a cell terminal initiates a voice call, say to a POTS terminal, the MSC/VLR that serves this cellular terminal takes full control of this call, e.g., name setup, charging thing and handover control. This MSC is referred anchor MSC, and this anchor MSC would now not change due to consumer mobility and stays unchanged until this name finished.

Once the supply BSC decided that a handover is needed, it sends handover required message to MSC (step 1), with target mobile identity included. If the MSC determined out that target cellphone is managed with the aid of some other MSC (e.g., MSC_B in this case), a function handover message is been sent to this goal MSC (step 2). The target MSC prepares radio channel (step 3, 4), and units up connection for speech between anchor MSC and itself (step 6). Once succeed the anchor MSC problem a handover command to supply BSC and cellular terminal (step 7, 8). The cellular terminal would handover to target phone after receiving such command. Once the handover is detected by goal BSC, the target BSC notifies target MSC, and target MSC then notifies the anchor MSC (step 10, 11). The anchor MSC then switches voice move to goal MSC and releases radio and community useful resource related to this call at source side.

During the procedure, a handover range (HON) is allotted by way of goal MSC for this cellular terminal. The HON is used with the aid of supply MSC to route call-related signaling and establishes speech connections between MSCs. After this simple inter-MSC handover, if this cell terminal with one ongoing voice calls is going to pass into another telephone managed with the aid of to a third MSC, say MSC_C, a subsequent inter-MSC handover would be performed. In such case, the BSC sends a handover required message to MSC_B, with goal cellphone identity. The MSC_B figures out that goal phone belongs to MSC_C, and then MSC_B ship the function handover message to the anchor MSC. The anchor MSC will contact MSC_C for fulfill this further handover procedure.

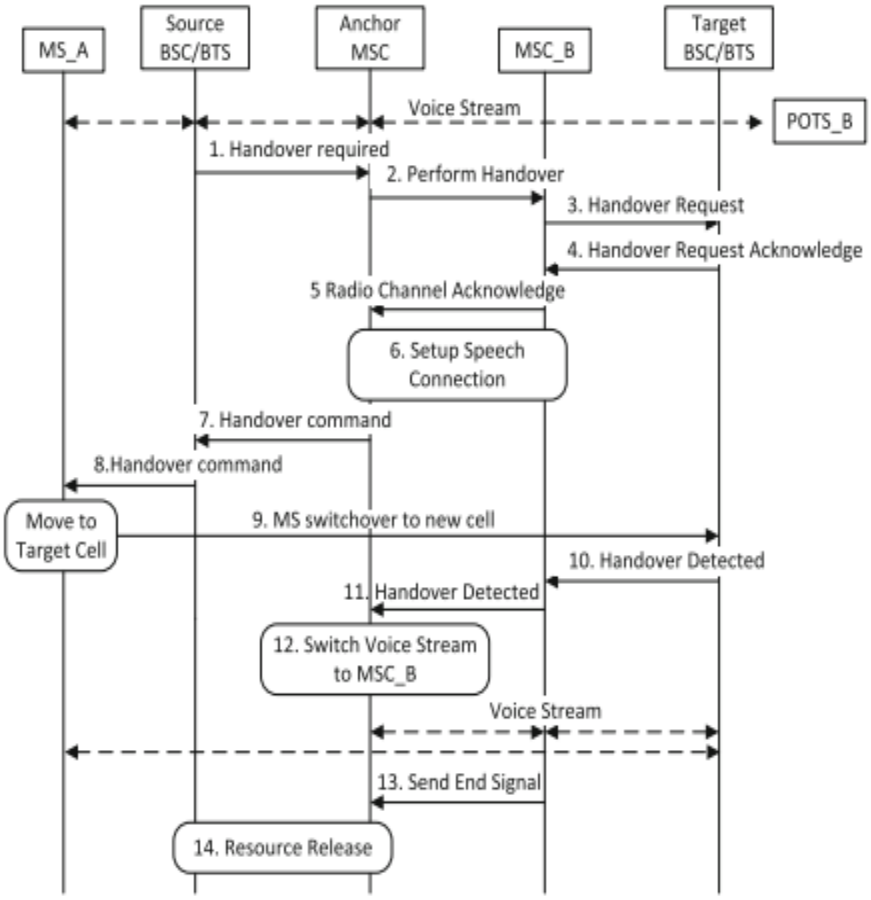

Figure II.4: Inter-MSC handover procedure.[13]

II.4.1.3 Handover Control Within PS Domain

1- PS Handover

Packet-switched (PS) handover is first of all added for GERAN, which is used to handover a cellular terminal with one or more packet flows from a supply mobile phone to a goal cell, the place at least one of the cells is a GERAN telephone. During this procedure, real-time packet switching with strict QoS requirements on low latency and packet loss are supported through the "make-before-break" approach.

Depending on the areas of supply and goal cell, PS handovers are classified into intra-BSS HO (located inside the identical BSS), intra-SGSN HO (within one-of-a-kind BSSs and belong to the identical SGSN), and inter-SGSN HO (within unique BSSs and belong to unique SGSN). If source and goal cell use exceptional radio get entry to types or use unique type of interface join to core network, then this is an inter-RAT/mode HO. All these HO manners consist of a preparation phase and an execution phase.

One traditional system of inter-RAT/mode and inter-SGSN handover, GERAN A/Gb-mode to UTRAN/GERAN Iu-mode handover, is shown in Figure II.5.

During training phase, source BSS decides and notifies 2G-SGSN a PS handover is required with Target RNC Identifier, supply telephone identity, a Source RNC to goal RNC transparent container, energetic packet flow Context lists (step 1, 2). Based on the goal RNC identifier, 2G-SGSN figures out that this is an inter-SGSN handover and similarly determines the target 3G-SGSN and sends ahead relocation request to this 3G-SGSN with MS context blanketed (step 3).

The 3G-SGSN reserves useful resource at goal aspect then return ahead relocation response with following parameters, SGSN addresses, and tunnel endpoint identifiers for both manipulate plane and user plane (for , those addresses and identifiers are used by using 2G SGSN to ahead data all through the handover procedure), target RNC to Source RNC container, to old 2G SGSN (step 6). Once received the response, 2G-SGSN considers training phase is finished (point a), and acknowledges source BSS, to let it command mobile terminal pass to goal mobile (step 7).

Within the handover command sent to terminal, target cell-related information is included, such as radio assets allotted in goal cell, device facts wished for get right of entry to the target cell (step

8). At the identical time, 2G-SGSN duplicates downlink packets despatched to source BSS and send them to 3G-SGSN. The 3G-SGSN sends these packets to goal RNC/BSS, and RNC/BSS may additionally start blind transmission to terminal on these allotted resources. For these packet waft requires ordered delivery, ancient 2G SGSN notifies 3G SGSN the sequence numbers of the GTP-PDU subsequent to be transmitted in the uplink and downlink course in Forward SRNS context message (step 9). After the ahead SRNS context message is despatched to RNC/BSC, similarly uplink N-PDUs received by way of the ancient 2G SGSN from the source BSS would no longer be forwarded to the GGSN.

After understanding that terminal has done the handover to goal phone via receiving handover whole message, the RNC/BSC shows (step 14) the completion of the relocation, and then, 3G SGSN is geared up to obtain uplink packets from goal RNC/BSC. If acquired any uplink packets from RNC/BSS, the 3G SGSN forwards these packets direct to GGSN. After notifying forward location entire to ancient 2G SGSN (step 15), the ancient 2G SGSN begins a timer after sending back acknowledgment. Upon the expiry of this timer, the historical 2G SGSN stops forwarding packets to the new 3G SGSN.

The new 3G SGSN sends an update PDP context request to GGSN after receiving acknowledgment from 2G SGSN. If direct tunnel is used in the course of instruction phase, RNC/BSS addresses and tunnel endpoint identifiers and a DT flag would be furnished to GGSN, as a substitute of the new 3G SGSN addresses and tunnel endpoint identifiers, in this request message (step 17). After response this request, the GGSN forwards downlink packets to both RNC/BSS if direct tunnel is used or 3G SGSN, alternatively of 2G SGSN.

If has been handover to a new routing area, the terminal should provoke the routing place update manner (step 19). By the usage of direct tunnels, the packet switch delay is reduced, packet forwarding from historic 2G SGSN to new 3G SGSN and ordered transport characteristic avoids packet losing and ensuring in-sequence packets shipping at some stage in the handover procedure.[14]

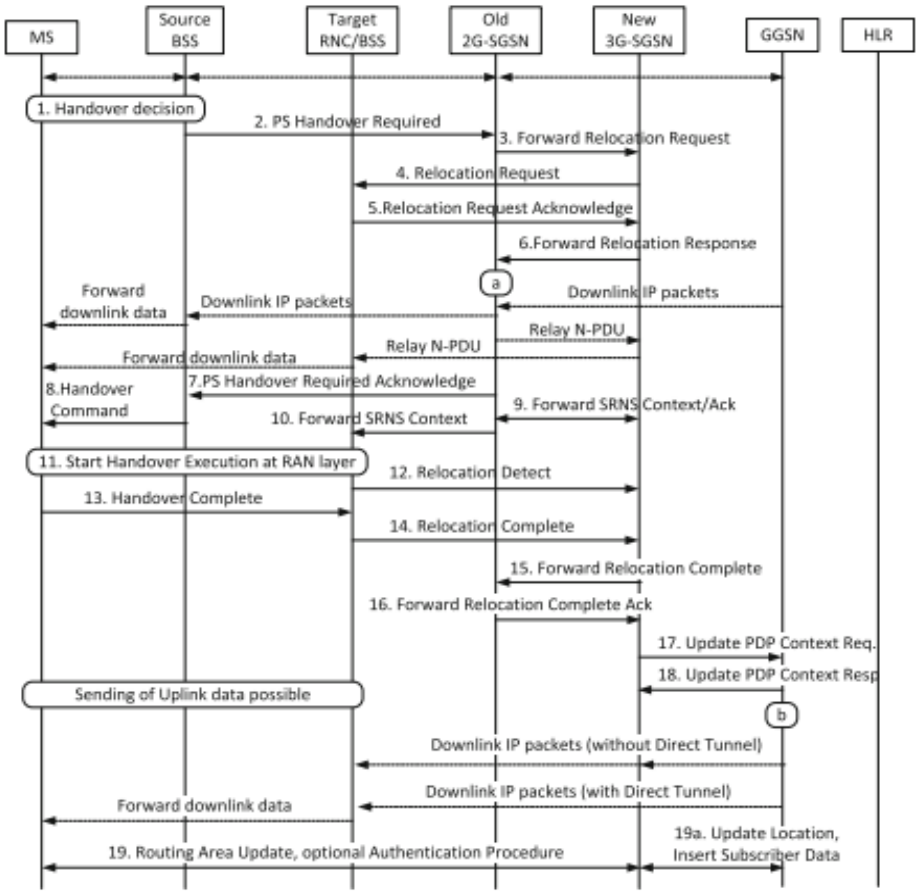

Figure II.5: Inter-RAT/mode handover procedure, from GERAN to UTRAN [13]

2- S1 Handover

The S1-based handover is used when the X2-based handover cannot be used, e.g., the goal eNodeB has no connection with the supply eNodeB, or the supply eNodeB knows that the X2 handover is no longer feasible or allowed primarily based on local configuration, or after a failed X2 handover to the goal eNodeB and etc.

It is supply eNodeB who determine coming near handover is an X2 handover or an S1 handover based on above facts upon receiving the terminal's measurement file (step 0) Figure II.6.

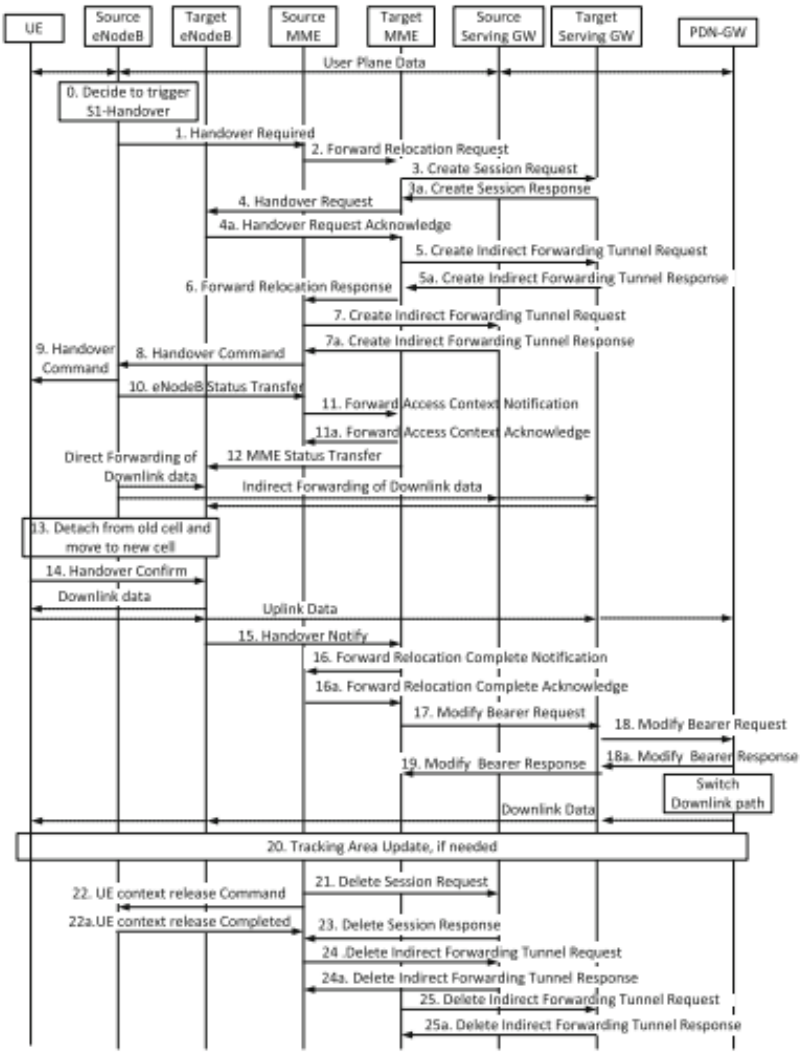

Figure II.6: S1 handover, with MME change and/or Serving GW change [13]

S1 handover system on LTE side is also used when the source get entry to system is GERAN or UTRAN and the goal access device is LTE.

The supply MME based totally on the received target cell-related information in step 1, such as target eNodeB identity, goal tracking place identity, to figure out whether or not to select a new MME. The supply MME selects a target MME that serves the target monitoring area, if the source MME could not serve this terminal or the target monitoring place (step 2).

When the target MME finds out that the source Serving GW cannot proceed to serve the terminal, it would choose a goal Serving GW based totally on community topology, which should limit the

likelihood of changing Serving GW in the future. The supply MME can also additionally select a new Serving GW if the supply MME continues to serve this terminal.

If a new Serving GW is relocated, assets for tunnels between the goal eNodeB and the goal Serving GW are reserved (step 3), e.g., the Serving GW addresses and tunnel endpoint identities for each bearer to be used for the uplink traffics are back to MME (step 3a).

The MME requires target eNodeB to prepare bearer resource (step 4). The Serving GW address and tunnel endpoint identity for every bearer to be set up, and corresponding QoS parameters are indicated to target eNodeB. The goal eNodeB returns which bearers have been set up correctly and which have now not to MME (step 4a). For those bearers have been setup, the eNodeB tackle and tunnel endpoint identification used for downlink traffics for each bearer are additionally signaled. There is a small-time duration between the source eNodeB sends handover command (step 9) to terminal and PDN GW switches downlink information switch to goal Serving GW (right after step 18a). During such period, downlink records are nonetheless sent to source eNodeB. For these bearers (decided with the aid of eNodeB) that carriers consumer facts requiring lossless and ordered delivery, statistics forwarding of downlink information is performed. Direct forwarding tunnels between source and target eNodeB have to be set up and used if it is possible. Otherwise, the supply eNodeB suggests this to MME in step 1, and oblique forwarding need to be used instead. If MME determined to use indirect forwarding, then tunnels for oblique forwarding are set up from source eNodeB to target eNodeB, with the aid of source Serving GW and by goal Serving GW if Serving GW is relocated. The node addresses and tunnel identifiers of such tunnels are signaled in step 4a, 5, 5a, 6, 7, and 7a. The oblique forwarding tunnel for downlink data, with and barring Serving GW relocated, is shown in Figure II.7.[13]

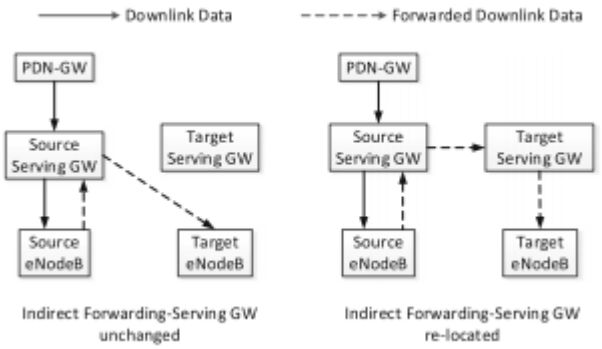

Figure II.7: S1 handover, showing indirect forwarding path for downlink data

To fulfill lossless and in-order delivery (i.e., PDCP status preservation) for user facts subject to indirect forwarding, the source eNodeB sends an eNodeB fame transfer-related records such as PDCP and HFN repute of those radio access bearer to facilitate PDCP repute protection (step 10 to 12).

After confirming that a terminal has moved to goal side, the target eNodeB starts offevolved forwarding acquired forwarded statistics from the supply side and notifies MME that the terminal has finished the handover to the goal eNodeB. Upon receipt of such confirmation (step 16), the source MME (regardless having been relocated or not) begins a timer to supervise when resources in source eNodeB and resources in source Serving GW (if relocated) shall be released. If MME is relocated, the target MME additionally starts offevolved a timer to supervise sources for indirect forwarding at the goal side. The length of the timer is chosen cautiously to ensure that such resource releasing only takes place after this useful resource is now not needed. On the expiry of such timers, step 21 and 25 are performed, respectively, such sources at the source facet and goal aspect would be released.

The MME replace bearer-related information, such as goal eNodeB addresses and tunnel endpoint identities, is used for downlink visitors of those widespread bearers (by target eNodeB) to a Serving GW (step 17). For these non-accepted bearers, MME releases them through triggering the bearer release procedures. If the Serving GW is relocated, the target Serving GW replace bearer records with PDN GW (Step 18). Such facts consist of goal Serving GW assigned Serving GW addresses and tunnel endpoint indenters for each bearer (for both accepted and non-accepted). Then, PDN GW switches downlink facts transfer to a new path, i.e., starts sending down hyperlink records to the goal Serving GW, and sends “end marker” packets on old downlink course as soon as the switch is completed, to notify source eNodeB that there is no greater downlink packet coming. The Serving GW sends it assigned Serving GW addresses and tunnel endpoint indenters for uplink visitors to the goal eNodeB (step 19). If the Serving GW is not relocated, this Serving GW sends “end marker” packets on old downlink direction once it starts sending downlink packets to the target eNodeB.

The terminal initiates monitoring location update method at target facet if it detects that it has entered a tracking vicinity which is now not in its saved TAI list, or different conditions for initiating this method are met (step 20).

The source eNodeB may also cancel the handover method at any time earlier than commanding terminal to cross to goal cell. And if none of the bearers requested through the supply facet should be set up at the target side for the duration of the practise phase, the goal eNodeB rejects this handover.

3- X2 handover with Serving GW relocation

During X2 handover, MME is unchanged but Serving GW is changed to a new one, Figure II.8. The handover guidance and execution of this manner are equal as these X2 handover besides Serving GW relocation.

The MME decides that Serving GW should be relocated to a new one after receiving route switch request from the target eNodeB (step 1). Afterward, person plane tunnels for every bearer at the goal aspect are mounted from step 2 to 5, which is comparable to that of S1 handover with Serving GW relocated procedure, as well as the identical downlink packets coping with of the PDN-GW for both procedures. Uplink statistics from terminal may additionally be received and forwarded to source Serving GW, by means of goal eNodeB, before receiving direction switch acknowledgment (step 7). Once received, the goal eNodeB sends uplink user facts to target Serving GW. This is why the IP connection between goal eNodeB and source Serving GW need to be introduced for this procedure. Otherwise, S1 handover is used instead.

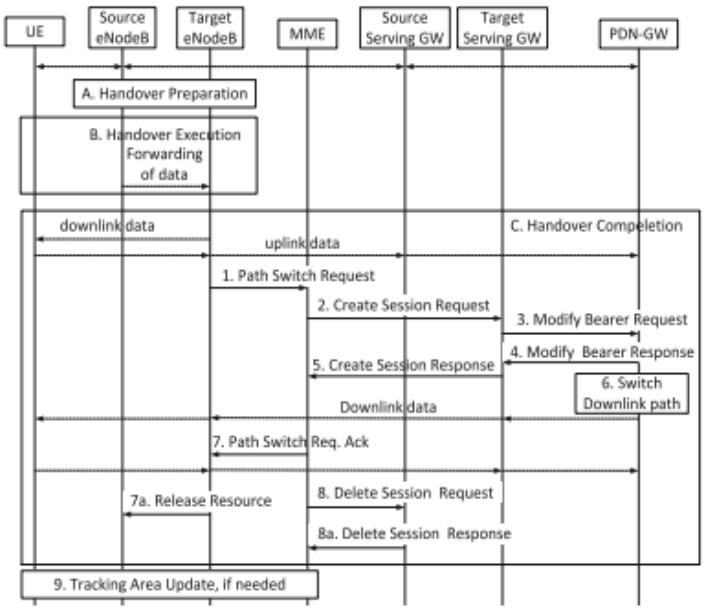

Figure II.8: X2 handover, with Serving GW change

II.5. Conclusion

After the above, we gave an overview of the mobility management and its models in the various systems (GSM/UMTS/LTE), also we gave a comparison on the various entities and how they work based on the reference model for mobility management.

After that the mobility management divided to three element ; the mobility , the location and the handover management , we deepened the mobility management in both modes (idle and connected mode) while the idle mode used for reselection and the connected mode for the handover , also we mentioned a lot of the handover techniques specially in the LTE (S1 , X2 handover).

With the huge increase in users and given the importance of mobility management in giving the optimal experience in the service and with the emergence of problems in the fourth generation in terms of mobility and protection led to the emergence of the fifth generation network to contain the largest number of users and with the solution of problems in the previous generation to give the best possible service

Chapter III:

5G & Mobility Management

III.1 Introduction

The worldwide economy and the global society are becoming increasingly dependent on information and communication technologies, especially on wireless connectivity which leads us to the fifth generation of wireless networks. The 5G will allow for new applications and unique service capabilities, also a whole new experience in term of speed, quality of service and more.

Nonetheless, to make it happens a huge transformation must be applied Based on an innovative architecture, which can scale and adapt to future needs, and a new radio interface, 5G will provide significantly better performance and new capabilities.

In this chapter we are going to cover Why 5G? What are the new technologies(pillars) of the fifth generation? What is the new architecture? And What is the mobility management presented in the 5G?

III.2 Why 5G

III.2.1 Definition of 5G

5G is the fifth technology wireless technology for digital cellular networks that started broad deployment in 2019. As with preceding standards, the protected areas are divided into regions referred to as "cells", serviced by means of character antennas. Virtually every principal telecommunication service provider in the developed world is deploying antennas or intends to installation them soon. 5G envisages now not solely one invented technology, however a science ecosystem of wireless networks working in synergy to provide a seamless verbal exchange medium to the give up user.[15]

III.2.2 The new services provided by the 5G

4G used to be designed to improve capacity, consumer data-rates, spectrum usage and latency with admire to 3G. 5G ambitions at being much extra than a simple evolution of 4G, as it will be a key enabler of the future digital world, the subsequent generation of ultra-high broadband infrastructure that will guide the transformation of procedures in all financial sectors and the developing customer market demand. This is reflected in ITU-R’s defined objective for IMT-2020:

“Enabling a seamlessly connected society in the 2020 timeframe and beyond that brings together people along with things, data, applications, transport systems and cities in a smart networked communications environment”

In fact, 5G is designed to create the conditions to launch new applications and supply new unique service capabilities not solely to consumers, but also to new stakeholders (e.g. vertical industries, novel types of provider providers, infrastructure owners and providers).

Firstly, 5G will make sure unprecedented consumer journey continuity also in challenging situations. For example, HD video will be not unusual and available anywhere, teleworking will be possible additionally for these residing in small villages or traveling in high speed trains and airplanes. 5G systems will supply consumer get right of entry to anywhere and will pick out transparently for the consumer the nice performing gets right of entry to amongst the various available ones, based totally on heterogeneous technologies like WLAN, satellite, 4G and the new radio (NR) supplied through 5G. The desire of the best performing gets right of entry to will now not solely be based on throughput however on the most applicable metrics relying on the nature of the service; for instance, the proper balance between latency and throughput is very essential for an Augmented Reality (AR) consumer transferring around.

Secondly 5G will additionally be a key enabler for the Internet of Things (IoT), by way of providing the platform and services to join and accurate operate a large variety of objects. To make excellent use of the newly provided services of 5G, the surroundings in which we cross will have sensors and actuators spread everywhere. Since they require very low energy consumption to shop battery lifetime, the future community will have to locate tremendous methods to take care of a large number of objects requiring a quite dynamically changing amount of small energy. Objects, users and their private networks, whether body-worn or in a household, will be producers and buyers of data. Future smart phones, drones, robots, wearable devices and different clever objects will create neighborhood networks, the usage of a multitude of different get entry to methods. 5G will allow all these objects to join seamlessly and independently of a precise get admission to community technology.

Furthermore, quite a few mission-critical services will be natively supported by the 5G infrastructure, thanks to the extraordinary reliability and achievable-on demand low latency. 5G will cowl services which had been dealt with the aid of unique networks for reliability motives

such as public safety. It will additionally cover new services requiring real-time reactivity, such as vehicle-to-everything (V2x) verbal exchange offerings and industry functions (e.g. technique automation), paving the way closer to stronger self-driving cars, a whole lot of greater advanced manufacturing unit automation or remote fitness services.

Figure III.1: 5G new service capabilities

As a conclusion, 5G will effectively support the three cited different types of visitor's profiles, namely, high throughput (e.g. for video services), low power (e.g. for long–lived sensors) and ultra-reliable and low latency (e.g. for mission-critical services). In addition, the 5G infrastructure will cowl the community needs and contribute to the digitalization of vertical markets such as automotive, banking, education, metropolis management, energy, utilities, finance, food and agriculture, media, government, healthcare, insurance, manufacturing, actual estate, transportation and retail.[16]

III.2.3 5G enhanced performance

5G is mandated to drastically amplify the handy communication machine performance, according to numerous system parameters and Key Performance Indicators (KPI). As encouraged via ITU-R, 5G is consequently now not solely anticipated to be disruptive but additionally to act as an economy booster by using fostering the advent of:

- new offerings that will positively affect essential societal aspects.
- new approaches to capture business opportunities, especially for the new service providers.
- new enterprise fashions supported through superior ICT technological know-how enablers.

The 5G structure and its underpinning technologies will enable the usage of community functions and assets that are tailored to optimize specific services. Furthermore, permitting for even more advanced sharing infrastructure and spectrum capabilities.

Those capabilities will supply ubiquitous get entry to a large range of functions and services, and will allow for improved resilience, continuity, tons higher resource efficiency, and an average considerable decrease of system electricity consumption. At the same time, 5G will amplify the stage of safety and privateness of future communications. In addition, 5G will supply huge upgrades in ability and raise consumer facts rates. For instance, height facts fees up to 10 Gb/s will be available. A potential of 10 Gb/s/km² will be required to cover, e.g., a stadium with 30,000 gadgets relaying the match in social networks at 50 Mb/s. Moreover, reduced end-to-end latencies of the order of a millisecond are wanted to assist immersive interactive applications and make sure ultra-responsive cellular cloud-services.

Besides the human-centric applications, some of which have been outlined above, it is expected that a broad variety of Internet of Things (IoT), large Machine-Type Communication (mMTC) and especially Ultra-reliable Low Latency Communications (URLCC) applications will be mainstream by using 2025.

The capability of the telecommunication machine to fulfil the numerous and various new necessities coming from the above-mentioned purposes and the 5G system verticals will require necessary changes to the currently defined and applied structure elements of cell systems.

Figure III.2, taken from the ITU-R, record “enhancement of key capabilities”, compares current and imminent device parameters and KPIs and highlights the predominant benefits expected from 5G. It is important to spotlight that no longer all of the better competencies described above will be required by every 5G service, in all places and all the time. Each connected machine will usually have its combine of latency, bandwidth and site visitor’s intensity requirements. Also, each connected vicinity will have its specific characteristics: the community will now not furnish the equal insurance for a commercial enterprise district, a stadium, a residential area, or on board a vehicle. This is why the infrastructure has to be enhanced so to be flexible and able to dynamically adapt itself to the characteristics of the unique carrier demand expected in that unique area. 5G is therefore predicted to provide, for instance, extended coverage for mMTC offerings and excessive bandwidth for eMBB services.

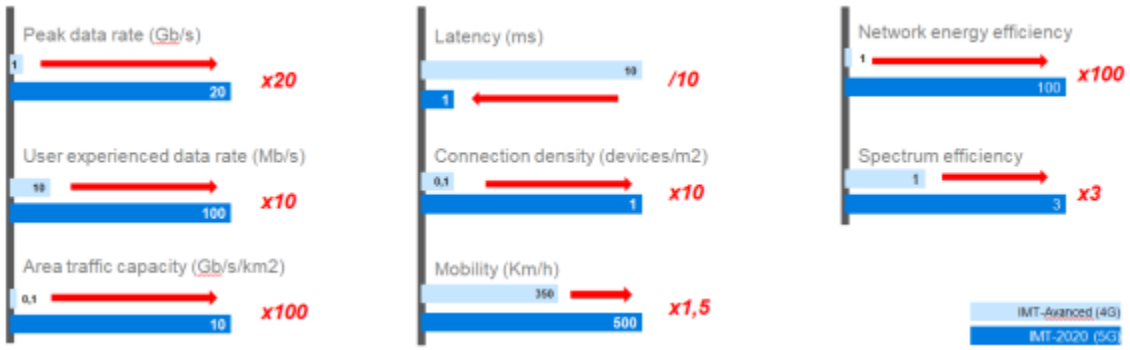

Figure III.2: IMT-2020, enhancement of key capabilities [16]

Radio based totally services count on regulated access to electromagnetic spectrum, only at unique frequencies. In order to supply very excessive normal gadget capacity, so to fulfil the new 5G provider requirements, especially the eMBB ones, it is required to make use of very large contiguous service bandwidths, from hundreds of MHz up to quite a few GHz. That will be possible, if contiguous frequencies are to be used, only thanks to higher provider frequencies, i.e. well above 6 GHz, in the decrease millimeter wave spectrum.

III.3 5G network architecture

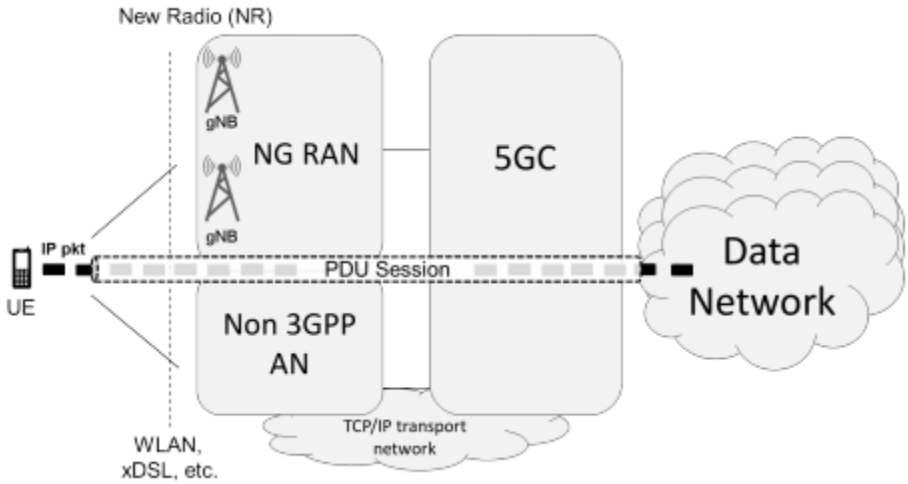

Figure III.3: 5G Network Architecture [17]

The fifth-generation network consist of a 5G access network (AN) and a 5G core network (5GC) Which is shown in Figure III.3. The access network itself is compose of a new-generation radio

access network (NG-RAN), which uses the 5G new radio interface (NR), and a non-3GPP AN (e.g. WiFi, xDSL, etc.) all connecting to a 5G core network.

The different network entities are connected by an underlying TCP/IP transport network, which supports diff-serv QoS.

III.3.1 New Generation Radio Access Network (NG-RAN)

As shown in Figure III.4, the NG-RAN consists of a set of 5G base stations, referred to as gNBs, which are related to the 5GC through a set of logical interfaces. As in LTE, gNBs can be interconnected through the Xn interface to improve mobility (e.g., handover) and management functions (e.g., inter-cell interference coordination).

The performance of a gNB is from time to time distributed. In that case, the resulting architecture is formed by way of a central unit (gNB-CU) that controls one or extra distributed units (gNB-DU) via the F1 interface. A dispensed unit is related to a remote radio head (RRH), i.e., the authentic radio transceiver. The central unit is once more break up in two parts, one for control plane functions (gNB-CU-CP) and one for user plane functions (gNB-CU-UP), following the control and user plane separation (CUPS) / SDN approach already delivered in the trendy LTE releases.

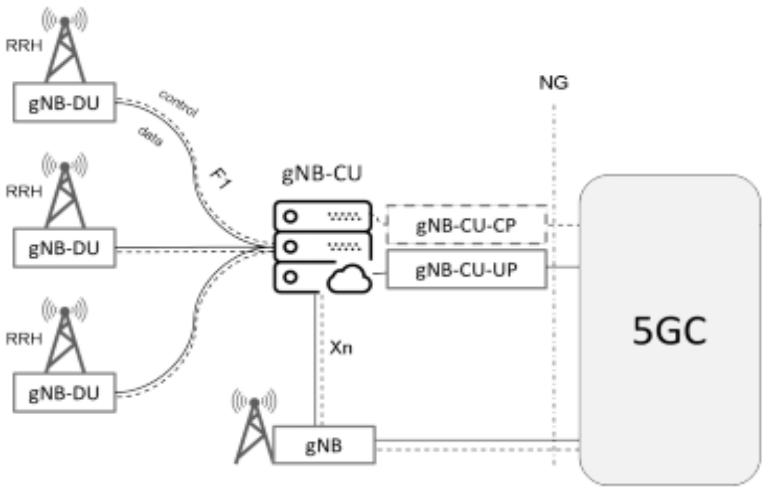

Figure III.4: Overall NG-RAN Architecture

Figure III.5 indicates the stack of the protocols crossing the radio interface and their placement on the aforementioned gNB units. The stack is nearly the equal as the LTE one, barring for the provider information adaptation protocol (SDAP) of the user plane.

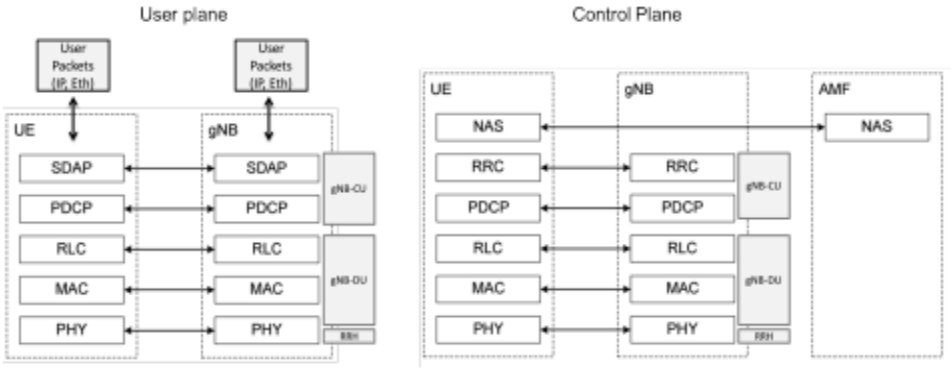

Figure III.5: NG-RAN Protocol Stack

The main functionalities of the unique layers are as follows:

- The physical layer (PHY) consists of the digital and analogue signal processing functions that the mobile and base station use to send and receive information. It is primarily based on OFDMA, with adaptive service spacing (15,30,60,120,240 kHz) and an adaptive modulation/coding scheme (e.g., from π/2 BPSK to 256 QAM).
- The medium access control (MAC) protocol provides low-level manipulate of the physical layer, exceptionally by way of scheduling facts transmissions between the mobile and the gNB.
- The radio link control (RLC) protocol ensures reliable shipping of statistics streams that need to arrive intact (HARQ). It additionally handles segmentation.
- The packet data convergence protocol (PDCP) incorporates out higher-level transport features associated to header compression and security.
- The service data adaptation protocol (SDAP) maps the interplay between the packet of a QoS glide and an information radio bearer with the aid of marking the person data packets properly.
- The radio resource controle (RRC) is the signaling protocol used in "access stratum" processes involving the cellular and the gNB. It consists of connection institution and launch functions; the broadcast of machine information; radio bearer establishment,

reconfiguration and release; RRC connection mobility procedures; paging; and strength control.

- The non-access stratum (NAS) protocol is the signaling protocol used between the UE and the 5GC for PDU session management, security, mobility management, etc. The 5GC entity that takes care of controlling the UE is the access and mobility management function (AMF), which is similar to the LTE MME. [18]

III.3.2 5G Core Network (5GC)

The NG-RAN architecture to some extent, as well as its protocol stack, is similar to the LTE one. However, the structure of the 5G core network is special in many ways.

The decomposition of the functions finished by using the community nodes of the preceding generations led to a 5G structure totally defined in terms of Network Function (NF) that are uncovered as services. Accordingly, as we can see in Figure III.6, each block title ends with the letter "F": function.

Another radical trade from the previous generations is the interface modeling, which has moved from "bit-oriented point-to-point" to "web-oriented service-based."

Indeed, 5G core is said to have a service-based architecture; wherever applicable, techniques are defined as services, so that it is viable to reuse them. There is a standardized point-to-point interface between any pair of interacting 2G, 3G and 4G network entities, and this interface makes use of a precise bit-oriented protocol. In the 5GC, the interactions among manage aircraft entities use service-based interfaces, supported through web-oriented tools such as HTTP/2.

The top phase of Figure III.6 indicates the set of network functions that structure the 5G control plane. All of them expose service-based interfaces. For this reason, they are depicted as being related by a community bus rather than via point-to-point links.

The interface identify is equal to the feature name, with an "N" used as prefix. In this arrangement, one NF queries a network repository function (NRF) to find out and allow conversation with different NFs. The insertion of a new community function, which include a third-party one, is only the insertion of a report in the NRF database.

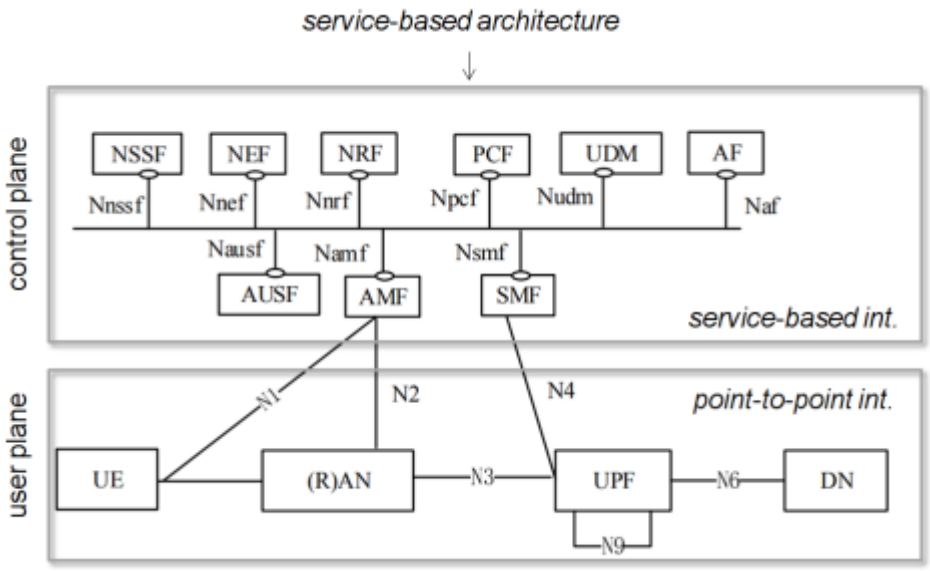

Figure III.6: 5G System Architecture, Non-roaming [17]

Let us conclude this part via describing the foremost roles of 5G NFs and their relation to 4G.

- The user plane function (UPF) handles the NG-U tunnel forwarding and the related records course services, such as anchoring for handover, QoS, and site visitor's coverage enforcement. There can be more than one UPFs related with a UE; these UPFs can be located in a single slice or in multiple ones. The UPF contains parts of the 4G SGW and PGW functionalities.
- The session management function (SMF) is the control section of a PDU session. That is, it configures NG tunnels, allocates IP addresses with DHCP, and configures visitors steering. The SMF consists of parts of the 4G MME and PGW functionalities.
- The access and mobility management function (AMF) handles all the 5GC signaling coming from and going to the UE. Unlike the SMF, it is a single function that is existing in multiple slices. It helps user get right of entry to the network and manages mobility through interacting with the UE and with other NFs The AMF carries phase of the 4G MME functionality.
- The authentication server function (AUSF) supports authentication for 3GPP and non-3GPP access. It contains part of the 4G HSS functionality.

- The unified data management (UDM) function can be considered a repository for UE-related information, such as credentials, identifiers, AMF details, and SMF assignments for the cutting-edge session. The underlying thought of the UDM is to create, anywhere possible, a central database for UE configuration information, so that the NFs can be designed as stateless services, enhancing architectural agility. The UDM incorporates section of the 4G HSS functionality.
- The policy control function (PCF) is a unified entity supplying coverage rules (QoS, filtering, charging, etc.) to other manage airplane functions, such as SMF. The PCF consists of phase of the 4G PCRF functionality.
- The network slice selection function (NSSF) selects the set of community slice situations serving the UE, along with the first-rate AMF for that purpose. It is now not existing in 4G.
- The network exposure function (NEF) exposes the competencies of networks and network/UE occasions for third-party, software function, area computing, and other purposes. It is no longer present in 4G.
- The network repository function (NRF) discovers network feature instances. When it receives an NF discovery request from a NF instance, it affords the located NF instances. It is now not current in 4G.
- The application function (AF) resembles a utility server that can interact with the other control-plane NFs. AFs can exist for distinctive software services, and can be owned by way of the community operator or with the aid of relied on third parties. For instance, the AF of an over-the-top application provider can impact routing, steering its site visitors closer to its external side servers [17]

III.4 The Different technology in fifth-generation

III.4.1 Millimeter wave

The usual sub-3 GHz spectrum is becoming an increasing number of congested and the present RATs are drawing near Shannon's potential limit. As such, lookup on exploring cm- and mmWave bands for mobile communications has already been started. Although the lookup on this discipline is nevertheless in its infancy, the outcomes seem promising.

There are three predominant impediments for mmWave cellular communications. First, the path loss is quite greater at these bands, compared to the conventional sub-3GHz bands. Second, electromagnetic waves tend to propagate in the LOS direction, rendering the radio hyperlinks vulnerable to being blocked by means of transferring objects or people. Last but no longer least, the penetration loss thru the constructions is considerably higher at these bands, blockading the outdoor RATs for the indoor users.

Despite these limitations, there are myriad advantages for mmWave communications. A substantial amount of spectrum is accessible in mmWave band; for example, at 60 GHz, there is 99GHz of unlicensed spectrum available. This quantity of spectrum is huge, particularly when we think that the world allotted spectrum for all cell applied sciences rarely exceeds 780 MHz [19]

This amount of spectrum can completely revolution is mobile communications by offering ultra-broadband wi-fi pipes that can seamlessly glue the wired and the wireless networks. Other advantages of mmWave communications encompass the small antenna sizes (λ/2) and their small separations (also round λ/2), enabling tens of antenna elements to be packed in simply one rectangular centimeter. This in turn approves us to attain very excessive beamforming positive aspects in exceptionally small areas, which can be applied at both the BS and the UE.

Incorporating smart phased array antennas, we can wholly exploit the spatial diploma of freedom of the wi-fi channel (using SDMA), which can further improve the machine capacity. Finally, as the cellular station moves around, beamforming weights can be adjusted adaptively so that the antenna beam is always pointing to the BS.

Recently, Samsung Electronics, an enterprise chief in exploring mmWave bands for cell communications, has examined a science that can obtain 2 Gbps facts price with 1 km range in

an urban environment [20].

Furthermore, Professor Theodore Rappaport and his lookup group at the Polytechnic Institute of New York University have verified that cellular communications at 28 GHz in a dense urban environment such as Manhattan, NY, is viable with a telephone measurement of 200 m the use of two 25 dBi antennas, one at the BS and the other at the UE, which is easily manageable using array antennas and the beamforming technique.

Last but now not least, foliage loss for mmWaves is sizable and may restrict the propagation. Furthermore, mmWave transmissions can also trip good sized attenuations in the presence of a heavy rain for the reason that the raindrops are roughly the same dimension as the radio wavelengths (millimeters) and therefore can purpose scattering. Therefore, a backup mobile device running in legacy sub-3 GHz bands may be wanted as section of the mmWave solution [19].

Figure III.7: 5G NR mmWave [21]

III.4.1.1 Physical Characteristics

The most important attribute of the mm-wave band for radio communication is its good-sized direction loss attenuation due exclusively to the distance between the transmitter and the receiver. Indeed, the specific attenuation in free house due to the atmosphere raises from 5·10−3 dB/km at 2 GHz to about 2·10−1 dB/km at 24 GHz to dramatically make bigger to 20 dB/km at 60 GHz, due the peak of absorption of oxygen: these numbers translate into an attenuation of 10 dB at 200 km, 50 km, and 500 m, respectively. In order to contain different propagation phenomena, a range of channel models have been proposed for mm-waves.

Moreover, the mm-waves are subject to the blockage phenomenon, as their propagation is generally averted by almost any physical object. This phenomenon is normally captured with the aid of both shadowing, modelling the presence of static objects, or fading, accounting for quickly attenuations versions due to moving objects.[22]

III.4.2 Massive MIMO

Massive MIMO antennas will increase region throughput and capacity density using massive numbers of antennas and MU-MIMO. Each antenna is individually-controlled and may

additionally embed radio transceiver components. Nokia claimed a five-fold expand in the potential amplify for a 64-Tx/64-Rx antenna system. The time period "massive MIMO" was once coined with the aid of Nokia Bell Labs researcher Dr. Thomas L. Marzetta in 2010, The utility procedure of this technological know-how has two benefits and is additionally integral for the multi-carrier science to work. First, many users will be capable to talk at the same time except restriction, due to a greater density of bases that will be receiving and transmitting signals. This amplify in reception and transmission of alerts will satisfy the demand for wi-fi communication. Second, its capability to slender the location in which signals are transmitted and obtained (Beamforming) appreciably reduces interference in the transmission system and consequently yields higher statistics transmission services.[15]

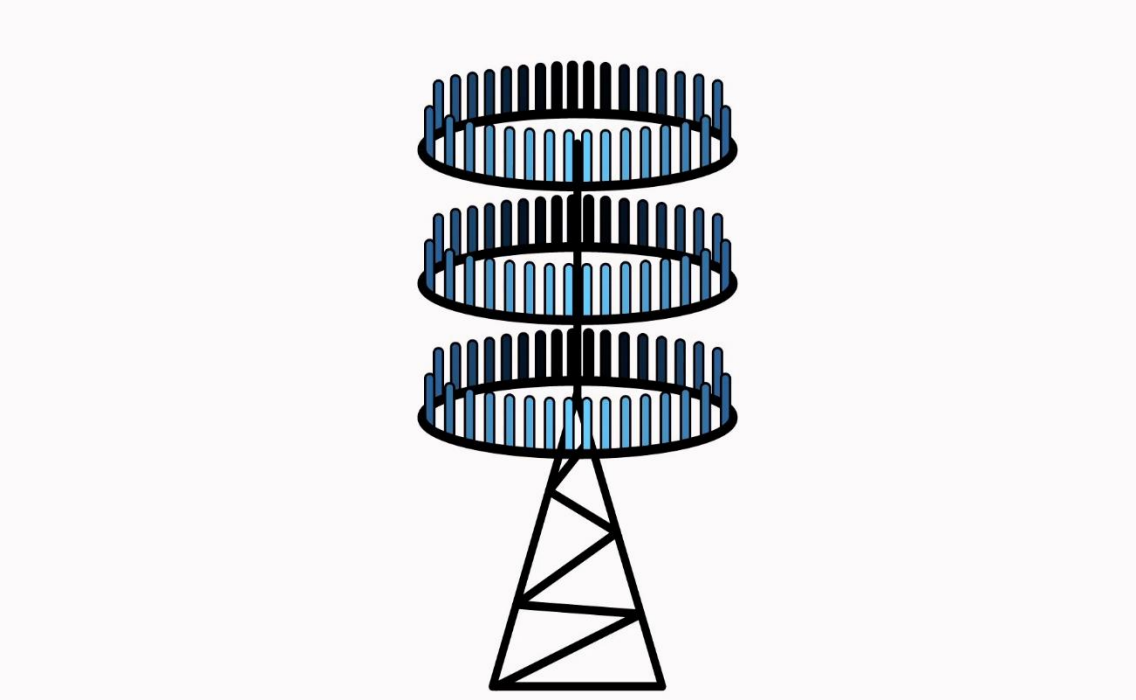

Figure III.8: Massive MIMO [21]

III.4.3 Beamforming

Beamforming or spatial filtering is a signal processing technique used in sensor arrays for directional signal transmission or reception. This is achieved by combining elements in an antenna array in such a way that signals at particular angles experience constructive interference while others experience destructive interference. Beamforming can be used at both the transmitting and

receiving ends in order to achieve spatial selectivity. The improvement compared with omnidirectional reception/transmission is known as the directivity of the array.

Beamforming can be used for radio or sound waves. It has found numerous applications in radar, sonar, wireless communications.[23]

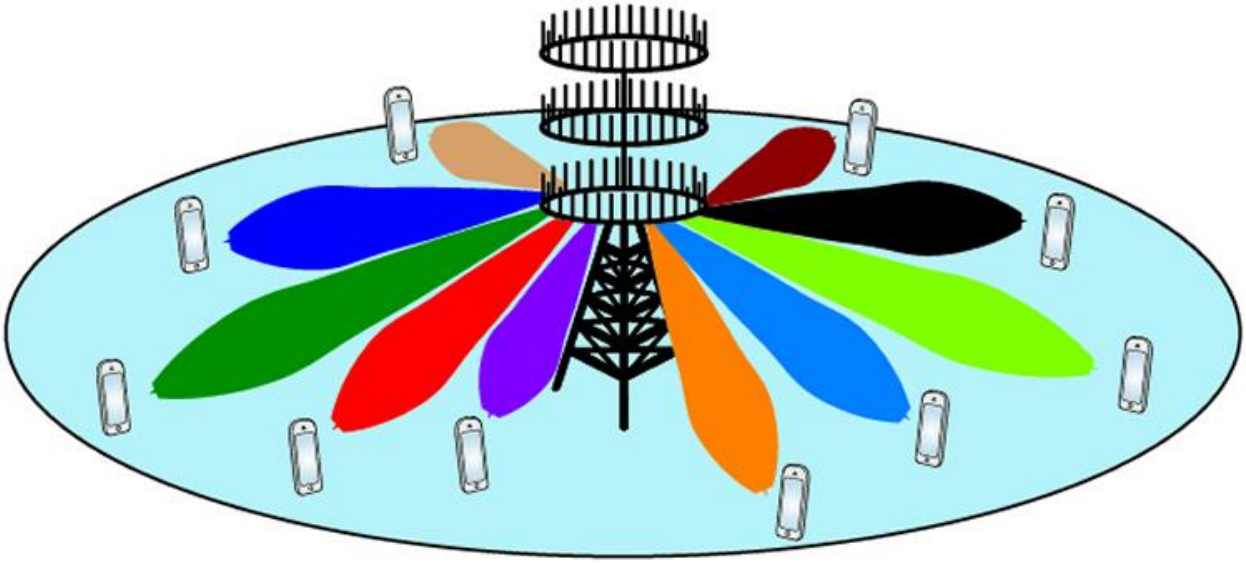

Figure III.9: Beamforming [21]

III.4.4 small cells

Telecommunications tools producers have taken standard macro radio designs and shriveled them down into what's referred to as a small cell. Small cells are smaller and more cost effective than a cellphone tower and can be installed in a variety of areas, bringing extra base stations closer to users. A giant variety of base stations increases the number of people a network can support, whilst decreased distance to customers decreases latency, enabling even faster connectivity.

The trend in 5G radio applications is to use greater frequencies and shorter wavelengths. Increasing the frequency increases the speed of sending/ receiving indicators and helps decrease the size of the antenna, which in turn shrinks the dimension of the cell. Shorter wavelengths result in a decrease in sign penetration and radius, reinforcing the want for small cells.

III.4.4.1 Small-cell coverage

A mobile tower (also known as a macrocell) is a large umbrella used to provide radio signals to hundreds of customers in giant areas with minimal obstructions. To extend the coverage of a macrocell, DASs are used in conjunction with the cell phone tower. DASs take a signal from the base station and boost it to increase the place the signal can reach.

While DASs are extraordinary for growing coverage, they do now not extend network capacity; the solely way to enlarge network potential is to add greater base stations, which is why small cells are so useful. Unlike macrocells installed on huge towers that cover hundreds of customers in the kilometer radius range, small cells serve as a complement, with tons smaller radius stages shut to humans and houses. Working as a base station itself to send and receive signals, a small cell not solely offloads some of the records potential of a macrocell, it additionally adds its personal information capacity, making the community greater robust.

Small cells do not cover the same area or number of users as a macrocell. Figure III.10 shows coverage for each type of small cell. small cells can serve as an enhanced alternative to multiple macrocells to cover more densely populated areas, complementing macrocell towers and becoming an essential factor for 5G deployment.[24]

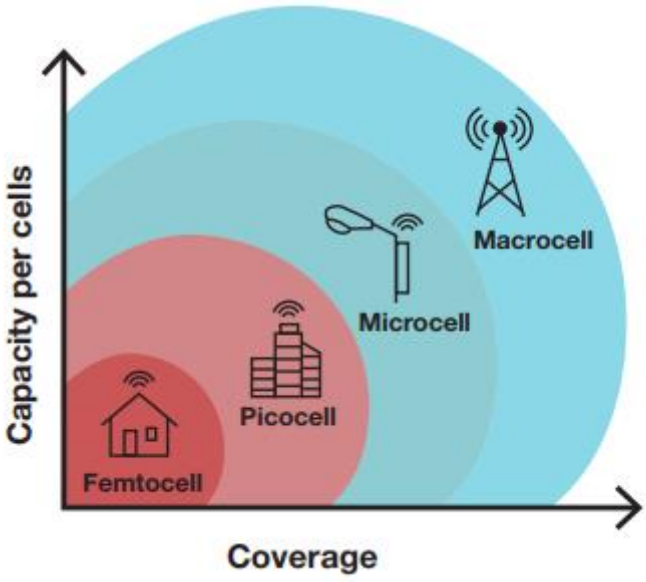

Figure III.10: Small-cell coverage [24]

III.4.4.2 Types of small cells

small cells they are normally classified by their coverage range. Table III.1 lists the sorts of small cells and what they are designed to support.

Femtocells, the smallest of the small cells, are intended for men and women to extend their private connectivity. Femtocell coverage is ideal for properties and small offices. Picocells, the subsequent step up, are used for large office structures or hotels. Above picocells are microcells, also called metrocells. Microcells are common on mild poles or atop buildings in dense urban areas. Another way to differentiate between the specific sorts of small cells is by their radio frequency (RF) strength output, which can dictate the insurance radius and variety of users.

Table III.1 Base station types [24].

Base station	**Type Number of users**	**Coverage (km)**	**Bandwidth (MHz)**	**RF (W)**	**Location**	**Users**
Femtocell	1 to 30	0.01	10	0.001 to 0.25	Indoor	Homes or small offices
Picocell	30 to 100	0.2	20	0.25 to 1	Indoor/ Outdoor	High-rise buildings, hotels, office buildings or parks
Microcell/ metrocell	100 to 2000	2	20 o 40	1 to 10	Outdoor/ Indoor	Shopping centers, transportation hubs, city blocks, stadiums, temporary events
Macrocell	>2,000	35	60 to 75	10 to >50	Outdoor	Suburban, city and rural areas

III.4.5 Softwarization and Virtualization

III.4.5.1 Software Defined Networking (SDN)

SDN is an umbrella time period to indicate a range of protocols and interfaces allowing network programmability. This is executed through decoupling the manipulate and consumer plane.

In the SDN concept, the user aircraft is substantially simplified and consists in stateless, distributed forwarding tables performing packet switching at very excessive speed. The tables are populated through a centralized manipulate plane retaining end-to-end course statistics for every service and offering help for superior features such as mobility management, policy and subscription manipulate.

Figure III.11 indicates the primary SDN mannequin in accordance to Open Networking Foundation (ONF). A provider consumer exchanges both statistics and management-control operations with some SDN provider. Service statistics is in the end forwarded by using some set of assets that are owned through the SDN provider. The service purchaser controls them thru the SDN controller by means of invoking moves on a set of digital sources that it perceives to be its own.[25]

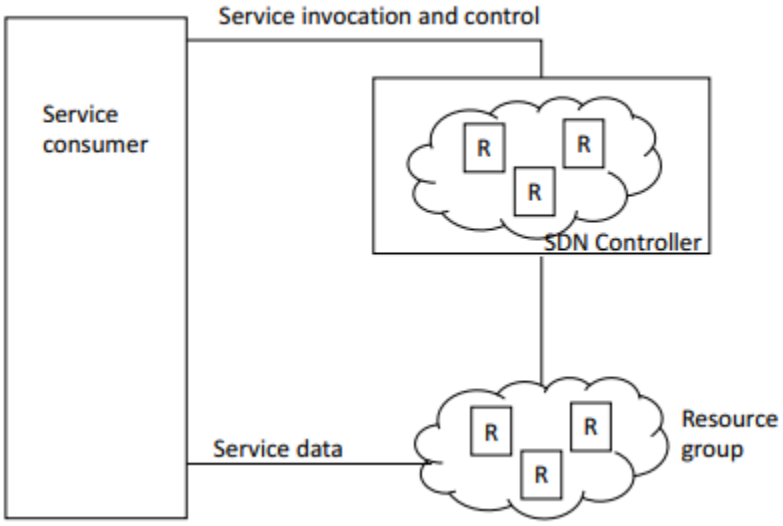

Figure III.11: Basic SDN model according to ONF [25]

III.4.5.2 Network Function Virtualization (NFV)

The NFV architecture defines how software features can be carried out in virtual

machines (VMs) and consolidated to share common physical sources in terms of compute, storage, and networking. Multiple functions can be instantiated within the same VM the usage of containers. VMs can be dynamically instantiated to cope with changing network demand in terms of site visitors and in phrases of presented elements and services.

With NFV, offerings are described as sequences of community features that procedure end-to-end flows. Figure III.12 indicates an example forwarding diagram for a cellular Internet carrier provider. Data flows from the developed eNodeB to the provider gateway and to the IP backbone. Mobility management, authentication and different control protocols flow through distinct community functions. Unlike cell networks, where a particular feature is activated network-wide, 5G allows the operator to prompt a characteristic on a per-service basis.

NFV and SDN do now not require each other, however are related in many ways. SDN affords an herbal answer to route packets between the Virtual Network Functions (VNFs) that symbolize every service. Additionally, it enables the virtualization of routing functions with a low overhead. Finally, it simplifies the rerouting of visitors flows after a particular VNF is moved from one bodily node to some other or, similarly, when an additional occasion of a VNF is elastically deployed in a new node to cope with increasing visitors demands.[26]

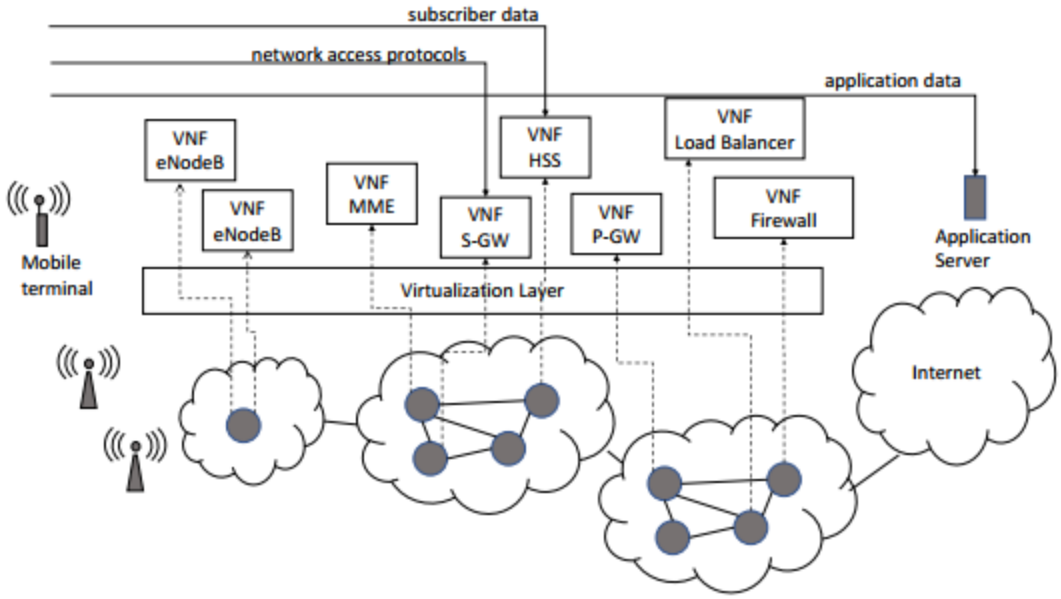

Figure III.12: Example of NFV forwarding graph [26]

III.5 Mobility Management, Handover In 5G

The mobility is a core feature of 5GS. with a similar principle in mobility management as for 3GPP systems but with some key differences.

Mobility Management is required to ensure the following:

- That the network can “reach” the user, for example to notify the user about incoming messages and calls.
- That a user can initiate communication toward other users or services such as Internet access.
- That connectivity and ongoing sessions can be maintained as the user moves, within or between access technologies.

III.5.1 Network-Controlled Mobility

The mobility of the UEs in RRC_CONNECTED state is managed by the network, which is labeled into two types of mobility, namely, cell-level mobility and beam-level mobility. The cell-level mobility requires explicit RRC signaling to be triggered, the results of that is the handover. The beam-level mobility does not require explicit RRC signaling to be triggered. The gNB offers the UE, by means of RRC signaling, with dimension configuration containing configurations of SSB/CSI assets and resource sets, as nicely as set off states for triggering channel and interference measurements and reports.

The fundamental steps of the inter-gNB handover signaling processes are illustrated in Figure III.13 The inter-gNB handover comprises the following steps:

1. The source gNB initiates handover and sends a Handover Request over Xn interface.

2. The target gNB proceed an admission control and reserve the RRC configuration as part

of the Handover ACK.

3. The source gNB reserve the RRC configuration to the UE in the Handover Command

message, which includes the cell ID and all information required to access the target cell, so that the UE can access the target cell without detecting that cell’s SI. In some cases, the information required for contention-based and contention-free random-access procedure can be included in the

Handover Command message. The access information to the target cell may include beam-specific information.

4. The UE moves the RRC connection to the target gNB and replies with the Handover Complete message.[27]

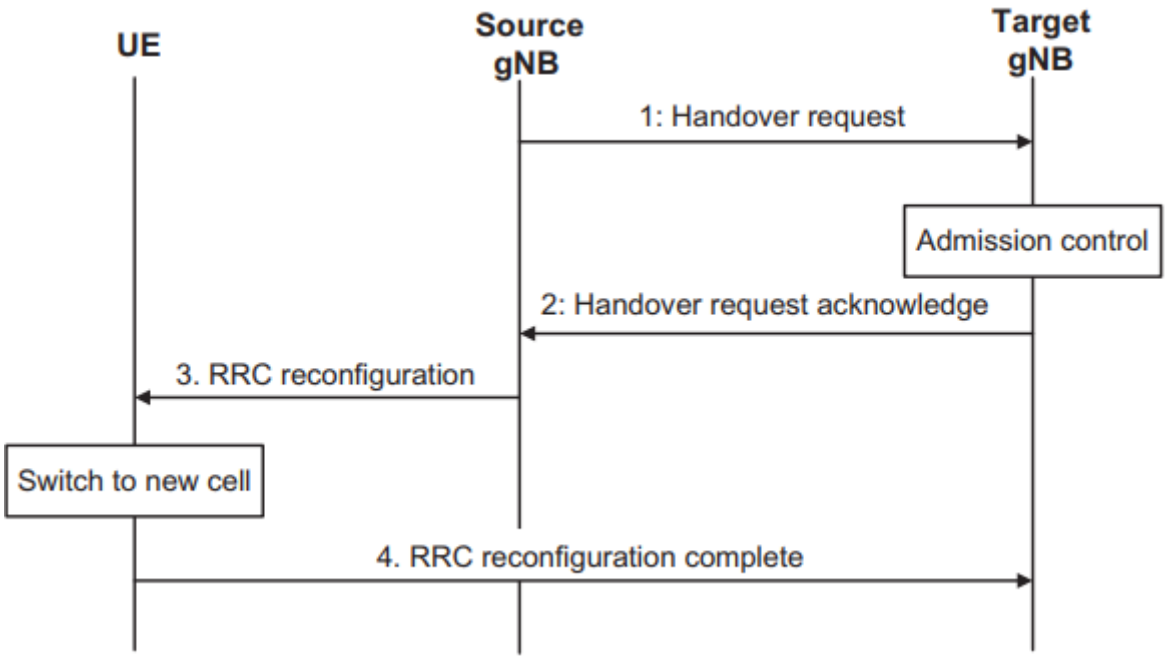

Figure III.13: Inter-gNB handover procedure [27]

III.5.2 Control-Plane Handover

The intra-NR handover consists of the preparation and execution phases of the handover technique carried out barring 5GC involvement, that is, practice messages are directly exchanged between the gNBs. The release of the resources at the supply gNB for the duration of the handover completion phase is precipitated by using the target gNB. The details shown in Figure III.14.

1. The UE context within the source gNB contains information concerning roaming and access restrictions, which were provided either at connection establishment or at the last tracking area update.

2. The source gNB configures the UE measurement procedures and the UE reports

according to the measurement configuration.

3. The source gNB decides to handover the UE, based on measurement reports and radio resource management (RRM) information.

4. The source gNB issues a Handover Request message to the target gNB passing a transparent RRC container with necessary information to prepare for the handover at the target gNB. The information includes target cell ID, C-RNTI of the UE in the source gNB, RRM configuration including UE inactive time, basic AS-configuration including antenna info and DL carrier frequency, the current QoS flow to DRB mapping rules applied to the UE, the UE capabilities for different RATs. After issuing a Handover Request, the source gNB should not reconfigure the UE, including performing reflective QoS flow to DRB mapping.

5. Admission control may be performed by the target gNB.

6. The target gNB prepares the handover with L1/L2 and sends the Handover Request Acknowledge to the source gNB, which includes a transparent container to be sent to the UE as an RRC message to perform the handover.

7. The source gNB triggers the Uu handover by sending an RRC Reconfiguration message to the UE, containing the information required to access the target cell, that is, the target cell ID, the new C-RNTI, and the target gNB security algorithm IDs for the selected security algorithms.

8. The source gNB sends the SN Status Transfer message to the target gNB.

9. The UE synchronizes to the target cell and completes the RRC handover procedure by sending RRC Reconfiguration Complete message to target gNB.

10. The target gNB sends a Path Switch Request message to the AMF to trigger 5GC to switch the downlink data path toward the target gNB and to establish an NG-C interface instance toward the target gNB.

11. 5GC switches the downlink data path toward the target gNB. The UPF sends one or more end-marker packets on the old path to the source gNB per PDU session/tunnel and then can release any user-plane/TNL resources toward the source gNB.

12. The AMF confirms the Path Switch Request message with the Path Switch Request Acknowledge message.

13. The target gNB sends the UE Context Release message to inform the source gNB about the success of the handover. The source gNB can then release radio and control-plane related resources associated to the UE context.[27]

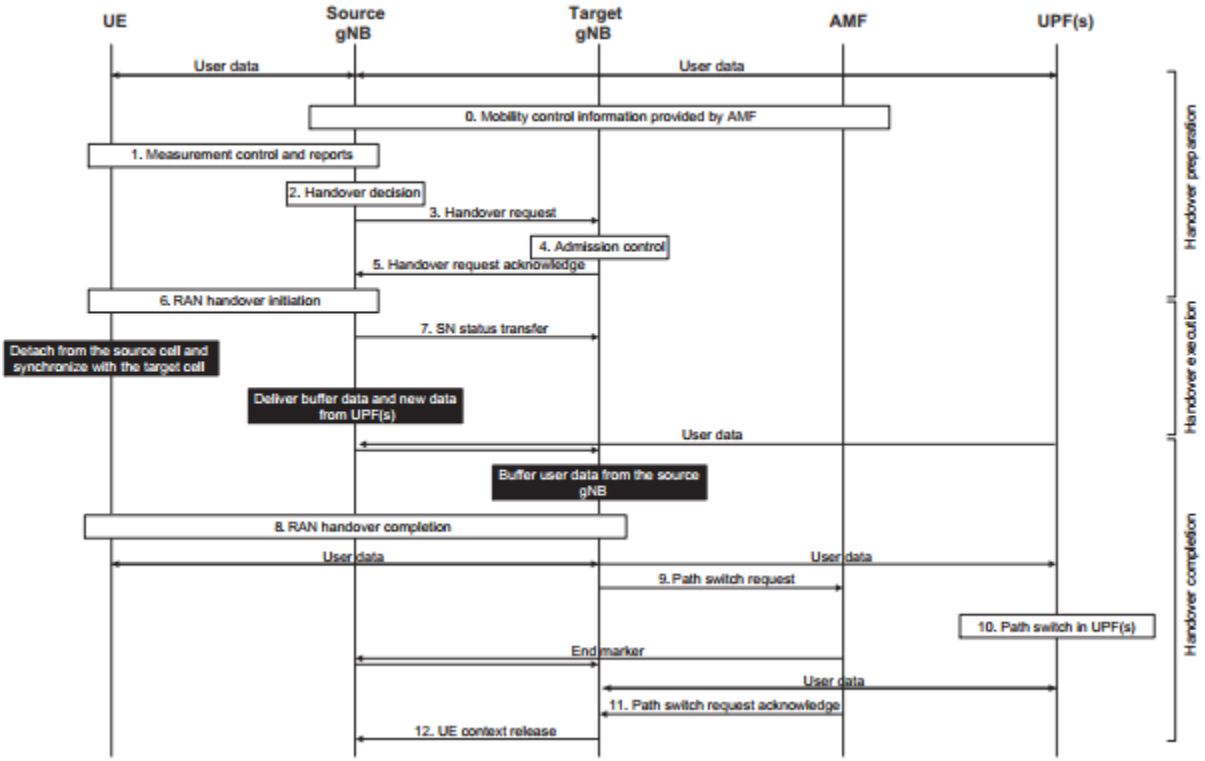

Figure III.14: Intra-AMF/UPF handover in NR [27]

III.5.3 User-Plane Handover

The user-plane aspects of intra-NR handover for the UEs in RRC_CONNECTED state include the following principles to avoid loss of user data during handover. During handover preparation, the user-plane tunnels can be established between the source gNB and the target gNB. During handover execution, the user data can be forwarded from the source gNB to the target gNB. Packet forwarding should be done in order, as long as the packets are received at the source gNB from the UPF or the source gNB buffer has not been emptied. During handover completion, the target gNB sends a path switch request message to the AMF to inform it that the UE has been granted access and the AMF then triggers path switch related 5GC internal signaling and actual path switch of the source gNB to the target gNB in UPF. The source gNB should continue forwarding data, as

long as packets are received at the source gNB from the UPF or the source gNB buffer has not been emptied.

The target gNB retransmits and prioritizes all downlink data forwarded by the source gNB excluding the PDCP SDUs for which the reception was acknowledged through PDCP-SNbased reporting by the UE, that is, the target gNB should initially send all forwarded PDCP SDUs with PDCP SNs, then all forwarded downlink PDCP SDUs without SNs before sending new data from 5GC. Lossless delivery, when a QoS flow is mapped to a different DRB at handover, requires that the old DRB to be configured in the target cell. For in-order delivery in the downlink, the target gNB should first transmit the forwarded PDCP SDUs on the old DRB before transmitting new data from 5G CN on the new DRB. In the uplink, the target gNB should not deliver data of the QoS flow from the new DRB to 5G CN before receiving the end-marker on the old DRB from the UE. The source NG-RAN node may request downlink data forwarding per QoS flow to be established for a PDU session and may provide information on how it maps QoS flows to DRBs.

The target NG-RAN node decides whether data forwarding per QoS flow should be established for a PDU session. If lossless handover is desired and the QoS flow to DRB mapping, applied at the target NG-RAN node, allows employing data forwarding with the same QoS flow to DRB mapping that was used in the source NG-RAN node for a DRB and if all QoS flows mapped to that DRB are accepted for data forwarding, the target NG-RAN node establishes a downlink forwarding tunnel for that DRB. For a DRB for which SN status preservation is important, the target NG-RAN node may decide to establish an uplink data forwarding tunnel.

The target NG-RAN node may also decide to establish a downlink forwarding tunnel for each PDU session. In this case, the target NG-RAN node provides information related to the QoS flows for which data forwarding has been accepted and the corresponding uplink TNL information for data forwarding tunnels to be established between the source and the target NG-RAN nodes [27].

III.6 Conclusion

The chapter gives us an overview of the fifth generation which include the basic technologies behind it: Millimeters waves, Massive MIMO, Beamforming, Small cells, Softwarization and Virtualization; and the new architecture which contains whole NR. And finally gives the

information that concerns the mobility management, and here we concentrate for the handover in both user and control plan.

Chapter IV:

SIMULATION AND

RESULT

IV.1 Introduction

The ever-increasing demand of wireless cellular data has motivated researchers to investigate the potentials of millimeter wave communication system. A substantial body of literature is currently available discussing physical measurements and formulations for millimeter wave channels.

To check the network ability to work in the real world, it must be runs in the simulator, the benefits of use it can avoid of losing money and test it without any problems with the ability to change the network protocols on the way.

In this chapter we going to exploit the NS3-MMWAVE module which can simulate the 5G networks in term of the mobility and the handover, and also, we going to present some scenarios and discuss the results.

IV.2 About NS-3 simulator

NS-3 has been developed to provide an open, extensible network simulation platform, for networking research and education. In brief, ns-3 provides models of how packet data networks work and perform, and provides a simulation engine for users to conduct simulation experiments. Some of the reasons to use ns-3 include to perform studies that are more difficult or not possible to perform with real systems, to study system behavior in a highly controlled, reproducible environment, and to learn about how networks work. Users will note that the available model set in ns-3 focuses on modeling how Internet protocols and networks work, but ns-3 is not limited to Internet systems; several users are using ns-3 to model non-Internet-based systems.

Many simulation tools exist for network simulation studies. Below are a few distinguishing features of ns-3 in contrast to other tools. ns-3 is designed as a set of libraries that can be combined together and also with other external software libraries. While some simulation platforms provide users with a single, integrated graphical user interface environment in which all tasks are carried out, ns-3 is more modular in this regard. Several external animators and data analysis and visualization tools can be used with ns-3. However, users should expect to work at the command line and with C++ and/or Python software development tools.

NS-3 is primarily used on Linux or macOS systems, although support exists for BSD systems and also for Windows frameworks that can build Linux code, such as Windows Subsystem for Linux,

or Cygwin. Native Windows Visual Studio is not presently supported although a developer is working on future support. Windows users may also use a Linux virtual machine.[28]

Figure IV.1: NS3 logo [21]

IV.3 The Millimeter wave module for NS-3 simulator

The mm-Wave module provides a basic implementation of millimeter wave user and infrastructure devices which include the propagation models, physical (PHY) and MAC.

Inspired by the LTE module [29], this module has been designed to provide a completely customizable simulation tool for mm-Wave devices.

The important features provided by the module are:

- a basic implementation of mm-Wave user devices and infrastructure devices (base stations),
- support for time division duplexing (TDD), a feature not implemented in the LTE module, (iii) a customizable OFDM based frame structure for data and control channels,
- support for downlink and uplink MAC scheduling,
- an outdoor mmWave channel model based on [30]
- customizable MIMO antenna system with beam forming at the user and infrastructure device.

The module is developed completely in C++. Figure IV.2 shows a schematic diagram of the mmWave module.

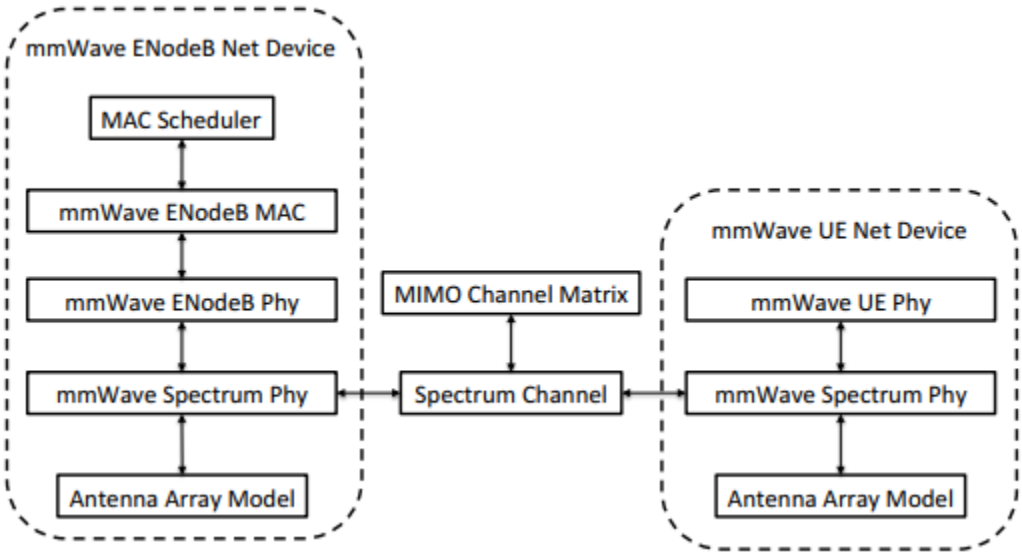

Figure IV.2: A schematic diagram of the mmWave device functionalities.

IV.3.1 Channel Model

The mmWave spectrum channel handles path loss, small scale fading and beam-forming gain. Path loss is calculated according to distance and link scenario [30]. Small scale fading is characterized as 3 clusters formed by 20 paths. Beamforming gain is computed based on a 64×16 channel matrix and associated antenna weights, which are generated offline using MATLAB.

IV.3.2 Physical Layer

The chief function of the physical layer is:

- to transmit signals sent from the upper layers over the physical channel,
- to process data and control signals received over the physical channel
- send associated primitives to the upper layers. The mmWave module supports TDD, which is likely to be adopted in 5G cellular networks, mainly to better support relays.

The physical layer is also in charge of computing the received SINR for data signals taking into account the beam forming vectors of the transmit and receive antennae and the spatial matrices for the channel. Control signals are assumed to be ideally transmitted and received.

IV.3.3 MAC layer

The MAC layer hosts the packet scheduler. The scheduler bases the scheduling decision on a TDD pattern, which determines the transmit-receive scheme to be used by each device. Based on a specified time granularity, the MAC and the PHY layers will interact and update the scheduling scheme. The infrastructure device will transmit the uplink scheduling information to the users in a control message.

IV.4 Installation

- In order to install NS3-MMWAVE module first must download packages:

```
sudo apt-get install gcc g++ python python-dev mercurial bzr gdb valgrind gsl-bin libgsl0-dev libgsl0ldbl flex bison tcpdump sqlite sqlite3 libsqlite3-dev libxml2 libxml2-dev libgtk2.0-0 libgtk2.0-dev uncrustify doxygen graphviz imagemagick texlive texlive-latex-extra texlivegeneric-extra texlive-generic-recommended texinfo dia texlive texlive-latex-extra texlive-extrautils texlive-generic-recommended texi2html python-pygraphviz python-kiwi pythonpygoocanvas libgoocanvas-dev python-pygccxml. [31]
```

- Now downloading the module:

```
Mkdir ns3
Cd ns3
Wget https://codeload.github.com/nyuwireless-unipd/ns3-mmwave/tar.gz/V2.0
Tar xjf ns3-mmwave-2.0.tar.gz
Cd ns3-mmwave-2.0.tar.gz/
```

- For the next step building NS3

```
./waf --build-profile=debug --enable-examples --enable-tests configure
./waf
```

- Now test the installation:

```
./test.py -c core
```

- To run an example:[31]

```
./waf --run hello-simulator
```

IV.5 Definition of terms used in the simulation

IV.5.1 SINR (Signal-to-interference-plus-noise ratio)

the signal-to-interference-plus-noise ratio (SINR) is a quantity used to give theoretical upper bounds on channel capacity (or the rate of information transfer) in wireless communication systems such as networks. The SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise. If the power of noise term is zero, then the SINR reduces to the signal-to-interference ratio (SIR). Conversely, zero interference reduces the SINR to the SNR, which is used less often when developing mathematical models of wireless networks such as cellular networks.

The definition of SINR is usually defined for a particular receiver (or user). In particular, for a receiver located at some point x in space (usually, on the plane), then its corresponding SINR given by:

$$SINR(x) = \frac{P}{I + N}$$

where P is the power of the incoming signal of interest, I is the interference power of the other (interfering) signals in the network, and N is some noise term, which may be a constant or random. Like other ratios in electronic engineering and related fields, the SINR is often expressed in decibels or dB.[32]

IV.5.2 RSRP (Reference Signal Receive Power)

Reference Signal Receive Power is the average power of Resource Elements (RE) that carry cell specific Reference Signals (RS) over the entire bandwidth, so RSRP is only measured in the symbols carrying RS.

- RSRP is the average received power of a single RS resource element.
- UE measures the power of multiple resource elements used to transfer the reference signal but then takes an average of them rather than summing them.
- Reporting range -44…-140 dBm

RSRP does a better job of measuring signal power from a specific sector while potentially excluding noise and interference from other sectors.

RSRP levels for usable signal typically range from about -75 dBm close in to an LTE cell site to -120 dBm at the edge of LTE coverage.[33]

IV.5.3 The Handover A3

The idea of the Handover A3 is to provide each UE with the best available signal quality (RSRP). This is achieved by performing a handover as soon as a neighboring cell offers a better signal.[34]

IV.5.4 A3-Rsrp Algorithm

A3-Rsrp which is also called as traditional PBGT algorithm. The goal is to provide each user equipment node with the best possible Reference Signal Received Power (RSRP) as shown in Figure IV.3. This is achieved by performing a handover as soon as a better cell is detected and event A3 (neighbors' cells RSRP become better than serving cells RSRP) is chosen. Handover is triggered for UE to the best cell in the measurement report. This handover algorithm is based on hysteresis and time-to-trigger parameters to the UE configuration. Hysteresis delays the handover in regard of RSRP. Time-to-trigger delays the handover in regard of time.[35]

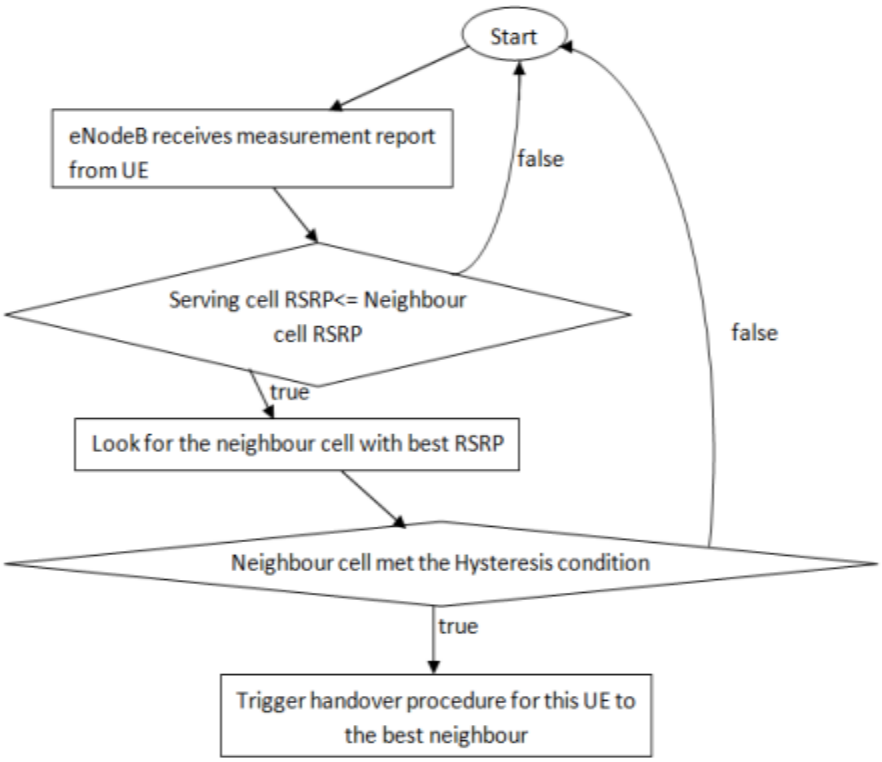

Figure IV.3: A3-Rsrp Algorithm Flowchart.[35]

In NS3 MMWAVE module the a3-rsrp algorithm can be found in the src/LTE/model folder, and the following lines are the important ones:

```
        if (measResults.haveMeasResultNeighCells
&& !measResults.measResultListEutra.empty ())
{
uint16_t bestNeighbourCellId = 0;
uint8_t bestNeighbourRsrp = 0;

    for     (std::list     <LteRrcSap::MeasResultEutra>::iterator     it     =
measResults.measResultListEutra.begin ();
it != measResults.measResultListEutra.end ();
++it)
{
if (it->haveRsrpResult)
{
if ((bestNeighbourRsrp < it->rsrpResult)
&& IsValidNeighbour (it->physCellId))
{
bestNeighbourCellId = it->physCellId;
bestNeighbourRsrp = it->rsrpResult;
}
}
else
{
NS_LOG_WARN ("RSRP measurement is missing from cell ID " << it->physCellId);
```

```
}
}

if (bestNeighbourCellId > 0)
{
NS_LOG_LOGIC ("Trigger Handover to cellId " << bestNeighbourCellId);
NS_LOG_LOGIC ("target cell RSRP " << (uint16_t) bestNeighbourRsrp);
NS_LOG_LOGIC ("serving cell RSRP " << (uint16_t) measResults.rsrpResult);

// Inform eNodeB RRC about handover
m_handoverManagementSapUser->TriggerHandover (rnti,
bestNeighbourCellId);
}
```

IV.6 Description of the Scenarios

In the NS3 MMWAVE module we use the "mmwave.c" script to simulate our work , by adding some changes: adding the EPC and the Internet ,increasing the number of UE and base stations , creating a custom vector that the UE walks by.

The experiment divided into two parts each part has three scenarios, first part is for the normal users (low speed) and the second part is for high speed users up to 200 Km/h.

And this is the parameters of the simulation:

First scenario:	Second scenario:	Third scenario:
• 1 user • 1 LTE base station • 2 MMWAVE base station • LTE EPC • Remote host • Bandwidth 1Ghz • Custom vector	• 5 users • 1 LTE base station • 2 MMWAVE base station • LTE EPC • Remote host • Bandwidth = 1Ghz • Distance between users= 2m • Custom vector	• 10 users • 1 LTE base station • 2 MMWAVE base station • LTE EPC • Remote host • Bandwidth 1Ghz • Distance between users = 2m • Custom vector

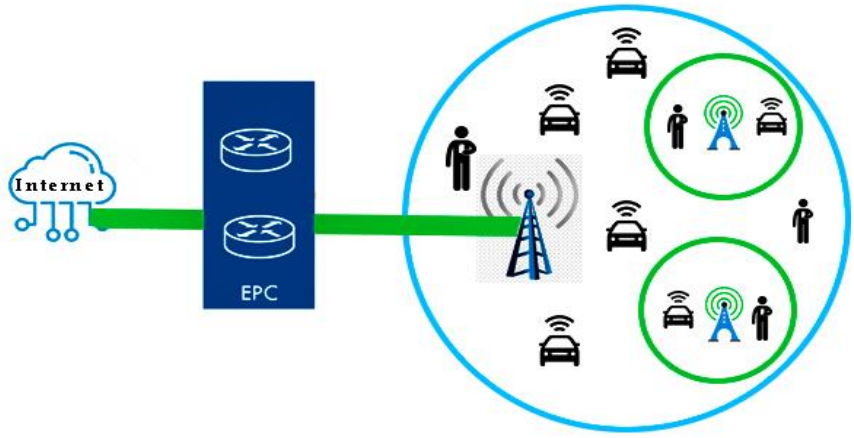

Figure IV.4: Scenarios based form

To study the mobility management (location registration and the handover) we extract the results of one user while it and the other users are moving to see the effect of the handover and the network density to both the quality of the connection and the received packet. All the users are moving and make calls in the same time. The results generated in a file called “RxPacketTrace.txt”, it contained all the necessary output to our simulation.

Now to execute the script just by typing in command prompt: ./waf scratch/mmwave.cc , Figure IV.5 shows what the code line do.

To show the simulation in a graphic interface; NS3 use NetAnim because it doesn’t have a graphic interface, by typing ./NetAnim inside netanim folder in NS3 MMWAVE module , by adding some lines in the script to generate the XML file and finely launch it in the NetAnim interface , Figure IV.6 shows a peek inside the interface of NetAnim.

```
File  Edit  View  Search  Terminal  Help
mostafa@mostafa-Lenovo-B50-70:~/Desktop/ns3-mmwave-2.0$ ./waf --run scratch/mmwave
Waf: Entering directory `/home/mostafa/Desktop/ns3-mmwave-2.0/build'
[2724/2786] Compiling scratch/mmwave.cc
[2745/2786] Linking build/scratch/mmwave
Waf: Leaving directory `/home/mostafa/Desktop/ns3-mmwave-2.0/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (1m55.229s)
bandwidth 0 = 1.00001e+09
bandwidth 0 = 1.00001e+09
************* UPDATING CHANNEL MATRIX (instance 68) *************
************* UPDATING CHANNEL MATRIX (instance 62) *************
************* UPDATING CHANNEL MATRIX (instance 27) *************
************* UPDATING CHANNEL MATRIX (instance 39) *************
************* UPDATING CHANNEL MATRIX (instance 83) *************
************* UPDATING CHANNEL MATRIX (instance 7) *************
************* UPDATING CHANNEL MATRIX (instance 3) *************
************* UPDATING CHANNEL MATRIX (instance 43) *************
************* UPDATING CHANNEL MATRIX (instance 40) *************
************* UPDATING CHANNEL MATRIX (instance 12) *************
m_lteOutputFilename LteSwitchStats.txt
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:2 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:2 Does not have a mobility model. Use SetConstantPosition if it is stationary
UE register to enb 2
UE register to enb 2
UE register to enb 2
UE register to enb 2
UE register to enb 2
************* UPDATING CHANNEL MATRIX (instance 3) *************
************* UPDATING CHANNEL MATRIX (instance 36) *************
************* UPDATING CHANNEL MATRIX (instance 44) *************
************* UPDATING CHANNEL MATRIX (instance 32) *************
************* UPDATING CHANNEL MATRIX (instance 75) *************
************* UPDATING CHANNEL MATRIX (instance 25) *************
************* UPDATING CHANNEL MATRIX (instance 9) *************
```

Figure IV.5: Launching a script in command prompt

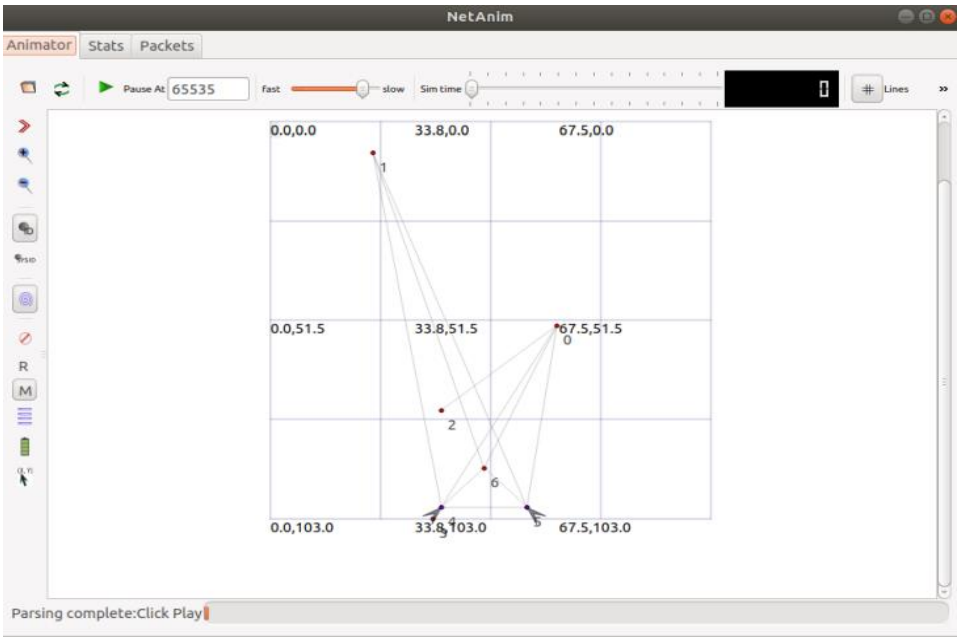

Figure IV.6: NetAnim interface

IV.7 Simulation Results and Discussion

The aim of our simulation is to see how does the mobility management during the movement of the users and while they perform the handover; in the ns3 trace file there are the value of SINR

that give us an idea of the quality of the mmwave links and we create a graph of it using Microsoft Excel ; however to see the number of receiving messages during the simulation we use the throughput which is the rate of successful message delivery over a communication channel. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps).

IV.7.1 first part (normal users)

First scenario:

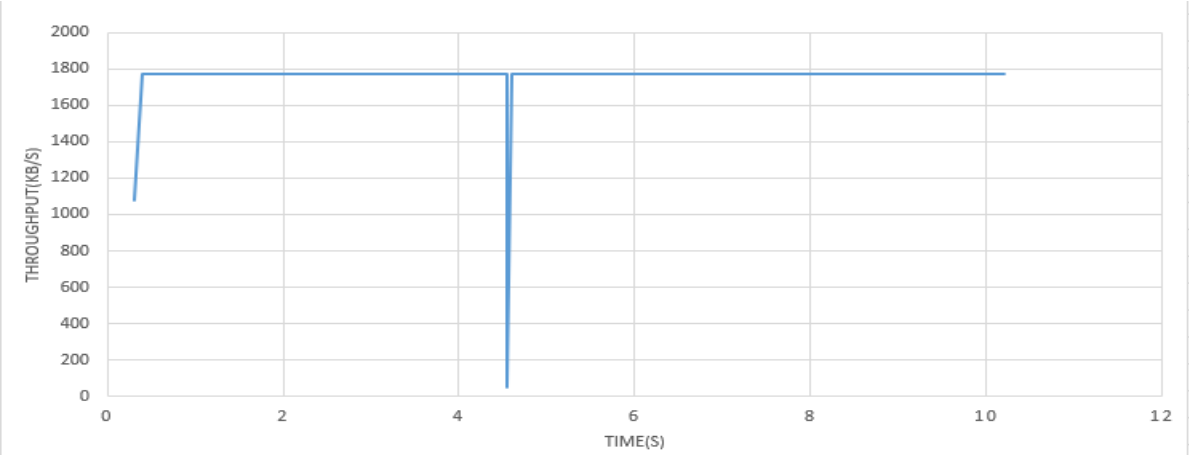

Figure IV.7: Throughput value of one user in relation to time

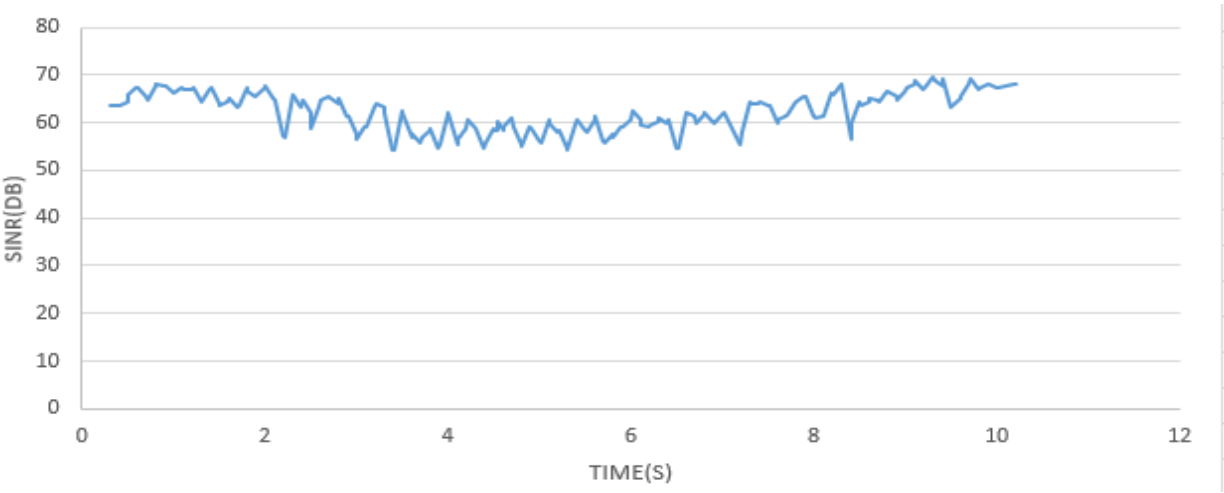

Figure IV.8: SINR value of one user in relation to time

The first scenario describe one user connected to one mmwave base station , and walk in a normal speed while sending packet toward the second mmwave base station , we created a stable vector to walk in and while the user moving there are a LTE base station in the middle to see the effect of doing that.

In the throughput graph it shows a stable value of 1800 Kb/s because of the ideal condition of one user only that is in the network , in 4.3 second a drops happens in the throughput value which is caused by the handover for a 0.5 microsecond which is a very quick moment and then it back to normal.

The SINR graph looks stable ,and average of 63 db which is a optimal case , the value range from 58 db to 68 db ; unusual happens when the handover is perform is that nothing happens to the SINR value it indicate that while only one user is the network , theoretically the handover doesn't affect the strong mmwave link while one only in the network.

Second scenario:

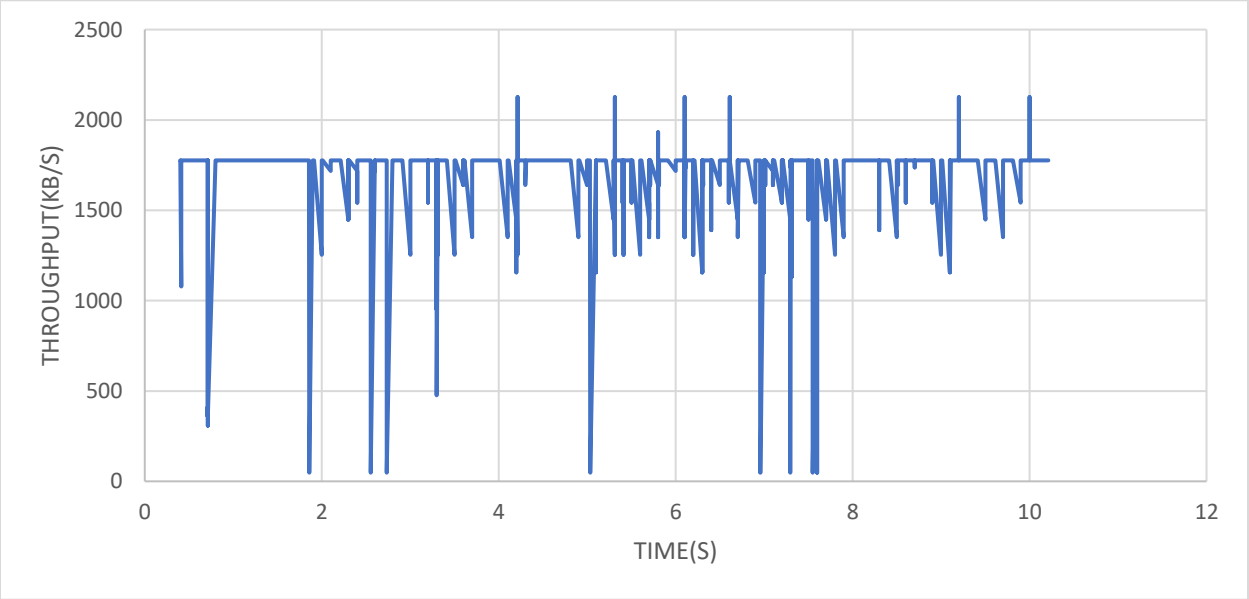

Figure IV.9: Throughput value of 5 users in relation to time

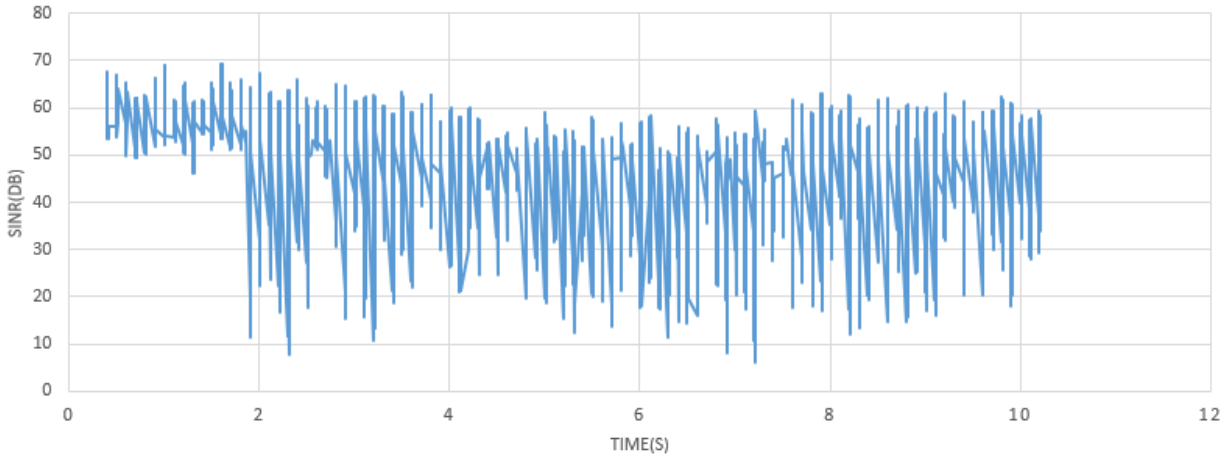

Figure IV.10: SINR value of 5 users in relation to time

The second scenario describe 5 users spaced between each other by 2m and each one is precedes the other , connected to one mmwave base station and they walk in a normal speed while sending packet toward the second mmwave base station , we created a stable vector to walk in and while the users are moving there are a LTE base station in the middle just like the first scenario.

Because the trace file is too large, we add a filter to one user only.

In the throughput graph it shows a changes in value , in some part being stable of 1800 Kb/s and the other part a change between 1200 Kb/s to 2000 Kb/s , but what can see is the dropped packet increase while the user in the handover case and also while the other users perform it which show the effect of the handover not only when a user perform it but also when others do the it to the receiving packet.

As we increased the number of users The SINR graph affected with that ,an average of 40 db Which decreased compared to the first scenario , it still great but the value range changes from 10 db to 68 db ; unlike the previous graph (Figure IV.8) a decreased in the SINR value because of the number of user which they are calling in the same time and also the handover here effect the SINR value like we said not only of the user itself but the others effect too.

Third scenario:

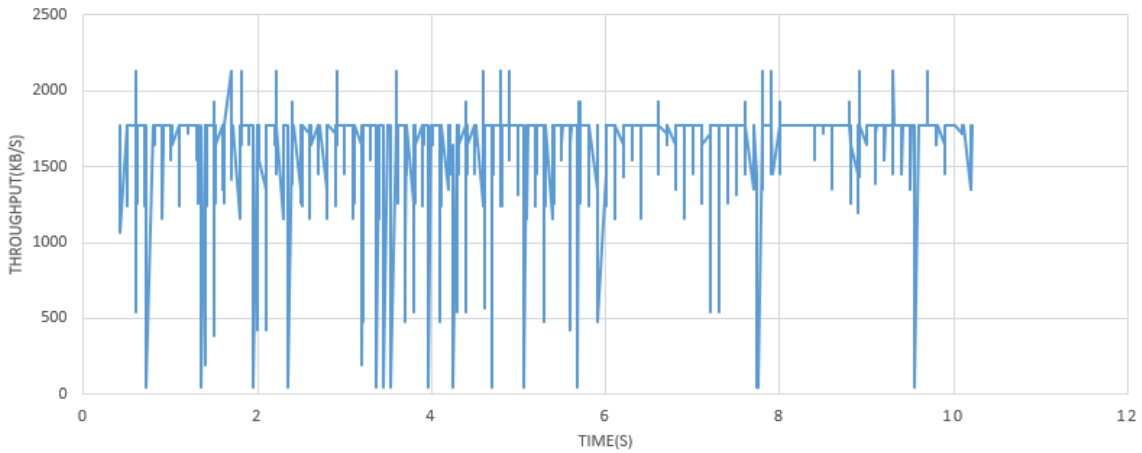

Figure IV.11: Throughput value of 10 users in relation to time

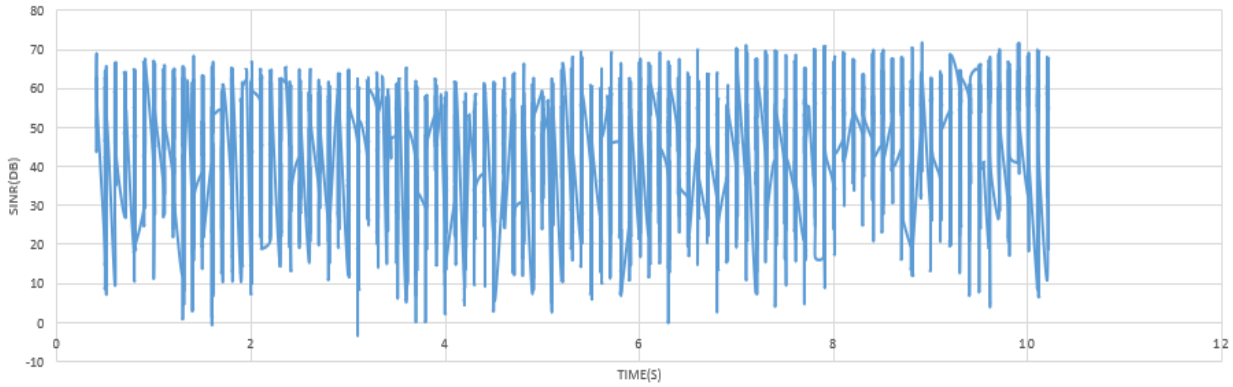

Figure IV.12: SINR value of 10 users in relation to time

The third scenario describe 10 users spaced between each other by 2m and each one is preceding the other, and all the parameters like the second scenario.

Compared to the previous throughput graph (Figure IV.9) here it shows also a changes in value , in some part being stable of 1800 Kb/s and the other part a change between 700 Kb/s to 2000 Kb/s , but also what can see is the dropped packet increase another time while the user in the handover case and also while the other users perform it , and we can tell that the number effect the receiving packets.

The SINR graph also affected as the number increased, an average of 32 db Which decreased compared to the second scenario, and for the value range changes from 0 db to 68 db which is a significant drop; and we don't forget the handover effect to the simulation too.

IV.7.2 second part (high speed 200 km/h)

First scenario:

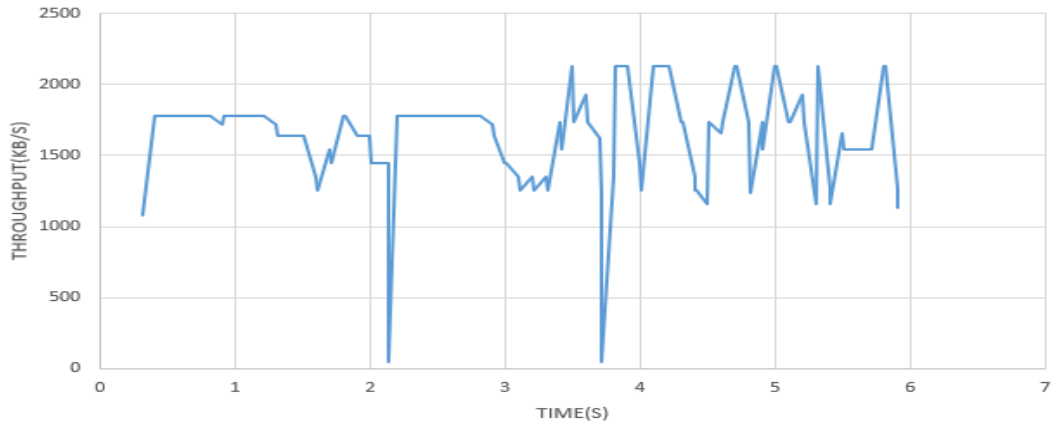

Figure IV.13: Throughput value of one user in relation to time

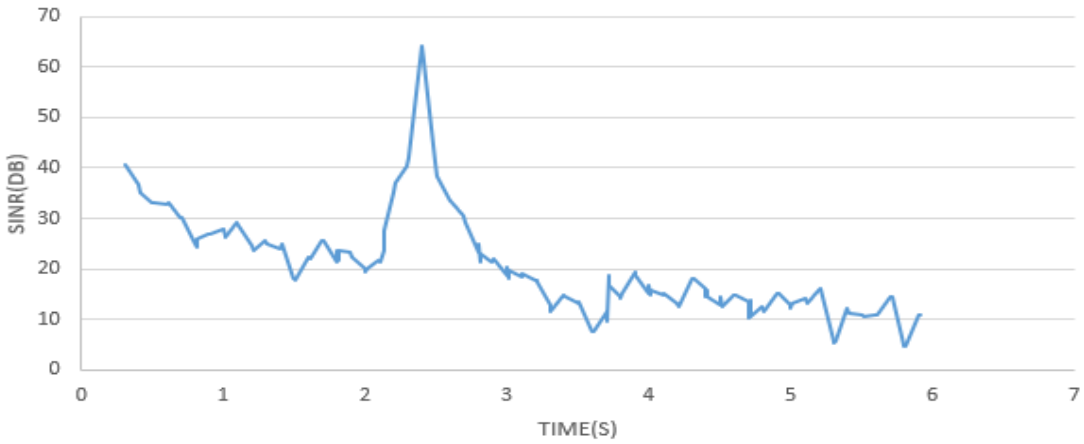

Figure IV.14: SINR value of one user in relation to time

The first scenario describe one user connected to one mmwave base station , and run in a speed of 200 km/h while sending packet toward the second mmwave base station , we created a stable vector to walk in and while the user moving there are a LTE base station in the middle like the previous scenarios. The aim of the second part is to see the effect of high speed to mobility management and how it will handle it.

The throughput graph shows a random value between 1200 Kb/s to 2000 Kb/s, and a huge dropped in packet in 2.3s and 3.8s; unlike the first part in the normal speed here even though the ideal condition but doesn't Ensures stability in data transmission.

The SINR graph decreased in the first part from 40db to 20db but fast jump to 63db while perform the handover to the mmwave base station and return to decreasing while the user drifting away, the SINR range in from 10db to 63db and an average of 28db which is good connection. and we see that the mmwave link is providing an acceptable result.

Second scenario:

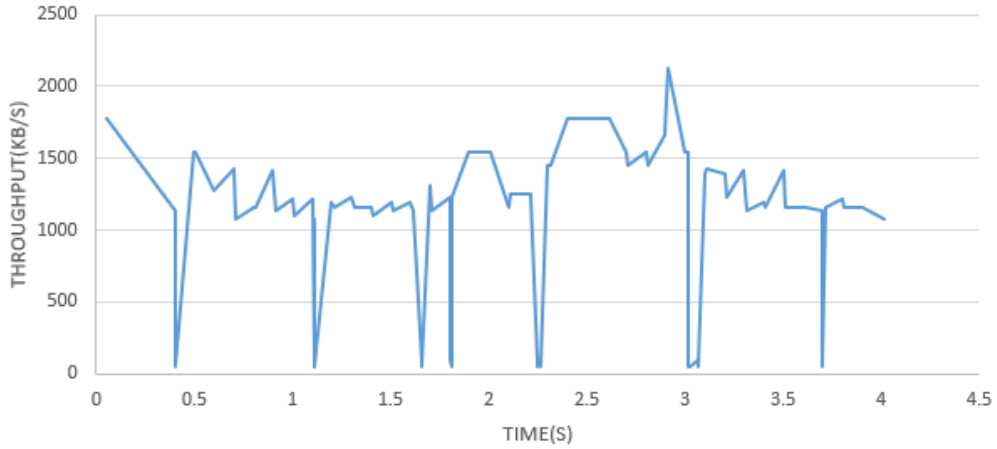

Figure IV.15: Throughput value of 5 users in relation to time

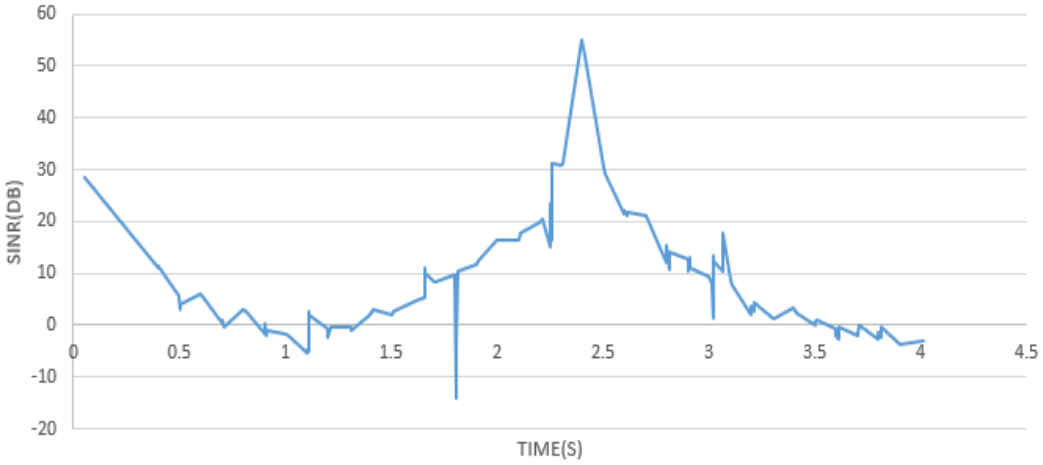

Figure IV.16: SINR value of 5 users in relation to time

The second scenario like the first but the number increased to 5 users connected to one mmwave base station , and runs in a speed of 200 km/h while sending packet toward the second mmwave base station , we created a stable vector to walk in and while the user moving there are a LTE base station in the middle like the previous scenarios.

like the previous the throughput graph shows a random value between 1200 Kb/s to 2000 Kb/s, but the number of dropped packets increased; while its look very random due the effect of high speed here we can tell it's not a good value.

The SINR graph decreased in the first part from 28db to -2db and then keep increasing to 58db while perform the handover to the mmwave base station and return to decreasing while the user drifting away, here the connection link become weaker than ever.

Third scenario:

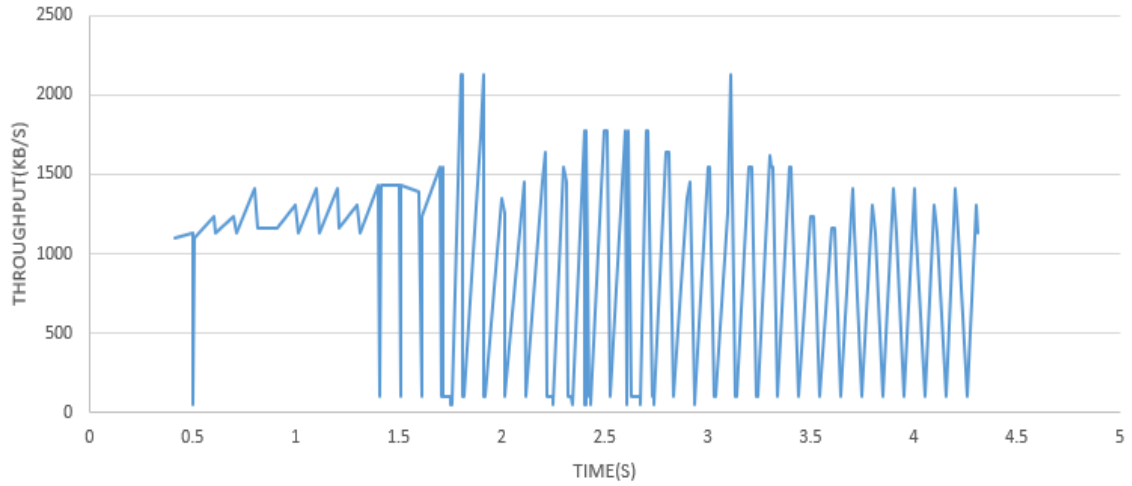

Figure IV.17: Throughput value of 10 users in relation to time

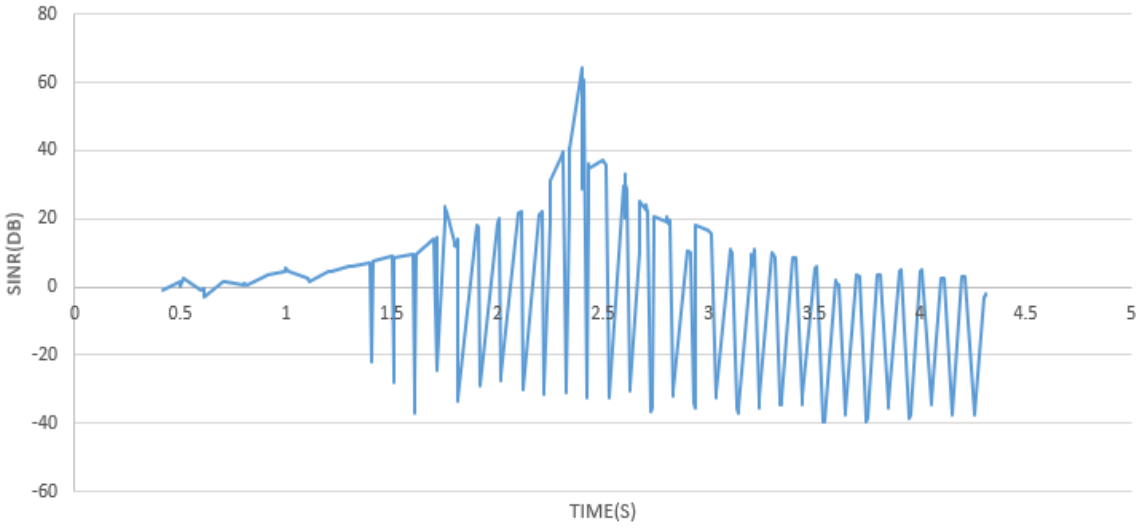

Figure IV.18: SINR value of 10 users in relation to time

The third and last scenario like the second but the number increased to 10 users connected to one mmwave base station , and runs in a speed of 200 km/h while sending packet toward the second mmwave base station , we created a stable vector to walk in and while the user moving there are a LTE base station in the middle like the previous scenarios.

here both the throughput and the SINR graphs show a worse result; here the as the number and speed increased the results become worse than ever.

IV.8 conclusion

In this chapter we saw the potential of the NS3 MMWAVE module, a powerful program that simulate an architecture contain the LTE EPC with the mmwave radio access to give an idea of the future 5G generation. After what we saw the mobility management affected as the density of the network (number of users) increased and also the high speed affected from it a lot and leads to a loses of packets.

General conclusion

After the above which presented the different wireless networks evolving after every generation, delivering every time the best experience all in term of speed, quality of the network and the reliability, which leads to the most advanced and development the 5 generation. We saw also the importance function in the networks which is the mobility management and how it is an essential in the networks.

The 5g make all the users and also the subjects connected to each other that what leads to the internet of things and make it possible , also with the different technologies that the 5G offers among them the new spectrum which is the millimeter waves that offer a higher frequencies than the radio waves between 3 and 300 Ghz, the beamforming that concentrate the millimeters wave to cover more area ,the massive MIMO that increase the number of antenna that increases the traffic and also by using the small cells that is simple and tiny to deploy in the networks to reach the places that the massive MIMO can't reach. Without forgetting the SDN and NFV that reducing the cost and make the 5g network more organizable this technologies work with each other to enhance and bring the next generation to a whole new level.

In the simulation chapter we uses the NS3 MMWAVE module that work with the LTE EPC part and for the radio access uses a custom mmwave MAC and Physique layer, we implemented an architecture that contain the LTE base station and the mmwave base station along with the LTE EPC ,and we saw the impact of registration and the handover to the network , what we reach that in the normal speed the mobility management doesn’t effect a lot but in the high speed along with the number of users can affect the mobility management in both the quality of the links and the receiving packets , which is not a new thing.

The results curves indicate a view of what is the importance of the mobility management that maintain the connection and in the same time bring a good quality, it effects from the handover which keep the developers always in continuous search to reduce the effect of it.

The module brings the radio access of the 5G more to life but to get more results in the future it must cover all the technologies and the core network of the 5 generation.

References

[1] Available Online: https://www.researchgate.net/publication/332035967 consult the 3.12.2019.

[2] Available Online: https://www.rfpage.com/evolution-of-wireless-technologies-1g-to-5g-in-mobile-communication/ consult the 7.3.2020.

[3] TONYE.E et EWOUSSAOUA.L, « Planification Et ingénierie Des Réseau DeTélécoms », mémoire pro 2 de télécommunication, Université de Yaounde I, 2011.

[4] AJGOU.R, et ABDESSELAM.S, Evolution de réseau GSM (GPRS, EDGE).

[5] Available Online : https://www.tutorialspoint.com/lte/lte_network_architecture.html consult the 7.3.2020.

[6] Jun-Zhao, S., Howie, D. & Sauvola, J. (2017). Mobility management techniques for the next generation, wireless networks, University of Oulu, Finland.

[7] Kakesh, K.R. (2016). A frame work for 4G wireless networks-overview and challenges.Journal of Excellence in Computer Science and Engineering, 2(1), 1-10.

[8] Uma, B. & Sumathi, S. (2016). High throughput, privacy and security for handover in 5G networks using software-defined networking. International Journal of Innovative

Research in Science, Engineering and Technology, 5(2).

[9] GPP TS 36.300 "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)"; Overall description; Stage 2;

Version. 11.7.0.

[10] Magister memory presented by H. TALEB " Location of a user in a mobile environment ".

[11] GPP TS 36.304 "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment

(UE) procedures in idle mode" v. 11.5.0.

[12] J. Manner and M. Kojo. Mobility Related Terminology. IETF RFC 3753, June 2004.

[13] GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access" v. 12.2.0.

[14] GPP TS 43.129 “Packet-switched handover for GERAN A/Gb mode; Stage 2”.

[15] Available Online: https://fr.wikipedia.org/wiki/5G consult the 10.3.2020.

[16] ITU-R, ITU-R, Rec. M.2083, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond", 2015.

[17] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2", version 15.3.0 Release 15.

[18] 3GPP TS 38.401: "NG-RAN; Architecture description",version 15.3.0 Release 15.

[19] Rappaport, T. S., Sun, S., Mayzus, R. et al. (2013) Millimeter Wave Mobile Communications for 5G Cellular: It Will Work! IEEE Access, 1, 335–349.

[20] Pi, Z. and Khan, F. (2011) An Introduction to Millimeter-Wave Mobile Broadband Systems. IEEE Communications Magazine, 49(6), 101–107.

[21] Google Image.

[22] Rappaport T.S., Xing Y., MacCartney G. R., Molisch A. F., Mellios E., Zhang J.: Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks-with a focus on Propagation Models. IEEE Transactions on Antennas and Propagation (2017) doi: 10.1109/TAP.2017.2734243

[23] Available Online: https://en.wikipedia.org/wiki/Beamforming consult the 10.3.2020.

[24] "Small Cells, Big Impact: Designing Power Solutions for 5G Applications" by Nicole Lemieux & Mingyue Zhao.

[25] Shafi, M., Molisch, A.F., Smith, P.J., Haustein, T., Zhu, P., De Silva, P., Tufvesson, F., Benjebbour, A., Wunder, G.: 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. IEEE Journal on Selected Areas in Communications 35(6), 1201–1221 (2017). DOI 10.1109/JSAC.2017.2692307.

[26] Mijumbi, R., Serrat, J., Gorricho, J., Bouten, N., Turck, F.D., Boutaba, R.: Network function virtualization: State-of-the-art and research challenges. IEEE Communications Surveys

Tutorials 18(1), 236–262 (2016).

[27] 3GPP TS 38.300, NR, Overall Description, Stage-2 (Release 15), December 2018.

[28] Available Online: https://www.nsnam.org/docs/tutorial/html/introduction.html consult the 9.4.2020.

[29] G. Piro, N. Baldo, and M. Miozzo, An LTE module for ns-3 network simulator, Proc. of Int. ICST Conf. on Simulation Tools and Techniques, pages 415{422, Barcelona, Spain, Mar. 2011.

[30] M. R. Akdeniz, Y. Liu, M. K. Samimi, S. Sun, S. Rangan, T. S. Rappaport, and E. Erkip, Millimeter wave channel modeling and cellular capacity evaluation, IEEE J. Sel. Areas Commun., 32(6):1164-1179, Jun. 2014.

[31] Available Online: https://www.nsnam.org/wiki/Installation consult the 10.4.2020.

[32] Available Online: https://en.wikipedia.org/wiki/Signal-to-interference-plus-noise_ratio consult the 10.4.2020.

[33] Available Online: https://www.cablefree.net/wirelesstechnology/4glte/rsrp-rsrq-measurement-lte consult the 10.4.2020.

[34] DJAMEL EDDINE BELGHOUL, MEBARKIA WALID: Study and modeling of the deployment of heterogeneous networks LTE-Advanced BELGHOUL, diploma of state engineer in computer science, National School of Computer Science, 2013/2014.

[35] Optimization of QoS in 4G Networks Using Handover Management NAMRATA KATTI, SEEMA SHIVAPUR, VIJAYALAKSHMI M. Department of Computer Science BVBCET, Hubli.