Analysis of security vulnerabilities in 5G standalone network

A DISSERTATION

submitted in partial fulfillment of the requirements

for the award of the degree of

Master of Technology

in

Wireless Communication

by

Meemoh Haque

201915010

Under the supervision of

Dr Priyanka Mekala

Dr.Supriya Goel

Dhirubhai Ambani Institute of Information and Communication Technology

June 2021

CERTIFICATE

I hereby certify that the work which is being presented in the M.Tech. thesis entitled **“”An Analysis of finding security vulnerabilities in 5G standalone network”,** in partial fulfillment of the requirements for the award of the **Master of Technology in ECE with specialization in Wireless Communications** is an legitimate record of my work carried out during August,2020 to June,2021 under the supervision of **Dr.Priyanka Mekala Assistant Professor, and Dr. Supriya Goel, Assistant Professor**, Wireless Communication System Lab,CR Rao AIMSCS Hyderabad,India

The matter presented in this thesis has not been submitted for the award of any other degree elsewhere.

Meemoh Haque

Signature of Candidate

Meemoh Haque

Roll No. 201915010

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

PriyankaMekala	Supriya
Dr. Priyanka Mekala	Dr. Supriya Goel
Thesis Supervisor	Thesis Supervisor

ACKNOWLEDGEMENT

First of all, I express my gratitude to the Almighty, who blessed me with the zeal and enthusiasm to complete this research work successfully. I am extremely thankful to my supervisors , Dr Supriya Goel , Assistant Professor,Wireless Communication System Lab,CR Rao AIMSCS Hyderabad and Dr Priyanka Mekala Assistant Professor,Wireless Communication System Lab,CR Rao AIMSCS Hyderabad for there motivation and tireless efforts to help me to get deep knowledge of the research area and supporting me throughout my M.Tech. dissertation work. Especially, the extensive comments, healthy discussions, and fruitful interactions with the supervisor had a direct impact on the final form and quality of M. Tech. dissertation work.

I am also thankful to Director, CR Rao AIMSCS Hyderabad for his constant support during the research work. I wish to thank the Research Staff of CR RAO AIMSCS Hyderbad for their full support and heartiest co-operation.

This thesis would not have been possible without the hearty support of my friends. My deepest regards to my Parents for their blessings, affection and continuous support.

(Meemoh Haque)

ABSTRACT

The first release of the 5G protocol specifications,3rd Generation Partnership Project (3GPP) Release 15 was released in 2017 and the first 5G protocol security specifications was published in 2018. There are various development made in the area of 5G which aims to connect various aspects of human life, no matter Whether it is rural area or urban,5G aims to provide a higher network speed, low latency and ubiquitous connectivity. 5G illustrates the convergence of various use cases of wireless communication and computer networking , which includes the components such as Software Defined Networks (SDN),Network Functions Virtualization (NFV) and the edge cloud.Due to the convergence of both technology it leads to various security challenges in SDN/NFV when connected with the 5G network.In future 5G will play a very crucial role in our life,thus network must ensure that all its components and the services which it is providing to the users must be secure. The threat landscape in 5G is huge as with 5G a large number of devices will be connected with the network. The Manuscript discusses about various vulnerability and security threats that exists in 5G networks. A complete end to end 5G standalone test bed is used for analyzing the security threats. Device capabilities ie.core and radio capabilities and pre-authentication signalling message are not security protected in 5G. Security features as compared to legacy network has been improved like the encryption of International Mobile Subscriber Identity (IMSI) but still there are known vulnerability that existed in LTE still exist in 5G which need to be investigated before deploying 5G worldwide.

Contents

List of Figures

List of Tables

List of Abbreviations

3GPP Third Generation Partnership Project

CA Carrier Aggregation

LTE Long Term Evolution

IMSI International Mobile Subscriber Identity

SUPI Subscription Permanent Identifier

MIMO Multi Input Multi Output

RRC Radio Resource Control

NAS Non Access Stratum

UE User Equipment

emBB Enhance Mobile broadband

URRLLC Ultra-Reliable Low-Latency Communication

DOS Denial of Service

mMTC Massive Machine Type Communications

SDN Software-Defined Networking

NFV Network functions virtualization

TMSI Temporary Mobile Subscriber Identity

SUCI Subscription Concealed Identifier

HPLMN Home Public Land Mobile Network

NSSF Network Slice Selec- tion Function

EEA EPS Encryption Algorithms

EIA EPS Integrity Algorithms

AMF Core Access and Mobility Management Function

AUSF ,Authentication Server Function

UDM Unified Data Management

SBA Service-Based Architecture

NGMN Next Generation Mobile Networks

PDCP Packet Data Convergence Protocol

TAC Tracking Area Code

NGAP NG Application Protocol

Chapter 1

INTRODUCTION

1.1 Introduction to 5G

With the increasing demands of users and revolutions in technology, there is an evolution in mobile network to meet the demands of the higher bandwidth, extensive higher data rate and ultra low latency [2] .5G will be able to solve the last-mile/-kilometer problem and provide a broadband access to the numerous users at very much lower cost as it will be using new spectrum and improvements in spectral efficiency [36]. It target orders of increase in magnitude of data rates, spectral bandwidths,device connectivity and coverage area. 5G aims to achieve 10 Gbps data rates in cellular networks. As compared to LTE there will be increase of data rates of up to 100 times of order 150 Mbps [5].

In terms of dense connectivity 1 million devices per square kilometre to support dense connectivity in Machine to Machine and IOT applications. There is a significant higher reliability as compared to previous generation . It requires 99.999% availability thus small probability of outrage. LTE system which is currently widely used operates in the range of frequency of 300 MHz to 6GHz band which is highly inadequate to meet the demand of higher data rates and connectivity in 5G , for overcoming these shortcoming the concept of mmWave [1] will be used which exploits the high frequency band ranging from 6-300 GHz thus significantly improving the data rates. There are various new 5G technology namely mmwave MIMO ,

Massive MIMO [15] , Non-orthogonal Multiple Access (NOMA) [16] , Cooperative Communication and Cognitive radio [18].

Various use cases that will be served with the upcoming of 5G network are namely :

1) **Enhance Mobile broadband(emBB)** : It aims to provide higher data rate as compared to previous generation. As compared to 4G, fifth generation network(5G) aims to provide 10 to 100X increase in the data rate ie. 10 Mbps.

2) **Ultra-Reliable Low-Latency Communication (URRLLC)**: This particular use case includes lower error rate and a very low latency. Requirement of a very high data rate is not that much required in mmTC.

3) **Massive Machine Type Communications (mMTC)**: With the Increase in number of IOT devices, huge data will be generated out of it. mmTC will deal with the dense massive connectivity of such IOT devices.

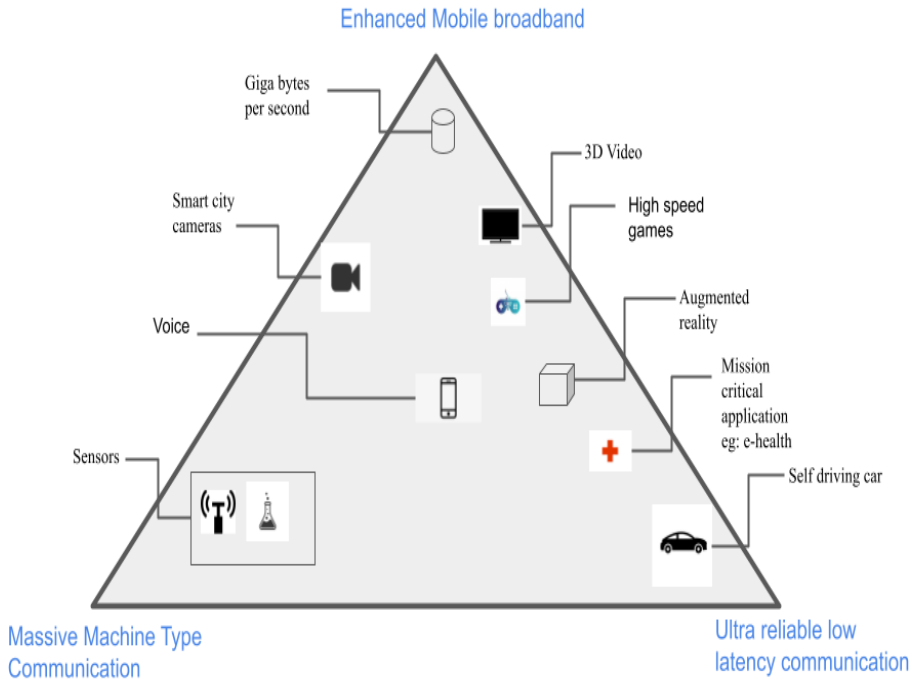

Figure 1.1: 5G Use Cases

SDN and NFV are the two main technologies that will support virtualization and hence will help in overcoming vendor lock in issue. SDN/NFV mainly includes various additional network components including: SDN controller, Orchestrator, Hypervisor, Security Function Virtualization, all of which introduce security risks. Besides SDN/NFV, there are other technologies such as cloud RAN, Mobile Edge

Cloud (MEC) and Network Slicing that will enable resource sharing in a optimal way and support low latency applications.

1.2 Advancement in 5G

- 5G uses a total new security architecture called Security Based Architecture(SBA). In SBA it requires that the controlling plane has to enable the security protection so that all the network function in the architecture securely and efficiently communicate within its serving network domain and also in other network domain [21].

- There is a stronger identity privacy protection. Unlike the legacy network in 5G the Subscriber Identity number(SUPI) is concealed and encrypted into Subscription Concealed Identifier(SUCI) and thus it is not released in plain text [6].

- In 5G after the authentication procedure authentication response is also send to Home Public Land Mobile Network (HPLMN) through control plane signalling . Thus there is increase in home control and higher security protection [21].

- Diameter which was the application layer protocol in control plane signalling in 4G has been replaced by more enhanced and efficient protocol HTTP/2 in 5G.

- The S-GW and P-GW has been divided into control plane and user plane ie. SGW $\rightarrow$ SGW-C and SGW-U , PGW $\rightarrow$ PGW-C and PGW-U.

- In 5G when UE selects the cell outside the registration area then it sends new registration request of type mobility updating instead of sending tracking area update in 5G.

- There is a new network function introduced in 5G called Network Slice Selection Function (NSSF) , it redirects traffic to a network slice. It also selects network slice instance to serve the UE.

1.3 New Technology Introduced in 5G

There are various new technology introduced in 5G that will help to support various new 5G use cases . Below there is a list of few technology that will play a key role in the deployment of 5G to support higher data rate, ultra low latency and higher dense connectivity :

1) Small Cells : Small cells are basically portable small base stations that can operate on minimal power [39] and can be accommodate every 250 meters in the city . It can help to prevent the signal to be dropped in the dense network. In the current traditional network it requires a large number of base station to achieve good connectivity , thus for 5G it will require a higher infrastructure. In small cells the size of antenna will be very small which will be transmitting millimeter waves. With the use of small cell there will be efficient use of the spectrum.

2) Massive MIMO : 4G base station can support a maximum of dozen antenna port, but in 5G it can support more than hundred antenna port at once, thus many antenna can be accommodate on a single antenna array [15] . Due to large antenna array it will increase the capacity of the mobile network drastically. This technology of supporting massive antenna array is called MASSIVE MIMO. MASSIVE MIMO is the future of 5G networks but with the large use of antenna there will be problem of interference which can be resolved by beamforming.

3) Full Duplex : Base stations and cellphones in traditional network depends on transceivers that interchange there roles if they are transmitting and receiving information over the same frequency, or operating on different frequencies if a user want to transmit and receive information at the same time.

With the advancement in 5G, a transceiver can transmit and receive data at the same time, on the same frequency [40].

The technology is termed as full duplex. for designing full duplex in devices, researchers have to design a circuit that can let the incoming and outgoing signals in such a way that they don't collide while an antenna is transmitting and receiving data at the same time.

1.4 Background & Motivation

Various security Advancement has been made in various generation namely 2G, 3G and 4G . In 2G there was the concern of fake base station attacks and also there was only one way authentication [22]. In 3G various Internet Protocol (IP) related vulnerabilities was found . 4G was more IP based network and due to the increase in the IP traffic it encountered various attacks eg. Denial of service (DOS) attacks. With the upcoming of 5G various new development is made like increase in data rate and reduction in latency but with all these advancement there are various security concerns with 5G . In [6] it was found that 5G is still vulnerable to attacks which was prevalent in legacy network.The solutions for various security concerns and architecture that were used in legacy network (3G & 4G) cannot be used in 5G. Similar like LTE security is the major concern in 5G. with the dawn of 5G protocol specification for the 5G system there have been numerous effort to overcome the protocol exploits that were encountered in the LTE. In LTE there is a issue of International mobile subscriber identifier (IMSI) catching , to overcome these issue 5G introduces Subscription Permanent Identifier (SUPI) which replaced IMSI , and with the advent of public key infrastructure (PKI) SUPI has been encrypted into Subscription Concealed Identifier (SUCI).

In LTE the pre-authentication message prior to security establishment were found to be insecure and was exploited by the attacker to launch various attack like bidding down and denial of service [4] , this particular aspect of pre-authentication message exploit has to be taken care in 5G as well , also it was found that in LTE various device capabilities were exposed in clear text and attacker by disabling it can downgrade the performance of the user , As 5G device will come more enhance device capabilities the operator must make sure to secure these capabilities.

In the below section the scope and the objective of the work will be discussed .

1.5 Scope & Objective of the present work

The scope & objectives of this thesis described as shown below :

- Designing of a complete end to end 5G standalone network using two open source tool.
- With the help of the 5G network the aim is to find security vulnerabilities in the network as per 3GPP standards.
- By finding the security loopholes the objective is to make the 5G network more secure when it will be deployed widely.

1.6 Our Contribution

The Contribution in the thesis of the author is listed below:

- Design of a 5G standalone test bed which consist of all the specification and procedure as per the 3GPP standards.
- Found various vulnerabilities in the 5G network which can affect the performance of the user on the UE side.
- The vulnerabilities were analyzed between UE and gnodeB. It was found that various pre-authentication message are not security protected along with that the device capabilities similar like LTE are exposed in clear text which can be exploited by the attacker to downgrade the performance of the user.

1.7 Thesis Outline

The thesis has been structured as follows:

- Chapter 2 consist of the literature survey which consist of security issues in various legacy network. It also discussed about the network architecture of 5G, Registration procedure and various recommendation for 5G security.
- Chapter 3 discusses about the Experimental setup and Methodology adopted by the author.
- Chapter 4 discussed about the results that is obtained by the experimental setup and its corresponding impact on the network.
- In the final chapter ie. chapter 5 discusses countermeasures and conclusion of the work is discussed.

Chapter 2

Literature survey

2.1 Security in Legacy network

2.1.1 Security in 1G

The cellular system has been evolved from 1G to now 5G, speed in each generation is increasing,so does it's security. In 1G it used analog communication.In analog signal processing it was difficult to provide efficient security services for 1G. In analog signal processing it was difficult to provide efficient security services for 1G. Data services and roaming was not included in 1G mobile network service list but mobile security threats start arising with the introduction of 1G. If the attacker need to eavesdrop a call, he have to utilize a radio scanner and tune it to the required frequency. By eavesdropping the calls, the attacker can obtain all the crucial user credentials such as the Mobile Identification Number (MIN) and Electronic Serial Number (ESN). These critical credentials can be used to clone another user to duplicate the original subscriber. 1G lacks mutual authentication.In 1G it used scrambling methods to protect the user information but these scrambling methods were not able to prevent the scanning threats, although it was not strong as encrypted methods used in later mobile generations.

2.1.2 Security in 2G

2G mobile networks came into existence in 1991. 2G provided voice as well as messaging features for the mobile users. 2G introduce data services, i.e.SMS (Short Message Service). 2G network provided various security features such as authentication of subscribers using shared-secret cryptography, encrypting the radio interface traffic and protecting the confidentiality of the subscriber's identity was achieved in 2G Network. With 2G network SIM (Subscriber Identity Module) card was introduced. SIM is used in each mobile phone and it is used to verify the identity of the mobile subscriber. 2G suffered from various set of security challenges. In 2G networks, attackers started using spamming as a pervading attacks for transmitting malicious information to the users. Due to which it resulted in a transmission of spam messages to user mobile. Interrupting the mobile communication with fake authentication parameter of rogue Base station was one of the security issue in 2G [24], [25]. It is found that still the future generation network suffers from the same issue. Stream ciphers, i.e. A5/1 and A5/2 are used in 2G networks to encrypt the calls . SMS is also vulnerable to security vulnerabilities due to its store-and-forward nature

2.1.3 Security in 3G

Third generation(3G) network supports high data rates and brand new services such as video calling , MMS (Multimedia Message Services), mobile television and mobile internet. Learning from 2G security there were various security advancement made

Table 2.1: Some security issues in 3G

S.NO	**Threats in 3G**
1	man in the middle attack
2	De-registration request spoofing
3	Location update request spoofing
4	Rogue base station

in 3G . The important security issues in 2G networks such as false Base station attack were corrected in 3G. 3G security architecture comprised of five important

set of Characteristic :

1) access security in network

2) domain security in network

3) domain security of user

4) application security

5) configurability and visibility of security [25].

3G networks were vulnerable to various attacks mainly comprises of eavesdropping, impersonation of a subscriber, user impersonation with compromised authentication vector such as RAND,AUTN etc, man-in- the-middle attacks, denial of service attacks by executing de-registration spoofing, location update spoofing and residing on a false Base station.

For the 3G security, data of the user and few signaling information are considered sensitive and therefore it should be integrity and confidentiality protected. The mechanism in UMTS that provides the guarantee of integrity in 3G is nothing but UMTS Integrity Algorithm which has been used in both the base station. The integrity algorithm operates only on the signalling data so to take care of both user and signalling data confidentiality mechanism has to be used. The confidentiality mechanism used in 3G is f8 algorithm.

2.1.4 Security in 4G

In 4G-LTE mobile devices switched were E2E (End to End) architecture and were IP based. 4G can attain a highest speed of up to 100 Mbps. The security architecture of 4G is the enhanced version of 2G and 3G networks. With 4G a new set of cryptography algorithms were introduced . EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA) were used [26] .Keys in 4G are 256-bits long whereas in 3G is 128 bit long. The primary 4G authentication mechanism in LTE is the Authentication and Key Agreement (AKA) protocol .

Index No.	Various Protocol Exploit found in LTE	Various List of Threats found in LTE
1	IMSI exposed in clear text	Device tracking,leak of location [37]
2	Initial Attach/Tracking update request	Denial of service [12]
3	Location tracking using RNTI	monitoring of the device , location leak [38]

For integrity and replay protection. 4G uses NAS (Non-Access Stratum) and RRC (Radio Resource Control) signaling protocol.Due to the IP connectivity of 4G core network with the Internet, it becomes open to millions of attackers and new security threats from the Internet . 4G networks is vulnerable to various IP based attacks such as IP address spoofing,TCP SYN DoS, User ID theft, Theft of Service (ToS), DoS(Denial of Service).

In 4G there is an issue of International Mobile Subscriber Identity (IMSI) catching ie.when a UE attach for the first time with the network in 4G it sends its IMSI in clear text in air interface which can be intercepted by the attacker to launch various attack to the user.

Main security threats in LTE [27] :

1) Physical attacks- A particular UE can be physically altered and it can be used to access and attack operator networks thus affecting the performance of the network.

2) Man-in-the-middle attacks- In man in middle attack an attacker intercept transfer of the user's identity between the UE and enodeB without any encryption. It is one of the weakness in the LTE.

3) Attacks on privacy of UEs. In LTE Attackers can use the paging procedures to track the mobile phones, injecting the paging requests several times and thus equate the temporary identity (TMSI) which was collected of the mobile phone with the paged permanent identity IMSI.

4) DoS and DDoS attacks. In DOS or DDOS the attacker can flood the network with all the signalling message , thus the service to the user can be compromised. compromised;

2.2 5G architecture and registration procedure

5G architecture is evolved with a number of advancements and changes like the base station is divided into Centralised unit(CU) and Distributed unit (DU).

In 5G there are two modes of network , one is standalone mode and the other is

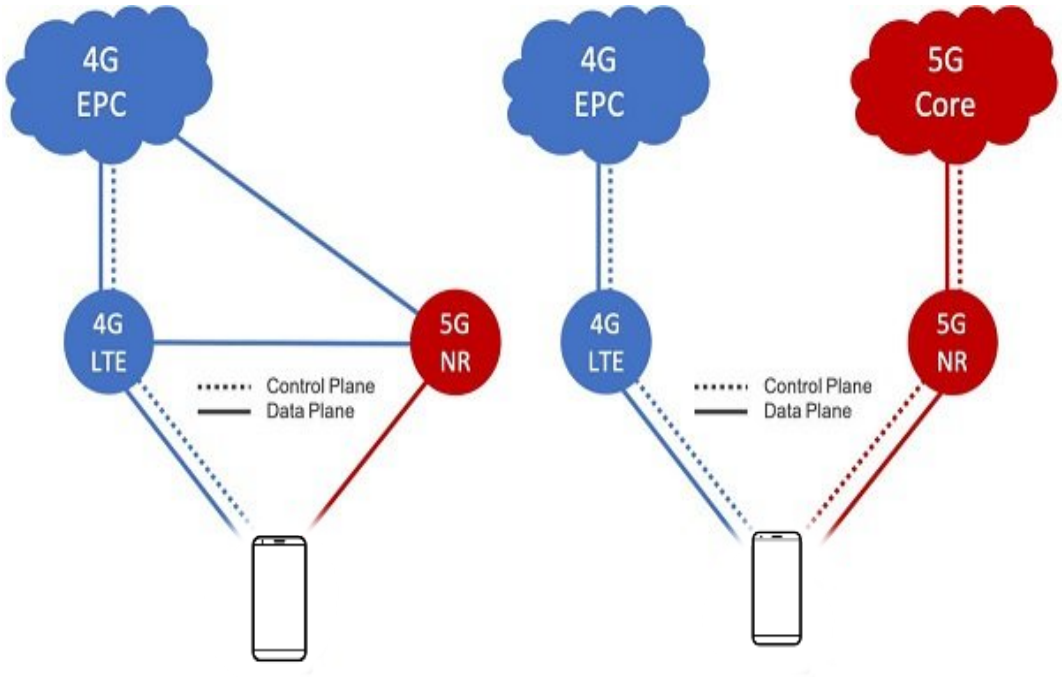

Figure 2.1: Different modes of network in 5G

non standalone mode as shown in the figure 3.1 . In non-standalone mode there are 5G NR but the UE will still be connected to 4G core and base station for signalling purpose. 5G NR only performs data offload hence 5G network cannot perform independently. Standalone mode is the future 5G network where base station is 5G NR and the core network is the 5G core .Figure 2 depicts a simplified 5G network architecture which comprises of User equipment(UE),5G access network(AN), core network and finally the data network.Unlike 4G in 5G the access network ie, gnodeB is divided into control plane and user palne. In LTE it is mainly connected state and idle state but in 5G there is a new state called deactivated state.

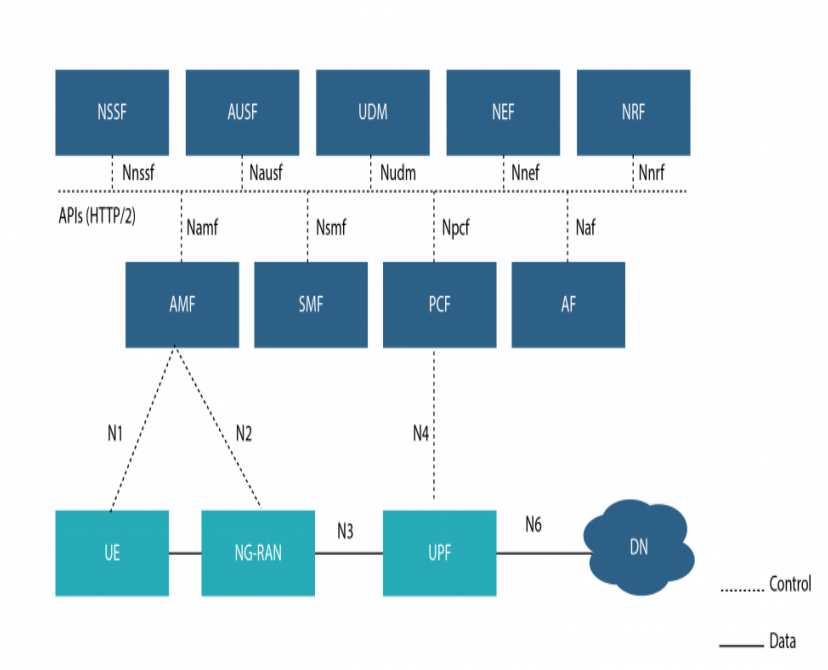

Figure 2.2: simplified 5G network architecture

2.2.1 Network architecture

Some of the important entities in 5G network are UE,access network and core network.UE is basically comprised of two parts.one is ME and the other is USIM. ME is the physical hardware which consist of IMEI which uniquely identifies the device and the USIM is the universal identity module which stores the information such as subscriber's SUPI, root key and public key. The SUPI is always encrypted and never released in air in clear text. 5G access network comprises of various gnodeB and divides the geographical area into various hexagonal cells. Whenever a UE want to establish a connection with the 5G core network it does it with the help of access network.gnodeB allocates radio resource to UE to setup the connection with the network. Core network consist of different network function such as Core Access and Mobility Management Function(AMF) ,Authentication Server Function(AUSF),Unified data management(UDM),Policy Control Function(PCF) etc. we will be discussing three important network function ie. AMF,AUSF and UDM. AMF is the access mobility management function which is responsible for registration procedure, mobility procedure, connection and reachability. It is the termination point for NAS signalling procedure. AUSF is the authentication server function which is responsible for managing the authentication procedure of both

3GPP and non-3GPP access.UDM is the unified data management which provides all the authentication credentials for 5G-AKA and and also it is responsible for storing and the managing the user identity information such as SUPI for 5G network.

2.2.2 Registration procedure in 5G

With 5G there have been various development made in various important procedure in 5G. The call flows is quite complex as compared to 4G. A simplified diagram of various flows is shown in the figure 4.

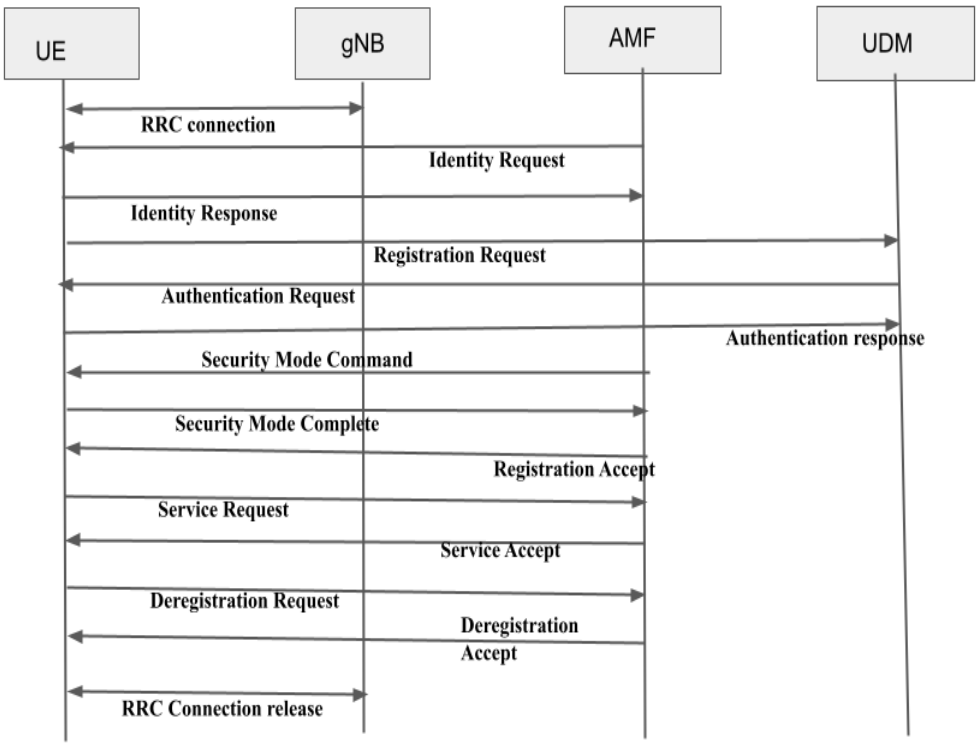

Figure 2.3: Registration procedure in 5G

In 5G initial attach message has been replaced by registration request message.After the registration procedure the network initiates the authentication procedure by sending a challenge in the form of authentication request which contains parameters like RAND and sequence number . If the UE succeeds it sends authentication response with the unique value RES otherwise it sends authentication reject with cause of either MAC or SYNC failure.After the authentication procedure network and UE need to reach to an agreement regarding the keys and algorithm to be

used in encryption which is done by security mode command. If the UE needs to de register and want to logout from all the resources allocated to it it sends deregistration request to the network and finally if UE due to roaming or any other reason lost the temporary identity information it initiates the identity request to the network.

2.3 Security in 5G

5G is committed to provide uninterrupted broadband services, it will provide connectivity to massive number of devices in the form IoT, and will provide the users and devices with high mobility in an ultra relia ble and affordable way [26]. As 4G was complete IP based network it opened door for various market opportunities . With 5G there is a new wave of a complete new ecosystem introducing various new use cases for vehicles, home appliances, health care, industry, businesses, etc., . With all these new developments there comes a new array of various threats and security vulnerabilities that will create a major challenge to both present and future networks [27]. Connecting the Bank for instance, 5G will connect critical security and high data speed infrastructures to the network, hence if any security breaches occur in such critical infrastructures can cause a huge catastrophic impact on the organization to which 5G serves. Thus, security of 5G and the system which is connected through 5G must be designed taking all the required precautions . In the below subsection, an overview of 5G security architecture is given, concentrating on the various security domains.

2.3.1 5G security Architecture

The security architecture is defined by 3GPP [21] consist of application stratum,transport stratum and serving stratum .

Figure 3 shows the simplified diagram of the security architecture of 5G which consist of following security domains :

- Network Access security(I) : The particular domain deals with the features and the mechanism that qualify the UE to authenticate and securely access

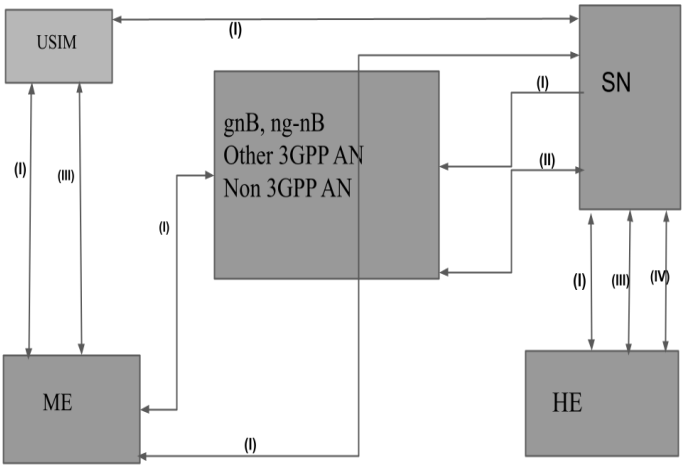

Figure 2.4: Security Architecture in 5G

the serving network. It includes all the 3GPP and non-3GPP access to secure the attacks on the radio interface. It also includes all the security context exchange between USIM and home environment (HE).

- Network domain security (II) : It includes the set of features and methods that makes the network nodes securely exchange the control plane and user plane within the networks.

- User domain security (III) : It includes all the sets of mechanism and features that helps to secure the access to user equipment's.

- Service-Based Architecture (SBA) domain security (IV): The particular domain includes security features such as network function registration, authorization and discovery for securing service based interfaces. It allows the network function in the service based architecture to securely communicate with each other and also checks weather if any new network function is implemented is properly securely integrated or not.

- Visibility and configurability of security(not included in the figure 3) : It includes the set of features and mechanism which makes UE know that the security feature which is implemented is in operation or not.

2.3.2 Recommendation for the security of 5G

Various recommendation has made by the Next Generation Mobile Networks (NGMN) for 5G network based on legacy network architecture and also due to the loopholes in the security measures adopted in previous network [7]. The recommendation includes the security challenges in access networks, and also various cyber-attacks against the users . In detail various recommendation proposed can be found in [7] and the important points are summarized below

1) Flash network traffic: It is estimated that the number of end user devices in 5G will grow exponentially which will consequence in significant Increase in the network traffic patterns which either non-intentionally or with a malicious intent. Thus, 5G must be able to successfully handle large increase in traffic and the network must provide durability whenever there is increase in traffic and also maintaining threshold level of performance.

2) Security in radio interface keys:In the legacy network architecture, also including 4G, in the home network the radio interface key is generated and it is sent to the visited network over insecure links and thus causing exposure of keys. Therefore it is necessary to secure the key first or it should not sent over insecure links such as SS7/DIAMETER.

3) User plane integrity:The UMTS and LTE systems provide protection to few signaling messages but it does not provide cryptographic integrity protection for the user data plane.Hence,it is stressed to provide protection at the transport or application layer .However, providing encryption at application layer will result in excess overhead for data transmission in packet headers and handshakes. Thus, it will be difficult to provide security to resource constraint IOT devices and lower latency 5G network.

4) Consistent in subscriber level security policies: When a user moves from one operator to another it should maintain the security measures. There can be a possibility that the security policies are not updated when user moves from one operator to another. To overcome these some subscription information and security policies

can be exchanged between the operators . This hints the possibility of using virtualization techniques so to keep security of the user or service unharmed with roaming.

5) Denial service attacks on the Infrastructure: DoS and Distributed DoS (DDoS) attacks can affect the operation of the network drastically. In DoS attacks the attacker exhaust the resources of the targeted devices. This threat can be more catastrophic as the machines that are located geographically far apart can launch attack to the user.Hence, the 5G network must be robust by adopting strong security measures against such attacks.

2.3.3 Crucial Areas in 5G security

The following section list out the challenging security issues related to the crucial security areas in 5G, i.e, access control, authentication, communication and encryption.

1) Authentication : Authentication plays a crucial role in confirming whether the device which wants to connect with the network is valid or not and vice versa . There are various authentication procedures involved in each generation, but in these section there will be emphasis on the 5G authentication procedure. Authentication is mainly divided into primary and secondary authentication. Primary authentication ensures device and network mutual authentication. In 5G primary authentication there is a built in home control mechanism by which the network is also acknowledged that the authentication process is completed successfully. In 5G there are basically two authentication mechanism used namely 5G-AKA and Extensible Authentication. Protocol (EAP)-AKA. Primary authentication can also be executed over non-3GPP technologies since it does not depend on Radio Access technology. For the data network outside the mobile operator domain it uses secondary authentication. For Mutual authentication key management and primary authentication procedures is used. For Mutual authentication and for provisioning keying material between the UE and the network key management and primary authentication procedures are used. An Anchor key KSEAF is provided by primary key and authentication management procedures . Authentication Server Function (AUSF) which

belongs to the home network provides KSEAF for the SEAF .Network Function(NF) issues UEs identity and serving network name to the AUSF so that it can perform the authentication. AUSF later uses the information provided by AMF for 5G AKA or EAP-based authentication Fig and

.

2) Access Control: The main objective of access control is to perform selective restriction to access the network for the users .It provides safe and secure environment for the users. It is the main pillar for any network security system. By the help of access control systems only authentic user are allowed to access the system. In [28], the author proposed an access selection scheme which was meant for D2D PLS along with multiple eavesdroppers. In the following proposed scheme, keeping the distance as threshold, D2D communication devices share their spectrum with the cellular users. The authors create a interference which is used by the authors to basically mislead the eavesdroppers through jamming. If there is a Optimal throughput achieved in the access selection scheme it will optimize the security level from eavesdroppers. D2D protection pair basically use to protect a single user. In [29], authors proposed Accountable and Privacy- Enhanced Access Control (APAC) to guarantee user privacy.

3) Communication Security : 5G communications projected to provide high data bandwidth,low latency communication and extensive signal coverage to support a wide range of 5G Use cases. Thus, 5G communication technology will be updated along with the architectural changes and integration of new technologies. With the introduction of new technologies and advancement it can lead to various security issues [30]. Various vulnerable area in the 5G communication are: UE side , Access network and 5G core network. It is also necessary to check the security of legacy network ie 2G,3G and 4G as the 5G network still suffers from the security threats encountered by the legacy network.

4) Encryption : Encryption is basically used to guarantee the confidentiality of data. End to End encryption is very much necessary in 5G network due to the introduction of new set of network services.

At Packet Data Convergence Protocol (PDCP) layer the radio traffic in 5G is en-

crypted just like 4G LTE network [33],For user plane, Non-Access Stratum (NAS) and Access Stratum (AS) there are three different 128-bit encryption algorithm. Some of the legacy network like LTE encryption algorithm will also be used in 5G . In 5G EPS encryption algorithm like null, SNOW3G and Advanced Encryption Standard (AES) will be used same as LTE [34] . In terms of identifier in 5G NR EEA (EPS Encryption Algorithm) is replaced NEA (NR Encryption Algorithm) [6]. In 5G the IMSI is encrypted and is never released in clear text in air .Due to IMSI catcher the attacker can track the subscriber. Thus , it helps to avoid the IMSI based attack . In [35] the author proposed a enhanced level of encryption algorithm for avoid IMSI catching.

2.4 Reviews on 5G and legacy network Security

An illustration of the related work in 5G security and finding vulnerability in 5G network is described in the following section: fields. Some of them are mentioned below:-

1) In [4] authors found various vulnerabilities in 4G network . Core network and radio network capabilities is intercepted by the enodeB before establishing the required NAS and RRC security. This loophole lead to various attack like device identification,Battery draining and bidding down attack.

2) In [6] the authors discussed about the various potential vulnerabilities and challenges involved in the security of 5G along with the possible solution for Pre-authentication message exploits.It also discuss impact of LTE protocol exploit on 5G.

3) In [2] authors discussed about the various 5G security threat and its landscape . Security landscape of various new 5G technology such as Software Defined Networking (SDN), Network Function Virtualization(NFV), cloud computing, Multi-access Edge Computing(MEC) and Network Slicing (NS) concepts were discussed in detail.

4) In [3] authors highlighted the issue of security in new 5G technology such as Software defined networking(SDN)and network function virtualization(NFV) . It also highlighted various issues around the 5G network and also provided a possible solution for all security threats in 5G.

5) In [9] the paper discussed a vulnerability in 5G-AKA where when we run two 5G-AKA session(race condition) simultaneously due to which the credential of one user user is assigned to another user.

6) In [10] the author examined the 5G paging procedure and found that the malicious user can link the subscriber's phone number with their IMSI and can track the subscriber location using the side channel information.

7) In [11] a systematic approach has been adopted for attacks and its respective countermeasure for mobile networks.

8) In [23] author have designed a formal methods to basically model and analyze various security properties of 3G AKA and found that the protocol vulnerability which was found can be exploited to break unlinkability of subscribers.

9) In [17] the authentication method mainly 5G AKA used in 5G was formally analyzed . It was found that the 5G AKA is vulnerable to linkability attack 10) In [27] authors proposed a detailed analysis on the data link layer of LTE protocols and discovered that a resourceful adversary can execute DNS spoofing attack.

11) In [22] authors found a significant quantity of attacks in relation to LTE system by using a symbolic model checker and a cryptographic protocol verification tool.

Chapter 3

Experimental setup and Methodology

3.1 Experimental Setup

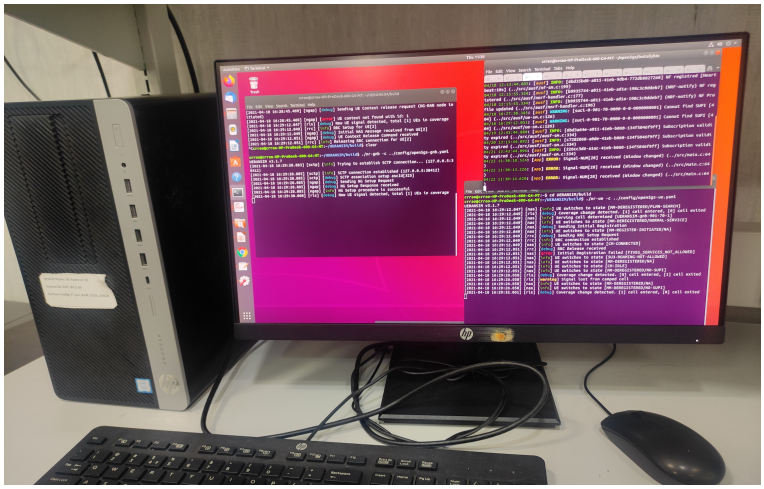

Figure 3.1: Test bed Enviroment

An end to end 5G standalone test bed is build using two open source software is as shown in Figure 3.1 to analyze the vulnerability in 5G network. The experimental setup consist of one i7 PC using Linux OS. In the system two important open source tool is used for building up an end to end test bed .The first open source tool is open5gs [31] which is the core network consisting of various 5G network function .For the RAN and UE an open source platform called UERANSIM [32] is used . The detail explanation of the tool and its features will be explained in the subsequent

section. The integration of the platform has been done . It supports various security encryption algorithm such as 5G EA0, EA1 etc and for the authentication procedure it supports 5G-AKA which is the enhanced version of EAP-AKA. It also supports exchange of various crucial signalling message between UE, gnodeB and the core network.

For integrating the 5G core and the gnodeB it was made sure that the internet protocol(IP) address of AMF and gnodeB is same , the tracking area code (TAC) is maintained same for both UE and gnodeB. The figure 3.2 shows the wireshark capture of various Signalling messages which is exchanged between UE and the 5G network.

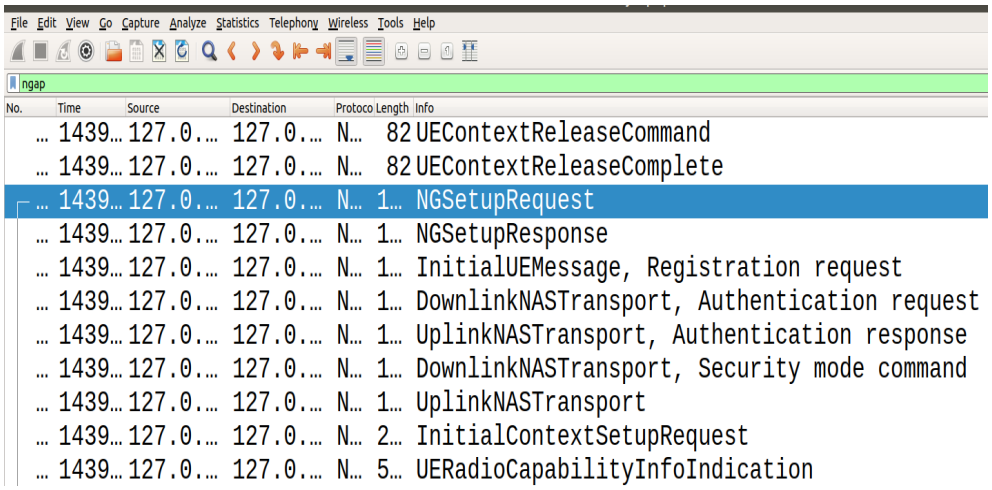

Figure 3.2: Data packets captured in wireshark in experimental setup

With the help of our testbed we were able to capture various device capabilities as well as pre-authentication messages.

3.1.1 Open5gs

Open5GS is a complete C-language based implementation of 5G and LTE core network. it is release 16 compliant and supports AES, Snow3G, ZUC algorithms for encryption. It supports features like USIM cards using Milenage , IPv6 ,Multiple PDU session and also it supports handover ie for 5GC Xn/N2 handover and for EPC it supports S1/X2 handover. For voice calling it supports VOLTE (voice over LTE). Figure 3.3 depicts the open5gs platform in the linux enviroment.

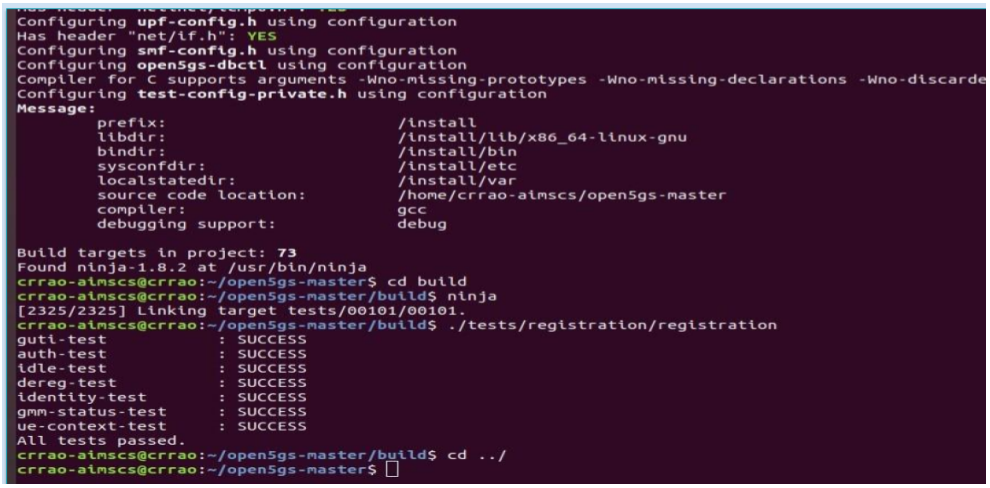

Figure 3.3: open5gs platform

3.1.2 UERANSIM

UERANSIM comprises of 5G UE and RAN (gNodeB). In basic terms it is the 5G mobile phone and the base station. Its application will be to test 5G core network and analyzing the 5G system.

There are 3 main interface that the platform ie. the Control Interface that lies between RAN and AMF , User Interface that lies between RAN and UPF and the Radio Interface that lies between UE and RAN. The control plane supports two important interfaces . Non-access stratum(NAS) which is the interface between UE and the core network and NG Application Protocol (NGAP) which is the interface between UE and the gnodeB.

Some of the important NAS features it supports are:

- Primary Authentication and Key Agreement
- Security Mode Control
- Identification
- Generic UE Configuration Update
- Initial and Periodic Registration
- UE and Network initiated De-registration
- UE initiated PDU session establishment

- UE and Network initiated PDU session release
- Service Request
- Paging

For integrity and ciphering algorithm it supports IA1, IA2, IA3, EA1, EA2, EA3 and for primary and key agreement procedure it has implemented 5G-AKA and EAP-AKA. Fig 3.4 shows UERANSIM in the linux enviroment. UERANSIM also

Figure 3.4: UERANSIM platform

supports features such as PDU Session Resource Setup , NG setup , Initial UE Message, Downlink NAS Transport etc.

3.2 Methodology

The methodology of the work is subdivided into different sub section :
1) The security vulnerability in LTE was explored from previous work [4] . It was found that in LTE the initial NAS message like Attach request and Authentication request were send before NAS security and the UE capability information were sent before RRC security , due to this these messages were sent in plain text without any security protection and hence a malicious user can intercept the message and can degrade the performance of the user . UE capability for eg UE category can be degraded to lower category by the malicious enodeB and as lower the category

lower will be the data rate , hence it will affect the user performance. In LTE it was also found that the initial NAS message for eg. Attach request was not security protected and can be intercepted by malicious gnodeB and an attach reject was sent to the UE due to which it caused Denial of service for the user for a long interval.

2) Before exploring the vulnerability in 5G a experimental setup was made using two open source tool namely Open5gs and UERANSIM as discussed in above section. Successful integration of both the tool lead us to capture different message of 5G end to end call flow as per 3GPP specification.

3) After setting up the Test bed a frame work was built as shown in figure 3.5 . As per the framework which was designed when the user equipment send a registration request of type mobility updating due to the change in the registration area a registration reject is send through the malicious gnodeB due to which all the previous stored security information and identifiers get removed and thus when the UE make a fresh registration request to the network it is made to exchange the core network and radio capabilities, which if exploited can lead to various attacks 4)

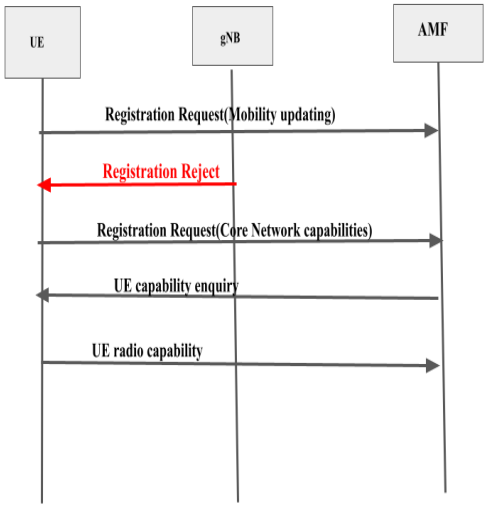

Figure 3.5: Setup to acquire the device capabilities

After Exploring the security vulnerability in LTE and setting up experimental setup for 5G , Vulnerability in 5G was explored . Similar to LTE it was found that in 5G also Initial 5G NAS message like Registration request and authentication request

was not security protected and malicious gnodeB can intercept it and can sent Registration reject and authentication reject respectively thus causing denial of service . The UE capability information similar to LTE was sent before RRC security thus can led to downgrade of user performance.

Chapter 4

Results and Discussion

Device capabilities can be sub-divided into two categories ie. core network and radio capabilities. In the below subsection a detailed analysis of crucial device capabilities is listed out that are exchanged during the registration procedure, along with the device capabilities we have listed out various NAS signalling messages which is not integrity or security protected and its corresponding impact if the parameter are disabled or changed:

4.1 List of insecure NAS signalling message

There are various NAS signalling message like Registration request , Registration reject , authentication request and authentication reject that is not integrity or security protected. This messages can be intercepted by the attacker without any security check and thus causing denial of service for the users. Here is the list of NAS signalling messages.

a) **Authentication failure**: When the UE tries to attach with the 5G Network, network sends the UE with Authentication challenge consist of RAND value as shown in figure 8.1 . If the UE succeeds the challenge it replies with authentication response consist of RES value, but if it fails it replies with authentication failure as shown in figure 8.2 which can be of two types ie. MAC failure or SYNC failure. If the MAC value which the UE receives is not correct then it sends MAC failure

thus confirming it is not a legitimate UE. In the case of SYNC failure UE checks the freshness of the SQN value which is send by the network to the UE during the authentication request, if it fails to do so then it respond with SYNC failure along with re-sync token AUTS which means it is the legitimate UE but due to delay in the arrival of the SQN value the UE replies with the failure message

Figure 4.1: Rand value in authentication request

Figure 4.2: MAC failure and SYNC failure captured

b) **Registration Reject**: When an UE attach with the 5G network it sends an initial UE message Registration request to the network through gnodeB,if there is a successful operation it sends the Registration accept to the UE nor it sends the Registration reject with various 5GMM causes. During our analysis we found that the registration request as well as registration reject is not integrity protected as shown in the figure 16 which means an attacker can setup a malicious gnodeB and can intercept the registration request and can send the registration reject , here attacker does not need any security key to send the reject clause .

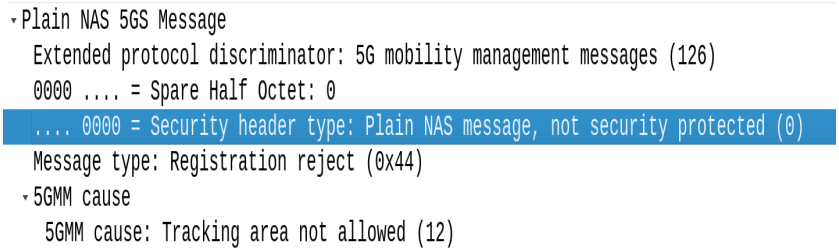

Figure 4.3: Registration reject with no security protection

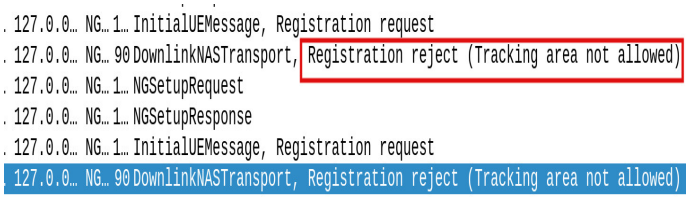

Figure 4.4: Registration reject with tracking area not allowed

c) **Authentication reject** Authentication request and Authentication reject are not security protected as shown in the figure 20 and the attacker can intercept the request message and can send the authentication reject message to the UE.

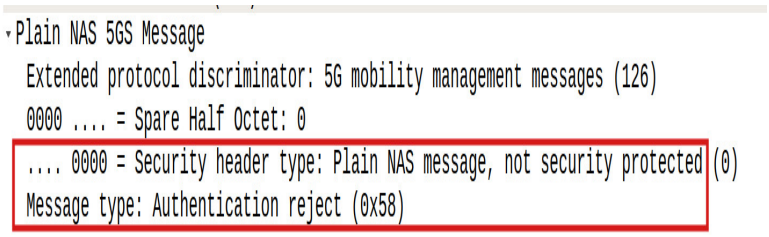

Figure 4.5: Authentication reject not security protected

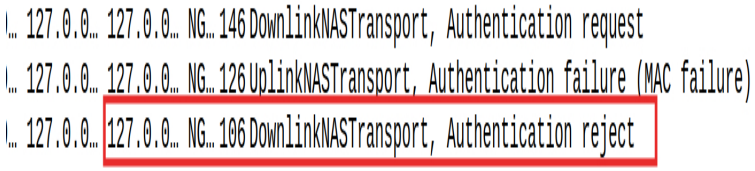

Figure 4.6: authentication reject sent to the UE

4.2 List of device capabilities exposed in clear text

a) **ROHC profiles**: ROHC is the header compression algorithm that is mainly used to compress header of different IP packets as shown in table 1. It is mainly used in voice communication in mobile networks. If a UE does not support ROHC it means it does not voice over IP.

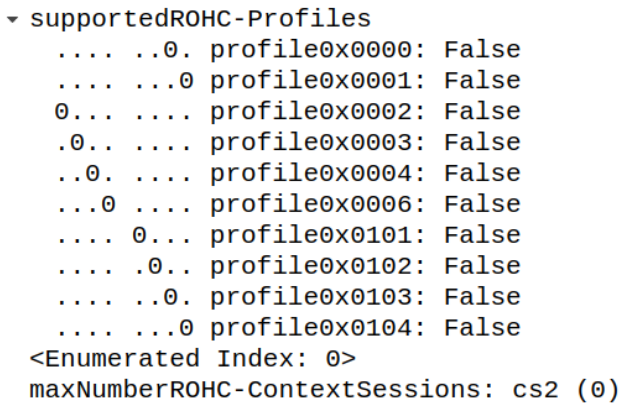

Figure 4.7: ROHC profile of 5G UE captured in wireshark

Table 4.1: ROHC profiles.

Profile Identifier	**Usage**	**RFC 4995**
0x0000	No compression	RFC 4995
0x0001	RTP/UDP/IP	RFC 3095, RFC 4815
0x0002	UDP/IP	RFC 3095, RFC 4815
0x0003	ESP/IP	RFC 3095, RFC 4815
0x0006	TCP/IP	RFC 4996
0x0101	RTP/UDP/IP	RFC 5225
0x0102	UDP/IP	RFC 5225
0x0103	ESP/IP	RFC 5225
0x0104	IP	RFC 5225

IMS capable UEs supporting voice' shall support ROHC profiles 0x0000, 0x0001, 0x0002.

b) **UE category**: UE Category is used to allow the gNB to communicate with all the UEs connected to it effectively. UE category as a whole defines the uplink and downlink performance .Till release 11 there was single UE Category But from Rel 12, the single category of UE gets decoupled into two individual categories, where ue Category DL defines the DL throughput performance and UE-Category UL defines the UL throughput performance. UE category for 5G has been captured as shown in figure 9

c) **CA and MIMO parameter**: Carrier Aggregation (CA) and Multi Input

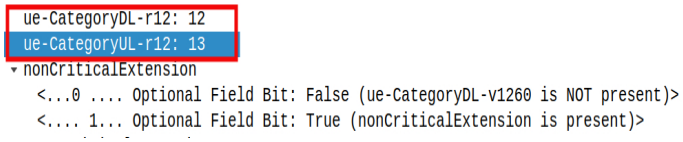

Figure 4.8: UE category captured

and Multi Output (MIMO) enhances and boost the capacity of the network . Both the parameter enhances the data rate of the technology. CA parameter is useful to increase the bandwidth and MIMO parameter is useful as it supports multiple antenna technology.

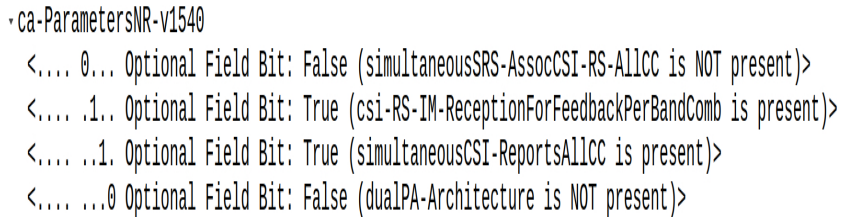

Figure 4.9: CA parameter of 5G UE captured

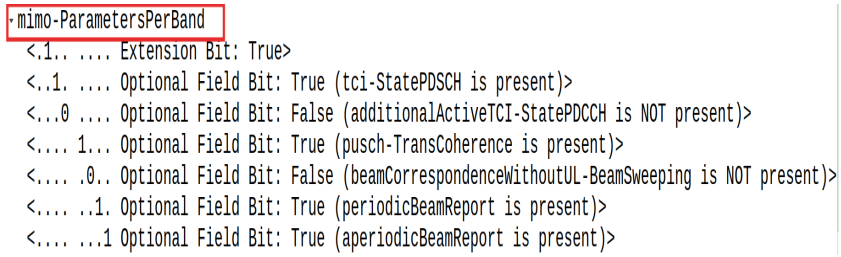

Figure 4.10: MIMO parameter of 5G UE captured

d) **Band** : Band refers to the list of radio frequencies supported by the UE.Usually UE supports multiple frequency band. Support of multiple frequency bands by UE is confirmed if UE supports intrafrequency handover . Bands supported by UE will depend on the region they are manufactured and sold.

Frequency band of 5G NR is usually divided in two different frequency ranges ie. FR1 and FR2. Frequency range 1 consist of sub-6GHz frequency bands, some of the bands are traditionally used by previous standards, but it also has been extended to cover potential new spectrum offerings from 410 MHz to 7125 MHz. FR2 consist of frequency bands from 24.25 GHz to 52.6 GHz. They have shorter range but higher

available bandwidth.

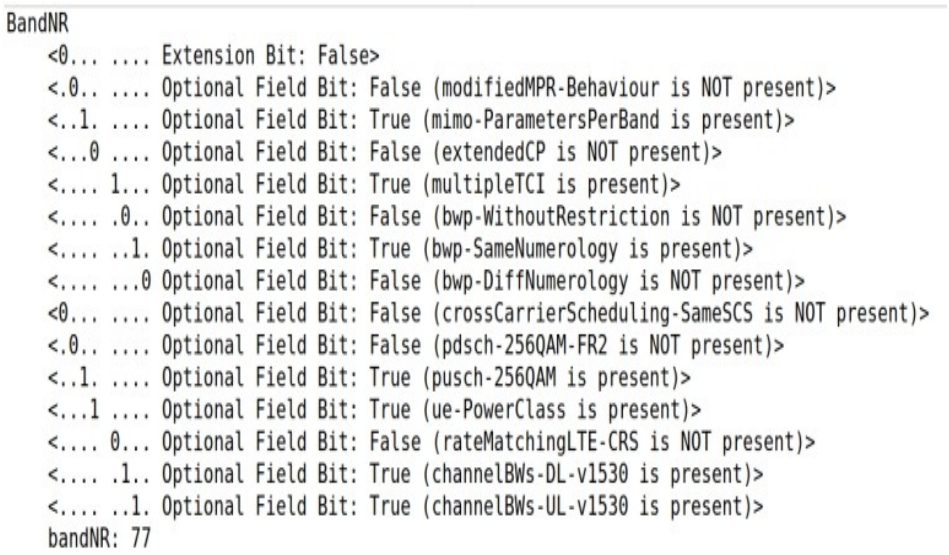

Figure 4.11: Band NR parameter captured

e) **Dual connectivity**: Dual connectivity is the new capability introduced in 5G. With these capabilities, a UE which is 5G capable can simultaneously and separately connect to both LTE and 5G network,thus it will help UE to achieve higher throughput and excellent coverage.

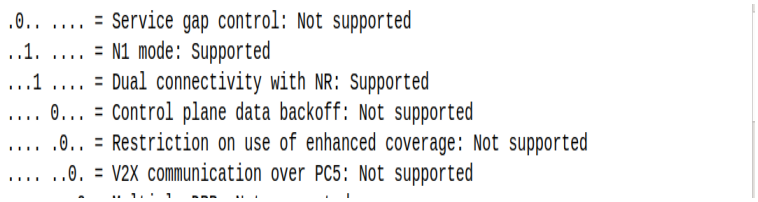

Figure 4.12: Dual connectivity with NR

f) **N1 Mode and UE usage setting** : Two important parameters which is exposed in clear text is N1 Mode and UE Usage setting. N1 mode is the mode allowing the UE to access the 5G core network via the 5G access network and UE usage setting informs the network what is crucial for UE ie. Voice or Data. A voice centric UE if unable to avail voice services in 5GS cell it will switch to E-UTRAN or 4G to avail the voice service, whereas if a UE is set to data centric it will not perform any reselection if voice services are not available

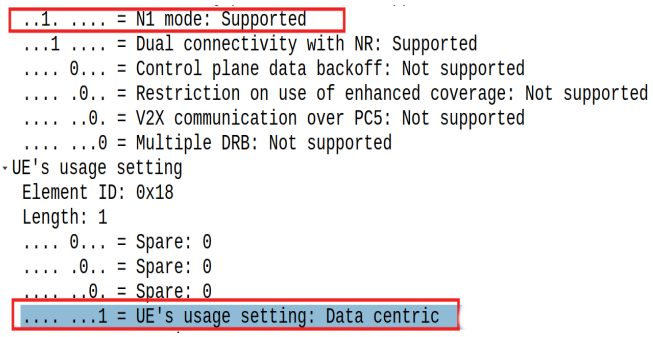

Figure 4.13: UE usage setting and N1 mode captured

g) **Ciphering algorithm** : Under UE network capability there are various ciphering algorithm like EIA-0,128-EIA-1 etc as shown in Figure 15 which is supported by the UE is sent in clear text to the gnodeB as shown in Figure 15.

h) **GUTI Persistence**: 5G-S-TMSI is generated by AMF during the generation

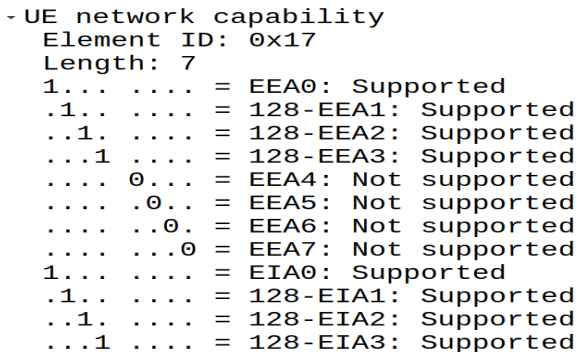

Figure 4.14: Various Supported ciphering algorithm sent in clear text by the UE

of 5G-GUTI. It uniquely identifies the UE within the AMF region. In 5G, the registration is done with UE sending its SUCI, AMF assigns 5G-S-TMSI to the UE, and in all the process after the assigning of TMSI the network uses TMSI of the UE to identify the user equipment,for instance when the UE is in idle mode the network identifies it in terms of its tracking area ie. network sends the paging message to all UE present in that tracking area along with the 5G-S-TMSI Of the desired UE. The UE responds to the paging message which helps the network to identify the UE. There is a strict requirement to refresh the TMSI(5G-GUTI) [14] whenever there is Initial Registration,Mobility Registration Update,Periodic Registration Update and Network Triggered Service Request,but in our experimental setup we found that the TMSI remained the same during two simultaneous service request triggered by the

UE , and also during the registration request of type mobility updating .

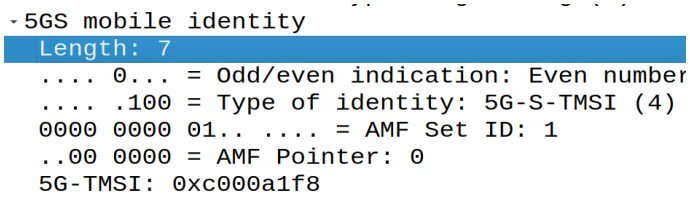

Figure 4.15: 5G-TMSI captured during service request in experimental setup

4.3 Exploitation of the device capabilities and signalling message

The device capabilities and pre-authentication signalling messages discussed above, if altered or disabled, can cause various attacks which can lead to the degradation of the network.

This section presents a classification of various type of attacks based on the device capabilities and signalling message.We present three class of attacks namely a) **Bidding down of devices** b) **Device identification** c) **Denial of service**

Bidding down of devices

Under bidding down of devices the following below are the critical parameters can lead to biding down of devices:

- **ROHC profile**: If the attacker disabled the ROHC profile, it will cause UE to loose its IMS voice calling capacity thus leading to bidding down of the device.

- **UE category** : Downgrading the UE category to lower values will downgrade(bidding down) the performance the UE . A Cat 6 will receive a maximum speed of 300Mbps in the downlink and with cat 1 in the downlink it will receive a maximum peak of 1 Mbps.

- **Carrier Aggregation (CA) and Multi Input and Multi Output (MIMO)** : AS MIMO and CA parameter are responsible for increasing the bit rate thus

disabling it will consequence in the degradation of the bit rate and thus bidding down the performance of the UE.

- **Bands**: As the band defines the range of frequency that the UE supports thus if the certain supported bands that the 5G UE supports especially the FR2 bands then the user will downgrade to the 4G band thus leading to bidding down.

- **N1 MODE and UE Usage setting**: If the attacker disables the N1 mode shown in Figure 14, the UE will loose its connectivity with the 5GC network and the UE will try to connect with the E-UTRA cell connected with EPC, thus leading to bidding down attack also if the UE usage setting is changed from data centric to voice centric and IMS voice service service is not available then the UE will disable the N1 Mode capability and will try to connect to 4G network thus affecting the performance,UE usage setting information also can be used by the attacker to identify mobile devices from other devices such as IOT as the following usage setting can only be supported by the cellular devices.

Denial of service

Under Denial of service the following below are the critical parameters can lead to Denial of service:

- **Registration reject**: In our setup we send registration reject with the cause tracking area not allowed and N1 mode not allowed to the UE as shown in the figure 17 .We found that due to the registration reject of TRACKING AREA NOT ALLOWED the UE went to continuous denial of state and due to the N1 MODE NOT ALLOWED We found our UE downgraded to a 4G network.

- **Authentication reject**: In our experimental setup, UE authentication reject by the malicious gnodeB as shown in Figure 21, thus leading to denial of service for the user for a long time.

Device Identification and monitoring

:

- **Ciphering algorithm** : It was found that EIA-0 was 1 for Huwaei,Samsung,Intel, Mediatek but was 0 for Qualcomm [6], Thus leading to device identification
- **GUTI persistence** : GUTI persistence can lead to the tracking of users thus results in device monitoring . In [13] it was found that GUTI remained the same for various instances which led to various passive attacks for the 4G network .
- **Authentication Failure**: In [25] it is validated that due to types of authentication failure ie. SYNC and MAC can actually as shown in Figure 18 lead to device monitoring or tracking of UE in 4G network. If the attacker setup the malicious gnodeB, then it can capture the RAND value and replay as it is sent in air and then replay the old authentication challenge already received by the user , this will result in the SYNC failure by the the targeted UE and the MAC failure by the non-targeted UE, thus leading to device tracking.

Chapter 5

Countermeasures,Future Work & Counclusion

5.1 Countermeasures

In these section we will discuss the countermeasures for the possible vulnerabilities that we discussed above.

3GPP should review and think about securing the core network and radio capabilities. The UE capability message should be acquire by the gnodeB only after establishing the required security procedure. If the UE capability message are properly secured before exchanging it with gnodeB the malicious gnodeB will not be able to acquire it and make changes to it.

Another solution for it is to use Digital signature on the important parameters discussed above. Digital signatures are derived by public key cryptography.It is also known as asymmetric cryptography.The user who creates digital signature of the particular data uses its private key to encrypt the data. Decryption of the data can only be done by using public key of the signer who has created the digital signature data. In [11] the authors discussed how PKI based secured bootstrapping mechanism can be used to secure the devices and avoid them to connect to the malicious base station. Here the base station using its secret key will create a signature and will attach the signature and certificate chain to the initial messages. The device when it receives the message will first verify the certificate chain and then the signature

5.2 Future Work

In the present work, the security gap of the access network has been explored . In Future, the security gaps in the core network of 5G network functions can be explored , as with the advancement in 5G large number of Internet of things (IOT) will be connected various security along with it will also come in play.
The Core network can also be integrated with Software Defined network (SDN) . It will enable the external control of control plane signalling through a SDN controller thus automating the network in a drastic manner but with the use of SDN various security threats can come which can be explored in the future work

5.3 Conclusion

.A 5G standalone test bed is presented along with its functionality. It was found that in 5G UE core network and radio access capabilities are exposed in clear text just like LTE which can be manipulated by the attacker and can downgrade the capabilities of UE . Along with the device capabilities it was also found that various pre-authentication NAS signalling messages like registration request/reject and authentication request/reject which are also not security protected and the attacker can intercept it without any security check and can cause denial of service for the users . A counter measure of using digital signature is also discussed to secure the capabilities of the UE that are exchanged with the gnodeB without establishing the security.

Summary of the findings			
Index No.	Type of signalling message	Type of Vulnerabilities Found	Possible Attacks found
1	NAS signalling message	REGISTRATION REJECT Not security protected.	Denial of service & bidding down attack
2	NAS signalling message	Linkability of the user due to authentication failure	Tracking down of the user
3	NAS signalling message	Service failure due to excess flooding of authentication reject.	Reduction of data rate
4	UE Network capability	GUTI Persistence as TMSI was not frequently changing	Tracking of the user.
5	UE Network capability	List of supported Ciphering sent in clear text by UE	By comparing with different vendors of UE it can lead to device identification.
6	UE network capability	Dual connectivity exposed in clear text	Dual connectivity supported or not exposed in clear text can lead to tracking of the 5G UE

7	UE radio capability	UE category exposed in clear text	Degrading the UE category Can led to bidding down of the performance
8	UE radio capability	Mimo & CA parameter exposed in clear text	Disabling the parameter will reduce the throughput of the user
9	UE radio capability	PDCP parameter called ROHC profile exposed in clear text	Disabling the ROHC profile can disable the calling ability of the user

Bibliography

[1] C. Seker, M. T. Güneser and T. Ozturk, "A Review of Millimeter Wave Communication for 5G," 2018.

2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey pp. 1-5, doi: 10.1109/ISMSIT.2018.8567053.

[2] Rabia & Kumar, Pardeep & Jayakody, Dush Nalin & Liyanage, Madhusanka. (2019). "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions"

[3] Ahmad, Ijaz & Kumar, Tanesh & Liyanage, Madhusanka & Okwuibe, Jude & Ylianttila, Mika & Gurtov, Andrei. (2017). 5G Security: Analysis of Threats and Solutions 10.1109/CSCN.2017.8088621.

[4] Shaik, Altaf & Borgaonkar, Ravishankar & Park, Shinjo & Seifert, Jean-Pierre. (2019). New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. 221-231. 10.1145/3317549.3319728.

[5] M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617-1655, thirdquarter 2016, doi: 10.1109/COMST.2016.2532458.

[6] Piqueras Jover, Roger & Marojevic, Vuk. (2019). Security and Protocol Exploit Analysis of the 5G Specifications. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2899254.

[7] Hu, Xinxin & Liu, Caixia & Liu, Shuxin & You, Wei & Li, Yingle & Zhao, Yu. (2019). A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2937997.

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

[9] Dehnel-Wild, Martin,and Cas Cremers "Security vulnerability in 5G-AKA draft." Department of Computer Science, University of Oxford"

[10] Khan, Haibat Martin, Keith. (2019). "On the Efficacy of New Privacy Attacks against 5G AKA. 431-438. 10.5220/0007919704310438."

[11] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino (2019) "Insecure connection bootstrapping in cellular networks: The root of all evil," in Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.,

[12] Shaik, Altaf Borgaonkar, Ravishankar Asokan, N. Niemi, Valtteri Seifert, Jean-Pierre. (2016). Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. 10.14722/ndss.2016.23236.

[13] Khan, Haibat Martin, Keith. (2020). A survey of subscription privacy on the 5G radio interface - The past, present and future. Journal of Information Security and Applications. 53. 102537. 10.1016/j.jisa.2020.102537.

[14] Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., Bertino, E. (2019). Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. Network and Distributed Systems Security (NDSS) Symposium2019.

[15] E. G. Larsson, "Massive MIMO for 5G: Overview and the road ahead," 2017 51st Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, 2017. pp. 1-1, doi: 10.1109/CISS.2017.7926182.

[16] A. Benjebbour, K. Saito, A. Li, Y. Kishiyama and T. Nakamura "Non-orthogonal multiple access (NOMA): Concept, performance evaluation and experimental trials," 2015 International Conference on Wireless Networks and

Mobile Communications (WINCOM), Marrakech, Morocco, 2015, pp. 1-6, doi: 10.1109/WINCOM.2015.7381343.

[17] Basin, David Dreier, Jannik Hirschi, Lucca Radomirovic, Saša Sasse, Ralf Stettler, Vincent. (2018) Formal Analysis of 5G Authentication. 1383-1396. 10.1145/3243734.3243846.

[18] Ridhima and A. Singh Buttar "Fundamental Operations of Cognitive Radio: A Survey," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019",pp. 1-5, doi: 10.1109/ICECCT.2019.8869190.

[19] Singla, Ankush Hussain, Syed Chowdhury, Omar Bertino, Elisa Li, Ninghui. (2020). Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks. Proceedings on Privacy Enhancing Technologies. 2020. 126-142. 10.2478/popets-2020-0008.

[20] Basin D, Dreier J, Hirschi L, Radomirovic S, Sasse R, Stettler V. A formal analysis of 5G authentication. InProceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security 2018 Oct 15 (pp. 1383-1396).

[21] 3GPP Technical Specification Group Services and Systems Aspects "Security architecture and procedures for 5G system," 3GPP TS 33.501, V1.0.0. March 2018

[22] S. Steig, A. Aarnes, T. Van Do and H. T. Nguyen, *"A Network Based IMSI Catcher Detection," 2016 6th International Conference on IT Convergence and Security (ICITCS), Prague, Czech Republic, 2016* pp. 1-6, doi: 10.1109/ICITCS.2016.7740306

[23] Borgaonkar, Ravishankar Hirschi, Lucca Park, Shinjo Shaik, Altaf. (2019) New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. Proceedings on Privacy Enhancing Technologies. 2019. 108-127. 10.2478/popets-2019-0039.

[24] Rappaport, T.S.. (2001). Wireless Communications: Principles and Practice, 2nd Edition.

[25] Curran, Kevin Maynes, Vivian Harkin, Declan. (2015). Mobile device security. International Journal of Information and Computer Security 7. 1. 10.1504/IJICS.2015.069205.

[26] Kutscher, Dirk. (2016). It's the network: Towards better security and transport performance in 5G 656-661. 10.1109/INFCOMW.2016.7562158.

[27] Forsberg, G.Horn,W.-D.Moeller,and V.Niemi LTE Security Hoboken, NJ, USA: Wiley, 2012

[28] L. Wang, J. Liu, M. Chen, G. Gui and H. Sari "Optimization-Based Access Assignment Scheme for Physical-Layer Security in D2D Communications Underlaying a Cellular Network," in IEEE Transactions on Vehicular Technology vol. 67, no. 7, pp. 5766-5777, July 2018, doi: 10.1109/TVT.2017.2789022.

[29] D. He, S. Chan and M. Guizani *"Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks," in IEEE Transactions on Wireless Communications* vol. 14, no. 1, pp. 389-398, Jan. 2015, doi: 10.1109/TWC.2014.2347311.

[30] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov "Overview of 5G Security Challenges and Solutions in IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[31] https://open5gs.org/

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

[33] S. Choi et al., "5G K-SimNet: End-to-End Performance Evaluation of 5G Cellular Systems," 2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, 2019, pp. 1-6, doi: 10.1109/CCNC.2019.8651686.

[34] A. R. Prasad, S. Arumugam, B. Sheeba, and A. Zugenmaier "3GPP 5g Security," Journal of ICT Standardization, vol. 6, no. 1, pp. 137–158, 2018.

[35] Norrman, Karl Naslund, Mats Dubrova, Elena. (2016) Norrman, Karl Naslund, Mats Dubrova, Elena. (2016) 10.4108/eai.18-6-2016.2264114.

[36] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," in IEEE Access, vol. 3, pp. 1206-1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[37] Piqueras Jover, Roger. (2016) LTE security, protocol exploits and location tracking experimentation with low-cost software radio.

[38] Rupprecht, David Kohls, Katharina Holz, Thorsten Popper, Christina. (2019). *Breaking LTE on Layer Two.* 1121-1136. 10.1109/SP.2019.00006.

[39] A. Kostopoulos, I. P. Chochliouros, I. Giannoulakis, A. Kourtis and E. Kafetzakis , "Small Cells-As-A-Service in 5G Networks," 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), 2018, pp. 1-5, doi: 10.1109/BMSB.2018.8436701.

[40] N. H. Mahmood, M. G. Sarret, G. Berardinelli, and P. Mogensen, "Full duplex communications in 5G small cells , "Full duplex communications in 5G small cells pp. 1665-1670, doi: 10.1109/IWCMC.2017.7986534.