Analysis of machine learning techniques to secure 5G networks.

Capstone Project

Presented by

Ali Jose LOPEZ GIRON

University of Alberta
Master of Science in Internetworking
Edmonton, Canada

Supervisor
MSc. Sandeep Kaur

February 2021

Word Count

Number of pages: 91
Number of words: 28052

ABSTRACT

Since the beginnings of the mobile communications, service providers have been trying to improve the customer experience not only in terms of reliable communications but also on security. At the beginning the communications were easy to intercept due to the lack of encryption and advanced mechanism to protect the identity with the aggravation of the absence of a unified communication standard that centralized efforts in terms of research and development. Enabling the portable devices to perform complex activities that go beyond of a simple call, security concerns have risen until such point that it is value in USD 156 Billion.

In this research, I analyze the architecture of the fifth generation of cellular networks with strong emphasis in the 5G standard released by 3GPP. In addition, I study the security landscape in this context and define a case study that tests the performance of supervised learning algorithms. In addition, I summarized the security landscape for the new generation of cellular network, I study the recommendations of the industry as the X.805 and NIST cybersecurity and finally I propose a recommendation based on the security domains architecture specified by the 3GPP group.

To collect all the information, this research relies on an extensive review of the latest standards released by the 3GPP group, the recommendation given by cybersecurity authorities and a large list of books that set the theoretical foundations of the findings and recommendations given throughout the Chapter 5. The data used to conduct the experiment was extracted from the Canadian Cybersecurity Institute which was generated with a benign profile system which simulated the behaviour of human interactions on Internet. Similarly, this data was merged with three DoS signatures to create a dataset with a representation of more than 1 million samples.

Key words: 5G, Protocol Stack, Virtualization, Latency, DoS, UDP, TCP, GTP, Authentication, Supervised Learning,

ACKNOWLEDGMENT

First, I thank god above all things for giving me the patient and support to overcome the difficulties during this journey.

I would like to thank Dr. Mike MacGregor for his academic guidance throughout the development of this journey as well as MSc. Sandeep Kaur for her technical support and advices in the development of the security perspective of this work

Finally, I would not be here today without the love, patience and encouragement from my friends and family specially my wife, mom, and dad; your infinite support during this time was my most valuable asset, this achievement is also yours.

Table of Contents

Table of Figures

Table of tables

CHAPTER 1

INTRODUCTION

1.1 Study Background

Since the commercial launch of the first generation of cellular networks, telecommunication companies have strived to provide a reliable service not only in terms of availability but also as a trustable channel to hold a phone a call or more recently to share data. In a recent survey published by the World Economic Forum [1] that intends to measure the impact of cybersecurity threats for Internet Service Providers, the vulnerabilities related to Social Engineering are the most common and expensive risks that companies and their customers have to deal with. In second place telecommunication companies are also prone to suffer malware attacks that exploit vulnerabilities in external applications and finally the Denial of Service (DoS) attack is listed third as one of the most severe attacks that disrupts the operation of the network.

Even government agencies, companies and hardware manufacturers have designed and implemented frameworks to protect their environments they also agree on the idea that they will experience more attempts to abuse their systems due to the massive adoption of Internet of Things (IoT), as well as the application of artificial intelligence to conduct attacks in barely-known forms which makes prevention and immediate response a difficult task to deal with. The Figure 1 shows the maturity state of Machine Learning and Deep Neural Networks. Although both are widely used in many IT applications, it is expected a massive adoption within the next two to five years.

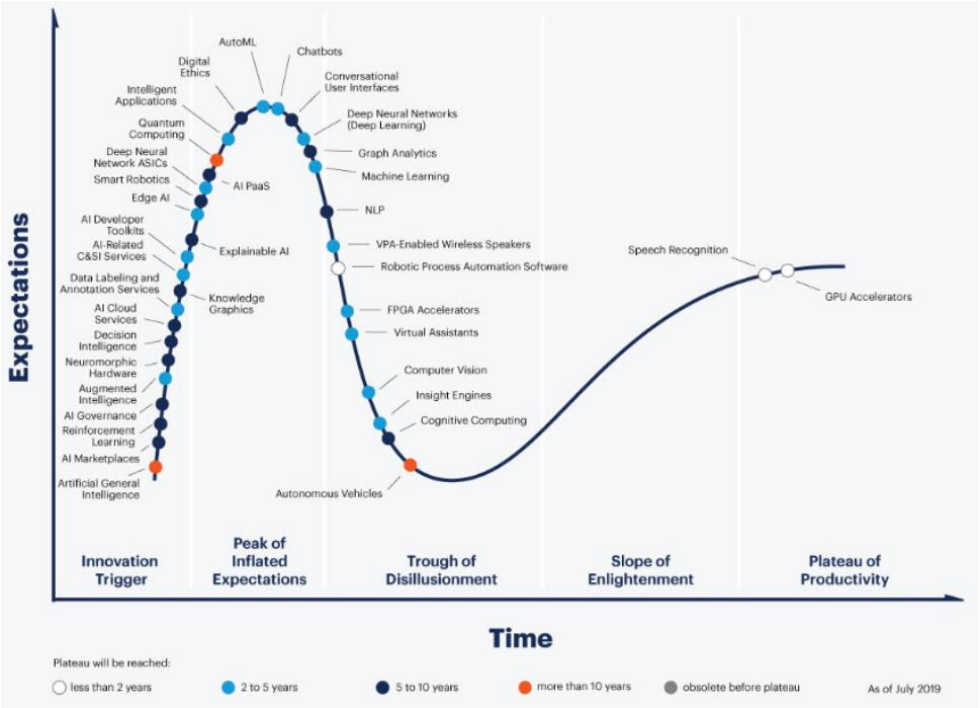

Figure 1. Hype Cycle for Artificial Intelligence, 2019. Source: Gartner 2019

1.2 Study Scope

Taking into consideration the risk assessment elaborated by World Economic Forum that summarizes the concerns of the most important ISP's in the world, this study will list the malicious activities that may disrupt the network operation. The same report indicates that there some other threats such as social engineering and malware distribution that affect directly and individually users as their cyber-security practices, then this research will be focused on studying the threats to the network itself, meanwhile the vulnerabilities of devices under control of subscribers can be analyzed in another research.

1.3 Capstone Structure

In order to prepare the case study, this research is divided in 7 chapters, the introduction, the research problem and methodology, the background information, the theoretical perspective, the analysis of results, and finally the discussion and conclusions.

Chapter 1: Introduction.

This chapter explains the scope of the capstone, the aim and objectives, the context, as well as the limitation of the study.

Chapter 2: Research problem and methodology

This chapter will define the research problem related to the cybersecurity events that affect the operation of 5G networks as well as the artificial intelligence mechanisms to detect these attacks.

Chapter 3: Background information

This chapter will show the evolution of the cellular networks as well as the best practices in cyber-security following the X.805 and NIST frameworks. This information will set the guidelines to design the framework associated to this project. This chapter will define the methodology to conduct the research and prepare the case study.

Chapter 4: Theoretical perspective

This chapter will study the 5G network architecture as proposed in the technical specification disclosed by the 3GPP group, it will go through the service requirements and the security considerations considered to standardize the technology, and will expose the machine learning techniques applied to network security.

Chapter 5: Analysis of results

This chapter will present the analytical framework to secure 5G networks, the assessment of machine learning techniques and the behaviour of the approach to be taken by simulating a DoS attack.

Chapter 6: Discussion

This chapter will compare the results with the theoretical principles studied in this project. Furthermore, it will assess the resulting framework and its adaptability to more complex scenarios.

Chapter 7: Conclusions

This chapter will summarise the final conclusions to be got from chapter 5 and 6, but it will also issue recommendations based on the outcomes of this project.

CHAPTER 2

RESEARCH PROBLEM AND METHODOLOGY

2.1 Research Problem

As indicated previously, one of the main concerns for ISP's is how to avoid disruption of their operations due to any cyber security event, these worries tend to worsen with the adoption of IoT (Internet of Things) and the introduction of new devices that intend to perform particular functions (i.e., automation, M2M communication) but with far less capabilities in terms of processing and storage which make them more vulnerable to the attack vectors. For instance, the objective of this research is to design an analytical framework to protect 5G networks, study the attacks that can impact the operation of the system and define a mechanism based on artificial intelligence to classify and detect malicious activities.

2.2 Methodology

To find a solution to the problem, this research will go through the following steps as a methodology to find one alternative to the problem stated above, assess its performance and generate valuable contributions or recommendations to the industry.

Technology Analysis

In order to understand the context of the 5G network, this project will conduct an analysis of the architecture based on 3GPP TR 21.915 Release 15. This step will define the environment that replicates a real case scenario.

Literature Review

The information to be reviewed will be oriented to understand the basic concepts about cybersecurity, machine learning and their application to 5G networks. This step will provide the theoretical background needed to define the cybersecurity framework to be applied in this research.

Identification of risks and vulnerabilities

This project will intend to enumerate a list of vulnerabilities that can be deducted from the network architecture itself, the portfolio of services specified in TS 22.261 and from previous researches.

Prototype cybersecurity solutions

After analysis of the previous steps, this research will output a security framework to detect the attacks that exploit the vulnerabilities mentioned previously. Initially, this project will study the National Institute of Standards and Technology Cybersecurity Framework (NIST) and the ITU-T recommendation X.805 Security Architecture for Systems Providing End-to-End Communications. Additionally, this part will study and define the mechanism of machine learning to be implemented in order to detect anomalies (supervised or unsupervised learning).

Implement network simulation

In order to assess the performance of the previous output, this capstone project will implement a Denial-of-Service attack to evaluate the behavior of the mitigation framework proposed before.

This environment will be simulated using 5G NetSIM v12.1, meanwhile the attack and defense mechanisms based on machine learning will be coded in Python.

Discussion

This step will assess the result of the implementation to validate the framework proposed. The result may prove the viability of this research or end up with a proposal with a different approach to tackle the problem

CHAPTER 3

BACKGROUND INFORMATION

3.1 Background Information

3.1.1 First Generation (1G)

The first generation of mobile communication was commercially launched in the 80's as an analog system called Advanced Mobile Phone System (AMPS) [2]. The architecture itself met the most basic principles of radio communication by integrating three major subsystems such as *The Mobile Unit (MU), The Cell Site (CS)* and *The Mobile Telecommunications Switching Office (MTSO)* [3]. The first network element (MU) was in charge of performing the following functions: Setup Channel Selection, Channel Tunning, Call Reception and Transmission, Failure Sequence Timing, Tone Switchook Supervision, Preorigination Dialing. The second network element (CS) had to carry out functions of RF Coverage, Location Data Collection, Component Calibration, Mobile Control, Message Relaying and Formatting, Switchhook and Fade Supervision. Finally, the (MTSO) executed the Transmission and Switching operations to other networks, Radio Channel Management, Remote Unit Maintenance, Cell Site and Mobile Control, Message Administration, Mobile Location and Handover Synchronization. The Figure 2 shows the architecture described by Fluhr and Porter in The Bell System Technical Journal.

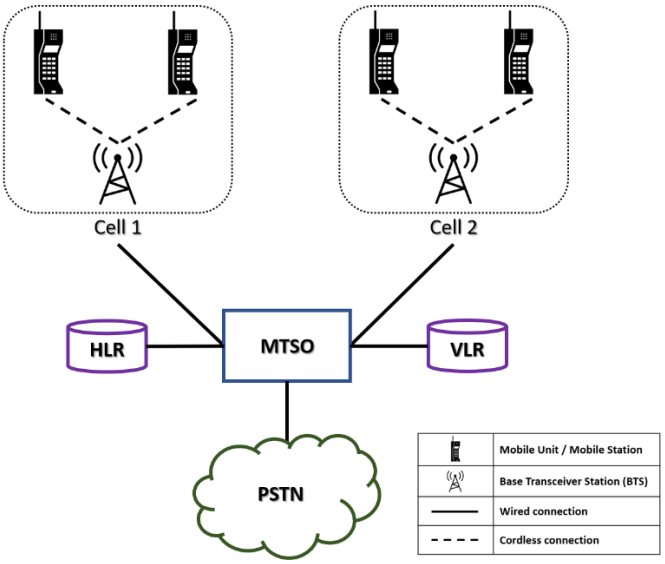

Figure 2. AMPS Network Architecture. Source: Fluhr and Porter (1978)

3.1.2 Second generation (2G)

The second generation of cellular networks was marked by the fierce competition between CDMA (Code Division Multiple Access) and GSM (Global System for Mobile Communications) [4]. The first one was an initiative released by Qualcomm Inc in 1993 meanwhile GSM was developed and released in Europe as an outcome of studies conducted by regulators, operators and manufacturers. Both technologies were able to introduce data services for their users, however, in terms of customer experience GSM differenced itself from CDMA with the fact that users needed to insert

a SIM card into the mobile phones to get the service meanwhile CDMA users had a phone associated to the phone number.

3.1.2.1 GSM

Launched in 1991, was the result of a series of meetings between government agencies, regulators, operators and manufacturers to improve communications based on analog technologies as well as deploy a common and reliable network able to provide roaming services within the 12 members of the European Economic Community. The outcome of these discussions was a technical specification called GSM that was able to handle multiple calls using one channel, allowed manufacturers to reduce dramatically the power consumption on terminals, operators were able to provide added-value services such as call forwarding and roaming and regulators and government agencies found an new source of revenue licensing the band of 1900 MHz. [5]

The basis of the architecture proposed was similar to the existing analog cellular network; however, it would add new network elements that would complement the functions as well as upgrade the network capabilities. The Figure 3 shows the GSM network architecture summarized in [5] with its components. It includes the Mobile Station (MS), the Base Station Subsystem (BSS), the Mobile Services Switching (MSC), the Network Databases and the Operation and Maintenance System.

The Mobile Station was comprised of the mobile phone and the subscriber identity module (SIM). The device does not perform any activity related to the GSM network, it just operates in the band designed for GSM and triggers the actions of send/receive calls. On the other hand, the SIM card contained the International Mobile Subscriber Identity (IMSI) number which is the identity of the user inside the network. The SIM also handled the authentication algorithm, the authentication key and the cipher key generation algorithm. [5]

The Base Station Subsystem was composed of the Base Transceiver Station (BTS) and the Base Station Controller (BSC), when a call was triggered, the MS established a communication with the BTS making use of the air interface to process the voice signal and convert it into data or vice versa. The BTS was mainly used to define a cell coverage area, meanwhile the BSC was in charge of the management of radio resources and centralize a group of BTS that integrated one or several clusters. [5]

The Mobile Services Switching was connected to the BSS through a high capacity link to route all the inbound or outbound calls. To improve its switching capabilities, the MSC was able to query the Network Databases to figure out the route of the call as well as the mobility parameters such as location registration and handover. [5]

The Network Databases were a cluster of powerful servers which stored very specific information for each user to validate the subscriber credentials, or check their plans to issue the bill monthly or simply, figure out the user location and route the call properly. In general terms, the Home Location Registry (HLR) and the Visitor Location Register (VLR) contained the user profile and the current location for billing purposes, meanwhile the Authentication Centre (AUC) held the

authentication and encryption keys and the Equipment Identity Register (EIR) kept the International Mobile Equipment Identity (IMEI) of the equipment that subscriber is using. [6]

The Operation and Maintenance System as indicated in [6], gives the Network Operation Center (NOC) the ability to manage the profile of users as well as the network configuration, performance monitoring and network maintenance.

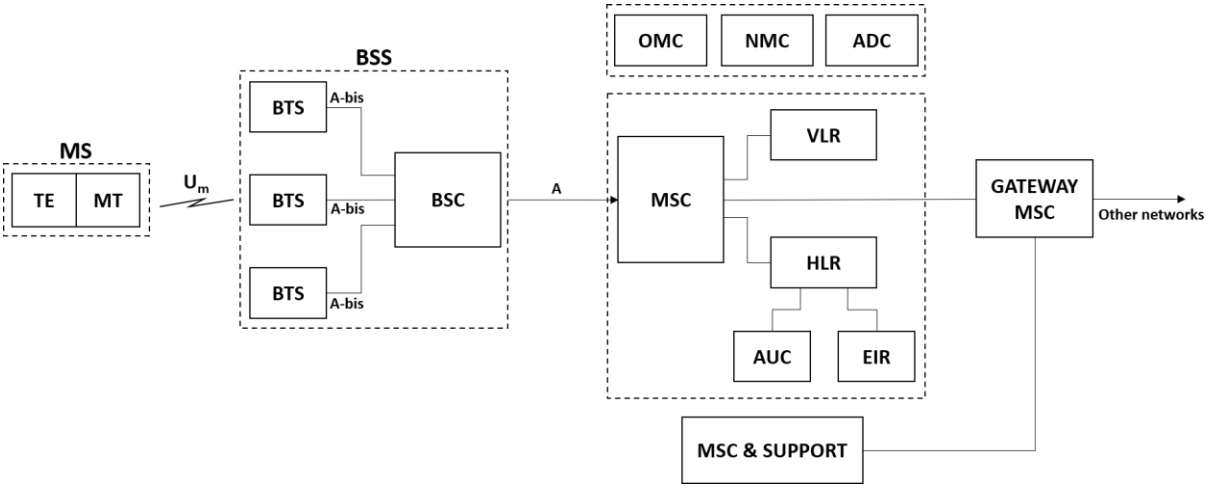

Figure 3. GSM Network Architecture. Source: Steele, Raymond (2001)

3.1.2.2 CDMA

CDMA was released in 1993 as an application of the ANSI-41 standard. Like GSM, it comprises a mobile station (MS) that is connected to the radio access network (RAN) through the air interface which is at the same time joint to the core network (CN) making use of the fixed interfaces of the network. [7]. The Figure 4 shows the detailed CDMA network architecture.

The mobile station allows users to establish a channel of communication to access the network. It includes the User Identity Module (UIM) which contains the subscriber information. [4] The radio access network delivers the data generated by the mobile station to the core network. The elements that make up this part of the network are the following: the Base Transceiver Station (BTS) and the Base Station Controller (BSC); the BTS itself represents the closest physical interface to the MS, meanwhile the BSC is in charge of call-processing, radio resource management, mobility management and transmission resources management. [7]

The core network is constituted by the following entities: Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Authentication Center (AC), Message Center (MC), and Short Message Entity (SME). Beyond the inherit functions of the core network, its key function in the architecture is processing the data coming from RAN to route it to the Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN). [7]

The key functions of each entity are summarized as follows: the MSC performs routing of the circuit-switched connections between the RAN and the PSTN. the HLR registers the geographical location of the user, so that the MSC can route the calls properly. The VLR keeps the ID of all MS hosted in a given MSC, once the subscriber moves into another MSC, the register is deleted. The AC manages the information needed to authenticate the users and encrypt the communication

channels. The MC carries out the tasks of processing (Short Message Service) SMS and finally the SME works as a gateway to exchange short messages with some other networks such as GSM.

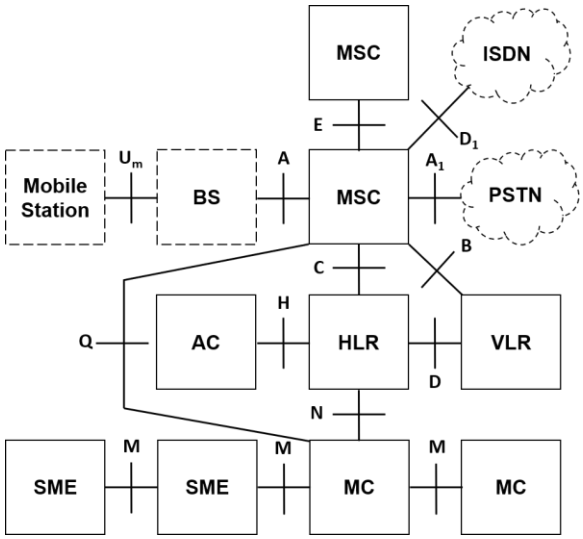

Figure 4. CDMA Network Architecture. Source: Vanghi, Vieri 2004

3.1.3 Third generation (3G)

The third generation of cellular networks is oriented to solve the problem of incompatibility between GSM and CDMA as well as accelerate the adoption of data services, adding a packet-switching structure that defines four classes of service which are the next ones: Class A (Conversational), Class B (Streaming), Class C (Interactive), Class D (Background). [8] The UMTS network also introduces a new approach oriented to differentiate the logical functions of the network entities. Figure 5 shows the Access Stratum which is in charge of performing the operations related to the access network, such as: handover and management of radio resources as well as the radio interface protocols. On the other hand, the Non-access Stratum executes the network functions that complement the access network, such as call control, session management or mobility management. [8]

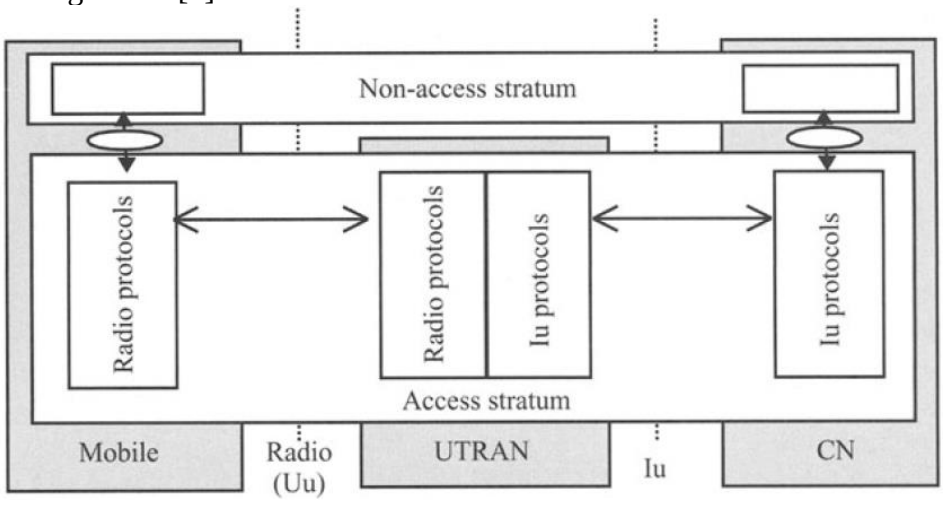

Figure 5. UMTS Access stratum and non-access stratum. Source: Lescuyer, Pierre (2004)

Figure 6 shows the network architecture of UMTS network. Like the previous technologies, Universal Mobile Telecommunications System (UMTS) network architecture consists of the access network and core network. The access network, also known as UTRAN, manages the radio resources and the access to the media, while the core network is still responsible for performing call processing and routing, authentication, user allocation and management of external communication. [8]

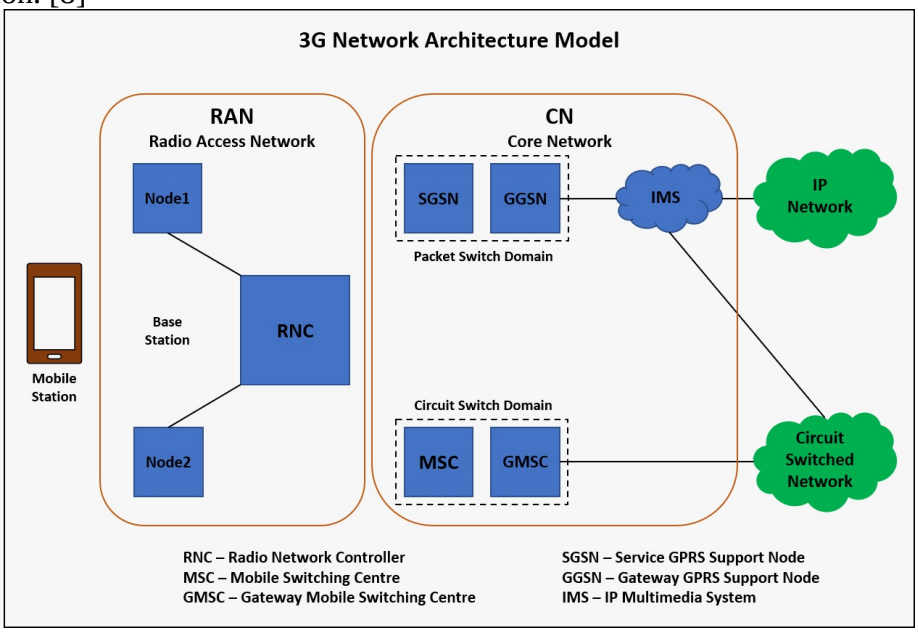

Figure 6. UMTS Network Architecture. Source: Lescuyer, Pierre (2004)

The block represented by the access network comprises two elements: the Node B and the Radio Network Controller (RNC). The first one still provides the radio functions to connect the UE, while the second one redirects the signals, either for the Circuit-Switched (CS) or Packet-Switched (PS) as the case may be.
The elements shown in the core network illustrate the connection between entities; however, the MSC, GMSC and VLR perform the functions of the Circuit-Switched (CS) while the SGSN, and the GGSN make up the Packet-Switched (PS). HLR, EIR and AuC are common for both systems and perform similar functions as in GSM.

3.1.4 Fourth generation (4G)

The massive growth of mobile data consumption pushed the industry to improve the communication technologies to adopt a technology that delivers high data rates and low latencies, so that the voice could be handled as a packet flow that exploits the capabilities of networking techniques such as VoIP. [9]

The Long-Term Evolution (LTE) architecture was released by 3GPP, with purpose of reducing the complexity of the previous generations by integrating all the services in a full IP structure that replaces the RNC and SGSN from the 3G network by an eNB and a series of gateways that provide full interoperability with other networks. [9]. The elements that integrate this architecture are as follows: eNB, MME, HSS, S-GW, P-GW, PCRF

The eNB is in charge of providing the radio coverage to a defined area. In this process there are two main functions. The first one is related to the normal radio operation to process downlink and uplink signals; the second one is oriented to perform signalling activities that were in hands of the RNC in UMTS. [9]

The Mobile Management Entity (MME) is in charge of high-level signalling when the UE is in idle mode. It registers the location of the subscriber and assigns a gateway as the user moves inside the network. The Serving Gateway (S-GW) is in charge of routing the data generated at the base station to the PDN. The Packet Data Network Gateway (P-GW) serves the network as an entity that interfaces with the external world. The Home Subscriber Server (HSS) is the entity that contains the information about the subscribers.

The Policy and Charging Rules Function (PCRF) is optional in the architecture. It can differentiate data flow according to policies configured for a given traffic, hence the network can provide superior QoS (Quality of Service) for circulating traffic.

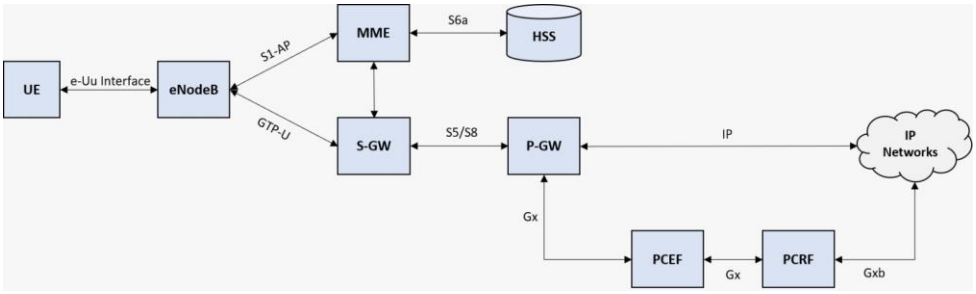

Figure 7. LTE Network Architecture. Source: Cox, Christopher (2014)

3.1.5 4G vs 5G

The evolution of the packet-based cellular network is boosted by the increasing need of provide time sensitive services in highly dense environments. Vendors such as Ericsson and Huawei agree on the idea that the evolution of 4G increases the capacity of the cellular network at least in 20 times which represents a business opportunity in terms of new products and services, but also a challenge for operators who need to increase the backbone capacity to meet the demand of traffic consumption that 5G networks can provide. Moreover, the introduction of a new technology in mobile networks implies some improvement in terms of spectrum efficiency with the adoption of mmWave that commercially has not been widely deployed but represents an opportunity for micro and femto cell to provide ultra fast speeds in where increase capacity is highly needed [10].

Metrics	4G	5G
Latency	10 ms	1 ms
Peak Data Rates	1 Gb/s	20 Gb/s
Spectrum	3 GHz	30 GHz
Connection Density	100k/Km2	1 million/Km2

Table 1. Comparison between 4G and 5G. Source: Hajlaoui, Zaier, Khlifi, Ghodhbane, Hamed and Sbita

3.1.6 The driving force behind the 5G network architecture transformation.

As mentioned, the introduction of a new generation cellular technology brings with it structural changes in the design of the network elements that provide the wireless service. The 5G network is going to fully adopt the separation of the control and user plane, hence the flexibility and scalability of the network is going to improve exponentially. In a paper publish by Huawei [11], the motivations associated to the 5G evolution are associated but not limited to the following points:

- **Complexity of service requirements:** since 5G networks are intended to be the catalyst to implement IoT devices, the wireless system must be able to provide a reliable service to support the diversity of requirements required by the UE's. The flexibility of the network must guarantee a smooth customer experience, not matter the converging technologies or the performance constraints.

- **Multi-connectivity and integration:** since the first stage of the deployment considers the coexistence of different Mobile Broadband (mBB) technologies, the smooth customer experience must rely on effective transitions of technology across the environment in where the users move. The network is responsible for guarantee service continuity while subscribers navigate the area of service, which means that the access is not going to be provided only by the traditional radio base station, but also by other non-3GPP access points.

- **Allocation of network elements:** because of the adoption of the CUPS approach, the allocation of services can be performed as required by the network. This means that real-time services may be fully deployed closer to the final user with the purpose of reduce latency, while the rest of the services can be implemented in cloud systems.

- **Orchestration of network functions:** due to the granular implementation of network functions, the management of these activities tend to be simple and efficient.

- **Fast service implementation:** the ecosystem of players that participates in the deployment of 5G systems is highly diverse, for instance, the implementation of new services relies on the ability of multiple players to integrate the landscape of services efficiently.

3.1.7 5G advantages and challenges

The implementation of 5G introduces a set of operational advantages that improves not only the efficiency of the network but also the user experience. Moreover, with the introduction of IoT, the requirements for these devices may be very specific in terms of power consumption, latency, or data rate. The following table summarized the advantages listed by ETSI [12] in comparison with the existing deployments of 4G.

Advantages	4G	5G
Peak data rate (Gbit/s)	1	20
User data rate (Mbit/s)	10	100
Spectrum efficiency	1x	3x
Mobility (km/h)	350	500
Latency (ms)	10	1

Connection density (devices/km2)	100k	1MM
Energy efficiency	1x	100x
Area traffic capacity (Mbit/s/m2)	0.1	10

Table 2. Summary of advantages 4G vs 5G. Source: ETSI

On the other hand, the introduction of the new technology also presents drawbacks for operators. In comparison with 4G, the adoption of mmWave reduces the range the cell station can reach as well as the penetration in-building which stresses the network operators in the sense that the current infrastructure must be expanded to provide the same coverage that legacy technologies currently do [13].

This issue mentioned above increases exponentially the cost of implementation for operators. Similarly, the implication of building new stations to comply with the current coverage patterns or even more improve it represents another challenge for service providers who need to deal with regulators and third-parties to build new infrastructure.

Finally, the security aspect is still a concern for every single player in the cellular network landscape. Even the 5G network introduces the Authentication and Key Agreement (AKA), there are still concerns related to privacy issues as shown across the development of this research. Moreover, the early implementations of 5G implies a dependency on legacy networks that may lead to disruptions that are well-known in the security landscape.

3.1.8 Security issues in cellular networks

The following chart summarizes the security issues characteristics of the cellular networks.

Security Facts			
	GSM	UMTS	LTE
Cryptography	Keys up to 128-bits long (A5/1)	Keys up to 128-bits long (KASUMI)	Keys up to 256-bits long (AES)
Hardware Security	Introduces SIM card to store the secret key of subscriber.		Introduces UICC to store cryptographic key and credentials.
UE Authentication	Uses authentication triplet (RAND, SRES, Kc)	Introduces AKA protocol	Implement AKA protocol
Air Interface	Communication between UE and BTS is encrypted using 64-bits keys (A5/1, A5/2, A5/3)	Communication between UE and BTS is encrypted using 64-bits keys (KASUMI)	Integrity protection must be provided to control plane, but optional to user plane.
Backhaul Sec	Not defined	Not defined, if needed, it has to be provided by the application layer.	Tunneling must be provided if physical protection to the interface is not guaranteed.
Core Network	Not defined	Encryption is provided only to signalling messages	CN divided into multiple security domains.

Table 3. Security issues for modern cellular networks.

The evolution of the cellular networks is correlated in several aspects. Each generation has strived for efficiency to address the limitations of previous designs; however, the most important featured introduced in modern architectures was the implementation of systems that would allow users to have access to Internet by deploying a relative fast IP platform that later would be full IP-based for 4G and 5G networks. Consequently, this research will be focused on analyzing the last two generations since they are meant to coexist in short, middle term.

3.1.8.1 Security in 4G

With the introduction of strata in UMTS to differentiate logical functions from network entities, it also originated a new approach to design the network security. The architecture proposed for 4G networks, in a similar way to 3G, defines five security features across three layers called Application stratum, Home/Serving stratum and Transport stratum. These three are intended to accomplish security objectives by implementing mechanisms inherent to their functions. [14]

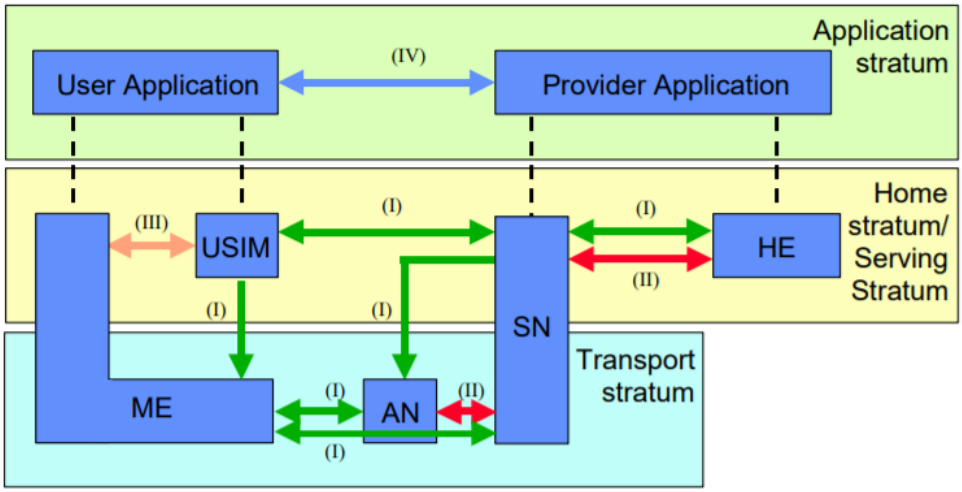

Figure 8. Overview of the security architecture in 4G. Source: TS 33.401

- **Network access security (I):** mechanisms to allow UE to authenticate into the network to get the service.
- **Network domain security (II):** mechanisms to secure the communication when signalling and user plane data is shared
- **User domain security (III):** mechanisms implemented at the UE to secure the communication between terminals and USIM.
- **Application domain security (IV):** mechanisms that secure communication between the user domain and the provider domain.
- **Visibility and configurability of security (V):** mechanisms that allow the network to inform what security features are enable.

Beyond the abstraction shown in the previous figure, the mechanisms associated to each security feature is given by the interaction of UE with the network. The first one is known as UE attach process. The figure 9 shows the flow of the process indicated in [15] but simplified in [16]. The description of messages presented in this research is focused on the security perspective of the process.

1) Attach Request
2) Authentication Data Request
3) Authentication Data Response
4) Authentication Challenge
5) Authentication Response

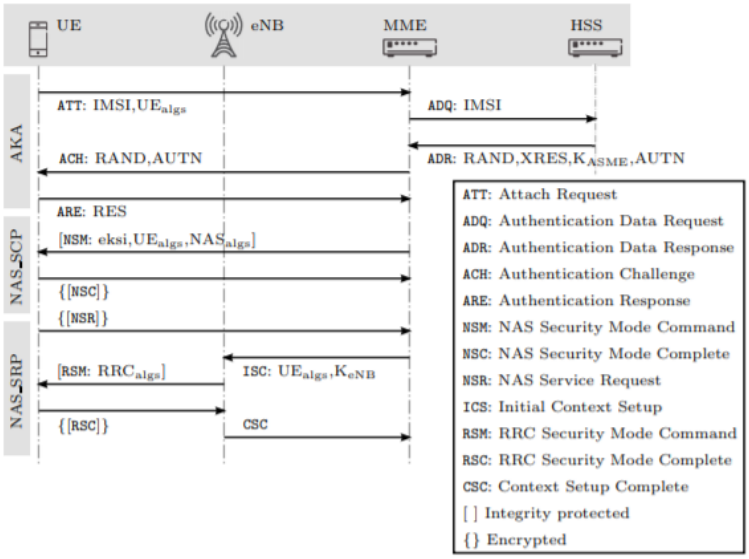

Figure 9. Security control and service request during attach process. Source: Ben Henda and Norman (2014)

3.2 Cybersecurity framework

3.2.1 Security for packet-based networks

The integration of packet-based communications to wireless networks adds benefits in terms of modularity and compatibility, however, it also brings with it all the vulnerabilities that have been present in traditional wired IP networks. Also, it adds the complexity of the wireless communication. This research will rely on ITU-T Recommendation X.805 to introduce the security architecture standardized to protect end-to-end communications.

Recommendation X.805 proposes to identify and divide the features of the end-to-end communication systems into three architectural components which are Security Dimension, Security Layers and Security Planes. This approach reduces the complexity of the solution, eases the security planning, embodies modularity and enhances the perspective on the network elements that can be targeted by attackers.

3.2.1.1 Security Dimension

Recommendation X.805 suggests eight security measures to handle most of the network security aspects as well as protect the network from well-known security threats.

- **Access control policy:** it proposes a Role-Based Access Control (RBAC) approach to manage the access to the functionalities provided by the network or applications at carriers or users levels.

- **Authentication policy:** it is referred to the mechanisms that can be implemented to validate the identity of entities and ensure the legitimacy of credentials.

- **Non-repudiation policy:** it intends to enable alternative methods of validation to prevent rejection of users by performing additional steps to proof the identity.

- **Data confidentiality policy:** this policy indicates that data cannot be readable by unauthorized entities if a data breach occurs. Methods associated to this policy are encryption, access lists and file permissions.

- **Communication policy:** it specifies that data in transit must be sent and received by authorized entities.

- **Data integrity policy:** it is oriented to ensure that data is protected from any attempt to alter the content by implementing verification methods at sender and receiver.

- **Availability policy:** it ensures that entities can access the resources of the network by given means. This policy must be designed to guarantee availability even when the network is impacted by any event.

- **Privacy policy:** it is charge of securing the data generated from user activities such as web-browsing, gps location, ip address granted, etc.

3.2.1.2 Security Layers

ITU recommendation also indicates that the network elements must be classify according to their functionalities in order to establish a hierarchy to secure the elements. Then, the security measures mentioned before must be applied to this hierarchy to create security layers. In general, these security layers are known as Infrastructure Security Layer, Services Security Layer and Applications Security Layer.

- **Infrastructure Security Layer:** it is related to the security of most of the components of the physical layer.

- **Services Security Layer:** it is related to the security services provided by ISP's. This covers basic functionalities such as connectivity and data transportation as well as more complex services such as location, instant messaging, QoS, etc.

- **Applications Security Layer:** it is oriented to secure critical applications that serve customers with IT platforms needed to perform daily life routines. Precisely, this layer is in charge of preventing attacks to the application in execution by clients, the servers that host the applications, the middleware between backend and frontend and the services provided by ISP's.

3.2.1.3 Security Planes

Since most of the networks are designed to have different layers working independently one from each other, the ITU recommendation specifies that the network activities must be protected by implementing the security measures mentioned in 3.2.1.1. These activities are going to be classified in 3 planes which are Management, Control and End-User plane.

- **The management plane:** the security measures to be implemented must protect the O&M functions such as the ones specified in the ISO model for network management tasks called FCAPS (Fault, Configuration, Accounting, Performance and Security)

- **The control plane:** it is the layer in charge of sending signalling and control information between devices to guarantee the proper configuration and operation of the network.

- **The end-user plane:** it is referred to the layer that allow users to get access to the network and its services.

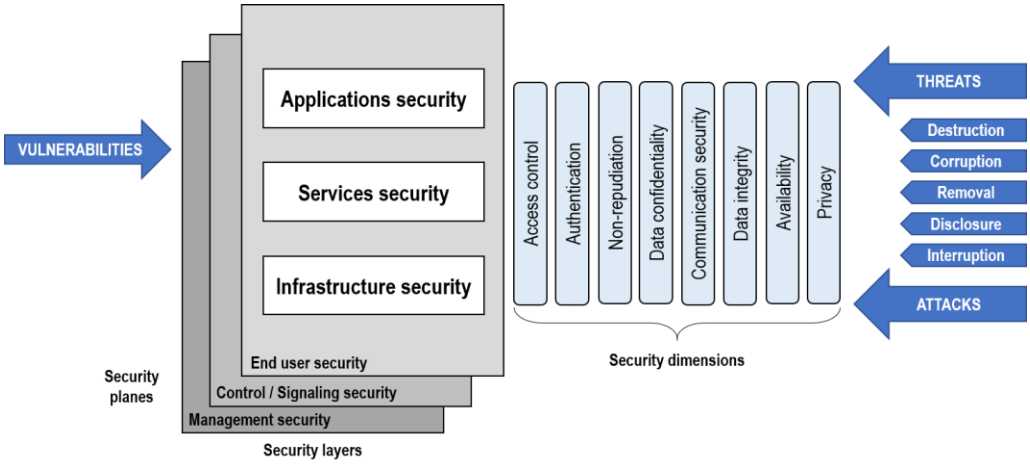

Figure 10. X.805 Framework. Source: ITU

CHAPTER 4

THEORETICAL PERSPECTIVE

4.1 Literature Review

This research pretends to study the convergency of cellular networks, cybersecurity and artificial intelligence. Since the theoretical background of these three disciplines can be extensive, the following sections will analyze the security perspective of them.

4.1.1 5G Network Architecture

As specified in [17], the 5G system was designed to provide fast Internet connections through wireless communications. The architecture makes use of Network Function Virtualization (NFV) and Software Defined Networking (SDN) technologies, it separates the User Plane (UP) functions from the Control Plane (CP) functions and reduces dependencies between the access network (AN) and core network (CN) which gives operators flexibility and scalability during the lifecycle of the network.

The independency of the AN and CN allows operators to allocate latency sensitive services closer to the AN and UE (User Equipment) which reduces the transit of data over the network. Finally, in [17] it is indicated that the network supports a unified authentication framework that supports Extensible Authentication Protocol (EAP) and is agnostic to 3GPP and non-3GPP networks [18]

In 5G networks, the architecture shown in figure 12, defines several Network Functions (NF) which are entities that can be implemented as a network element or a software instance running on a dedicated hardware. [19] These mechanisms are oriented to classify, categorize and process services according to their requirements. The figure 13 shows the NF's thar are considered essential, meanwhile, figure 11 shows the architecture.

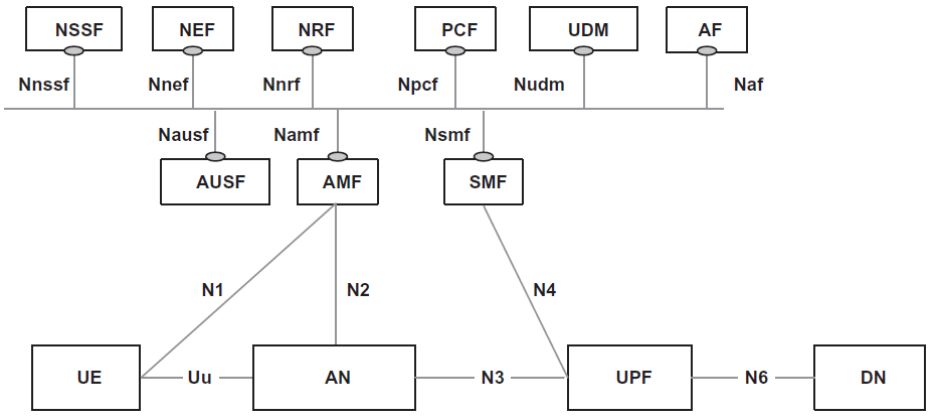

Figure 11. 5G Network Architecture. Source: TS 23.501

Network Functions	Functionalities
User Plane Function (UPF)	Anchor point for Intra/Inter RAT mobility External PDU session point of interconnect Data Network Packet routing and routing Packet inspection User plane part of policy rule enforcement Lawful intercept Traffic usage reporting QoS handling for user plane (UL/DL rate enforcement) Uplink traffic verification (SDF to QoS flow mapping) Transport level packet marking in the uplink and downlink Downlink packet buffering and downlink data notification trigger Sending and forwarding of one or more end marker to the source ARP proxy or IPv6 Neighbour Solicitation providing MAC address
Access Network (AN)	Functions related to the gNB.
Application Function (AF)	Interacts with core network (CN) to influence traffic routing, accessing to Network Exposure Functions and interacting with policy the policy framework for policy control.
Access and Mobility Management (AMF)	Termination of RAN CP Interface (N2) Termination of NAS (N1), NAS ciphering and integrity protection Registration management Connection management Reachability management Mobility management Lawful intercept Provide transport for SM messages between UE and SMF Transparent proxy for routing SM messages Access authentication Access authorization Provide transport for SMS messages between UE and SMF Security anchor functionality Location services management for regulatory services Provide transport for messages between RAN and LMF EPS bearer ID allocation for internetworking with EPS
Session Management Function (SMF)	Establishment, modify and release between UPF and AN node UE IP address allocation & management DHCPv4 DHCPv6 server and client functions ARP proxy or IPv6 Neighbour Solicitation providing MAC address Traffic steering at UPF to route traffic to proper destination Termination of interfaces towards policy control functions Lawful intercept Control and coordination of charging data collection at UPF Termination of SM parts of NAS messages Downlink data notification Initiation of AN specific SM information sent to AN via AMF (N2) Determine SSC mode of a session Roaming functionality

Table 4. Essential NF of 5G architecture. Source: TS 21.915

Additionally, there are other NF's which are the following

Network Functions	Functionalities
Network Exposure Function (NEF)	Expose network capabilities and events to other NF's Stores/retrieves information to the UDR Provision of information from external applications to 5G network Re-expose the information stored in UDR to other NF's or AF's.
Network Repository Function (NRF)	Receives discovery request and provide information to NF instance Maintains the NF profile of available NF instances and services.
Unified Data Management (UDM)	Generation of 3GPP AKA authentication credentials User identification handling

	Support of de-concealment of privacy-protected subscription identifier (SUCI) Access authorization based on subscription data UE's serving NF registration management Support service/session continuity by keeping SMF/DNN assignment of ongoing sessions MT-SMS delivery support Lawful intercept functionality Subscription management SMS management
Authentication Sever Function (AUSF)	Supports authentication for 3GPP access and untrusted non-3GPP access
Network Slice Selection Function (NSSF)	Selecting the set of Network Slide instances serving the UE Determine and map the NSSAI Determine the configured NSSAI Determine the AMF set to be used to serve the UE or a list of candidate AMF's by querying the NRF.
Policy Control Function (PCF)	Supports unified framework to govern network behaviour Provides policy rules to Control Plane functions to enforce them Accesses subscription information for policy decisions in UDR.
Unified Data Management (UDM)	Generation of 3GPP AKA authentication credentials User identification handling Support of de-concealment of privacy-protected subscription identifier (SUCI) Access authorization based on subscription data UE's serving NF registration management Support service/session continuity by keeping SMF/DNN assignment of ongoing sessions MT-SMS delivery support Lawful intercept functionality Subscription management SMS management
Unified Data Repository (UDR)	Storage and retrieval of subscription data by the UDM Storage and retrieval of policy data by PCF Storage and retrieval of structure data for exposure Application data
Unstructured Data Storage Function (UDSF)	Storage and retrieval of information as unstructured data

Table 5. 5G NF of 5G architecture. Source: TS 21.915

4.1.1.1 5G Access Network

The network element associated to the radio access network (RAN) is the gNB. Its functions are proving the radio and propagation services to the network such as Radio Bearer Control, Radio Admission Control, Connection Mobility Control, as well as the dynamic allocation of resources to the UE [20]. However, 5G access network takes advantage of the separation between the control and user plane to evolve towards the Cloud Radio Access Network (C-RAN), hence it must be able to support resource pooling, scalability layer internetworking and mobility. [21]

- **Cloud RAN:** it presents a distributed architecture that contains Band Base Unit (BBU), interconnected to a Radio Remote Unit (RRU) by an optical fiber. This system delivers the signal to the antenna in the frequency desired. In [22], it is indicated that C-RAN is a fully centralized system in where BBU performs duties of physical, data link and network layer as well as upper layer activities such as transport and security, meanwhile the RRU is in charge of RF duties to deliver the signal to the antenna.

  The centralized system provides significative advantage in terms of network expansion since a Radio Base Station (RBS) can increase its capacity by adding or replacing the BBU, however,

this approach has the drawback of demanding high bandwidth and computing resources to process the signal send by the RRU, then a partial centralized C-RAN pretends to reduce the resources needed in the BBU by performing demodulation at the RRU.

This approach is how 3G/4G networks were deployed through the NodeB/eNode B, however the introduction of Software Define Radio (SDR) allows to handle RRU resources independently of the BBU in where it is connected. Certainly, virtualization of BBU resources allows to manage in real-time the processing capacity designed for the BBU pool, hence the RRU's can cover a large physical area being managed by the centralized BBU [22].

- **Heterogeneous RAN**: this concept pretends to eliminate interferences between Macro Base Stations (MBS) and Low Power Node (LPN) by implementing processing techniques in which RRU's cooperate between them to improve utilization of the air interface as well as network resources such as Large-Scale Cooperative Spatial Signal Processing (LS-CSSP), Large-Scale Cooperative radio Resource Management and Large-Scale Self Organizing H-CRAN (LS-SON) [23].

- **Fog RAN:** it intends to exploit the processing capabilities at the edge of the network by adding cache to the user terminal as well as the RRU's, then the centralized system will manage the resources of the BBU pool.

4.1.1.2 The NSA vs SA architecture

The deployment of 5G technology is conceived to coexist with 4G while 5G is deployed massively. For instance, this research will analyse the Stand-Alone scenario and a couple of variants of the Non-Stand-Alone proposal that considers the transition of the deployments. The Stand-Alone architecture presented in [20] TR 21.915 shows a fully deployed 5G system in where 4G is not longer needed to perform the network functions. The gNB performs the radio and RAN functions and connects to CN directly through the NG interface.

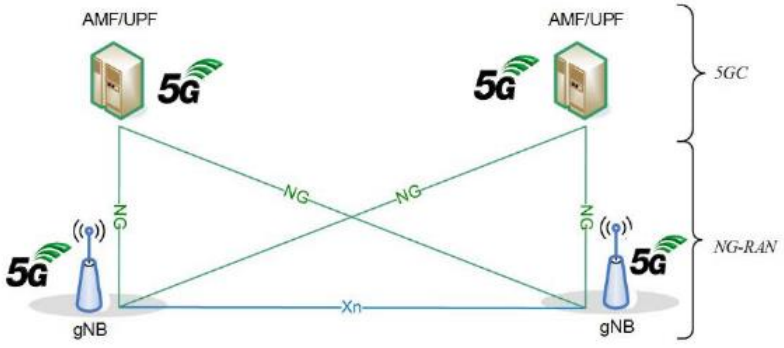

Figure 12. The Stand Alone 5G Architecture. Source: TR 21.915

It is also defined a Non-Stand-Alone architecture in where the en-gNB performs the functions of the Radio Access Network as well as provides the 5G radio interface. This entity interacts with the existing LTE CN and AN. This proposal is known as E-UTRA-NR Dual Connectivity (EN-DC) or "Architecture Option 3" as is shown in figure 13 [20].

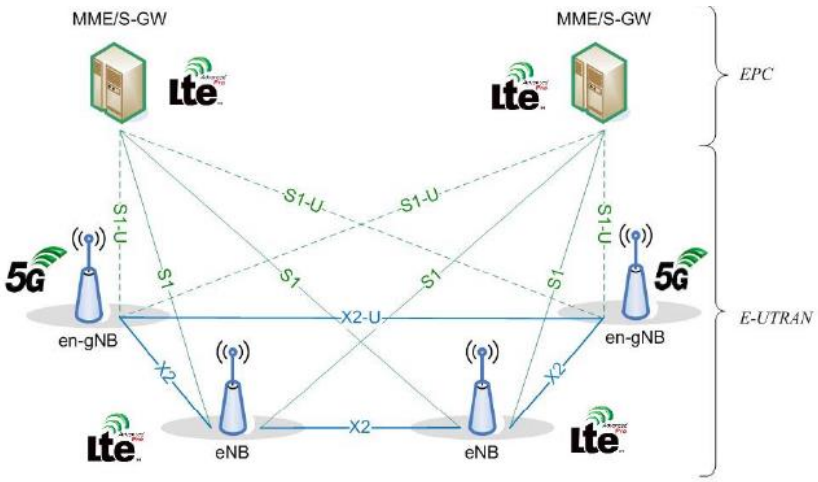

Figure 13. The Non-Stand-Alone Architecture. Source: TR-21.915

The other variant of the Non-Stand-Alone architecture which requires of the full deployment of the core network. This model introduces the concept of ng-eNB which is an entity that provides the functionalities of the LTE access network as well as the radio interface, but it may be connected to the 5G core network directly through the NG interface or to a master node gNB via the Xn interface. The figure 14 shows the NG-RAN architecture.

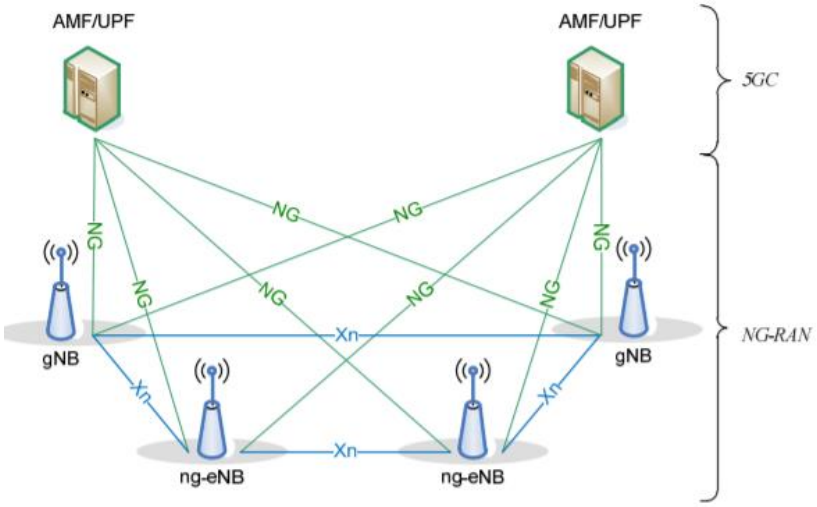

Figure 14. NG-RAN architecture. Source: Journal of ICT, Vol. 6 1&2, 59–76. River Publishers

4.1.1.3 Protocol Stack

As defined in [17], there are two protocol stacks defined for 5G network. On one side, the Control Plane Protocol Stack handles the signalling and control information from the UE through the AN until reach the CN, while the User Plane Protocol Stack transport data through the access stratum until reaching the external network or Internet [20]. The layer one protocol is identified as PHY, the layer two protocol is divided into four sublayers which are MAC, RLC, PDCP and SDAP, and the layer three is called RRC [19].

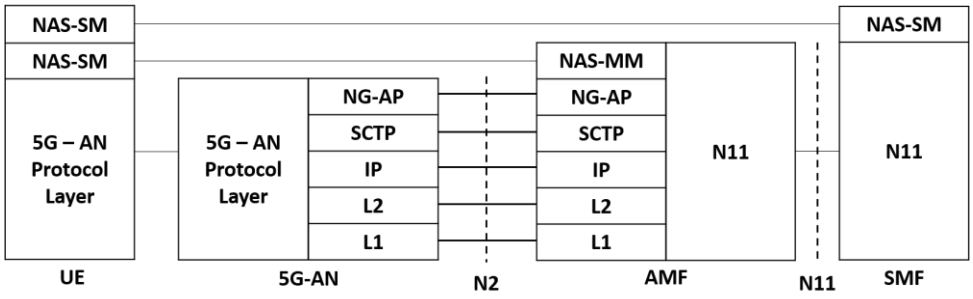

Figure 15. Protocol Stack - Control Plane. Source:

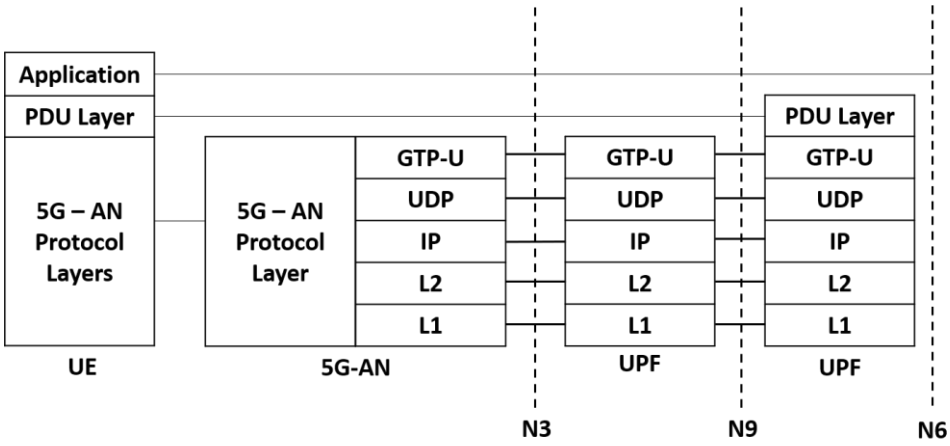

Figure 16. Protocol Stack - User Plane. Source:

4.1.1.4 Physical Layer

Frame Structure

The frame defined in [20] divides the time domain in 10 ms radio frames with 10 subframes of 1 ms.

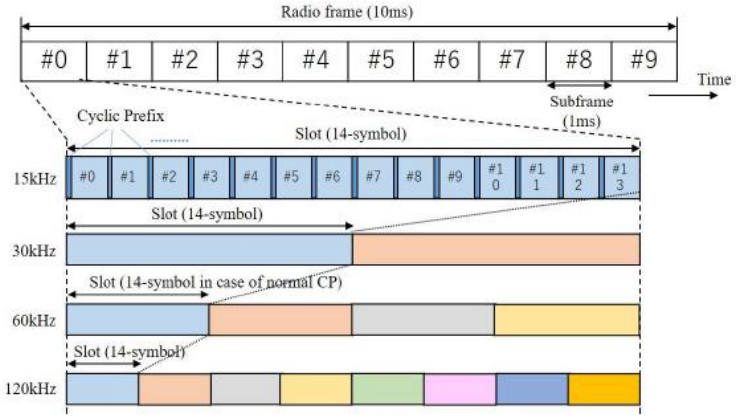

Figure 17. 5G frame structure. Source: TR 21.915

Spectrum and System Bandwidth

As indicated in [20], 5G can work in four type of bands. The first one is associated to the portion of spectrum that can be released if refarming is applied to an existing 4G network. The second and third type are described in Table 3, while the fourth one is related to the network capabilities to operate in supplemental uplink / downlink in FR1, FR2.

Frequency band	Frequency range	Channel Bandwidth (MHz)
FR1	410 MHz – 7125 MHz	5, 10, 15, 20, 25, 30, 40, 50, 60, 80, 90, 100
FR2	24250 MHz – 52600 MHz	50, 100, 200, 400

Table 6. 5G frequency bands. Source: TR 21.915

4.1.1.5 Data Link Layer

This layer is divided into four sublayers which are: Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Conversion Protocol (PDCP), and Service Data Adaptation Protocol (SDAP). Figure 15 shows the interaction with layer 1 and layer 3 as well as the services that are provided between sublayers. Table 3 summarizes the functions of each sublayer.

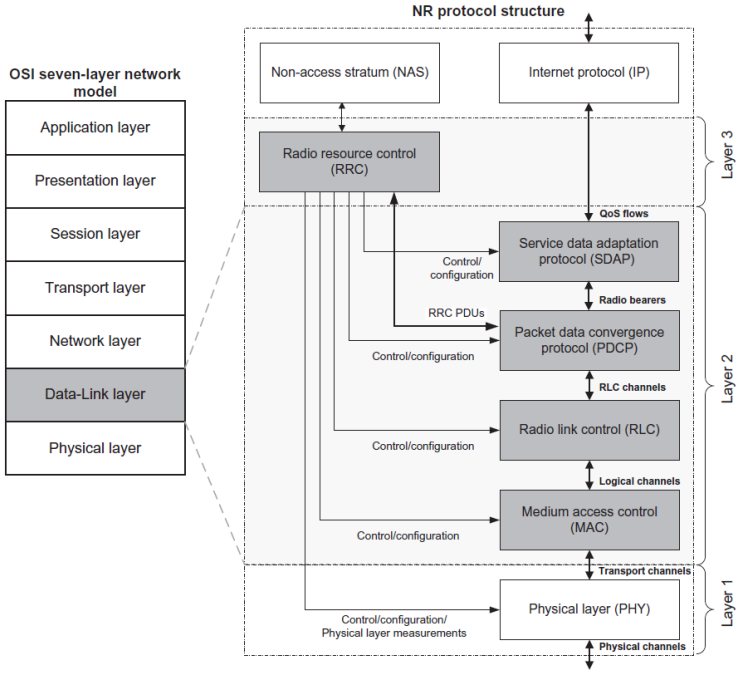

Figure 18. Sub-divisions of Data-Link layer

Sublayer	Services and Functions
MAC	-Mapping between logical and transport channels. -Mux/Demux of SUD's. -Error correction through HARQ. -Priority handling between UE. -Priority handling between logical channels of one UE. -Padding
RLC	-Transfer of upper layer PDUs -Sequence numbering independent of the one in PDCP -Error Correction through ARQ -Segmentation (AM and UM) and re-segmentation (AM only) of RLC SDUs -Reassembly of SDU -Duplicate Detection -RLC SDU discard -RLC re-establishment -Protocol error detection
PDCP	**For User Plane** -Sequence Numbering -Header compression and decompression: ROHC only; -Transfer of user data; -Reordering and duplicate detection; -In-order delivery; -PDCP PDU routing (in case of split bearers); -Retransmission of PDCP SDUs; -Ciphering, deciphering and integrity protection; -PDCP SDU discard; -PDCP re-establishment and data recovery for RLC AM; -PDCP status reporting for RLC AM; -Duplication of PDCP PDUs and duplicate discard indication to lower layers. **For Control Plane** -Sequence Numbering; -Ciphering, deciphering and integrity protection; -Transfer of control plane data; -Reordering and duplicate detection; -In-order delivery; -Duplication of PDCP PDUs and duplicate discard indication to lower layers.
SDAP	-Mapping between a QoS flow and a data radio bearer -Marking QoS flow ID (QFI) in both DL and UL packets.

Table 7. DLL Sublayer functions. Source: TS 38.300

4.1.2 5G enabling technologies.

4.1.2.1 Virtualization of Network Functions

In the context of cellular networks, operators make use of the NFV to integrate networking services into high-capacity servers that provide processing and storage capabilities. Operators take advantage of the flexibility and scalability that these housing systems provide to implement the network functions of the 5G systems in different locations as it is required by the network design.

With the introduction of 5G, the network operators can implement an architecture as shown in the figure below, in where there are four main blocks which are: Network Function Virtualization Infrastructure (NFVI), Virtualized Infrastructure Manager (VIM), Management and Orchestration (MANO), and Software-defined networking (SDN) controller.

The NFVI is built by all the physical computing and storage capacity as well as the networking resources that virtualized network functions need to operate. These devices are controlled by the VIM which is in charge of managing the virtual capacity of the underlying physical resources. The VIM is the key element that supports the principle of scalability in the network since the hardware can be expanded as much as required but still managed by the same entity without impacting the other integrators of the NFV architecture. In parallel, the MANO delivers while the SDN controller represents the anchor point for the network functions defined in the 5G architecture.

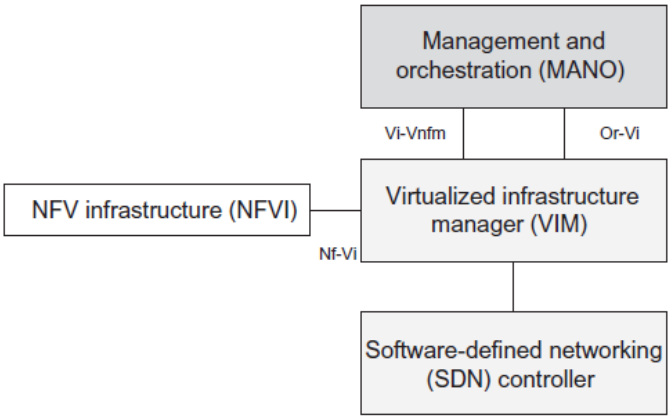

Figure 19. High-level of NFV architecture. Source:

4.1.2.2 Software-Defined Networks

Previously it was mentioned that 5G networks fully implement the CUPS architecture, for instance, the separation of control and user plane converts the traditional network elements in programmable entities who are in charge of managing the flow on traffic at the control plane and enforce the compliance of the SLA in the user plane. By configuring the control plane, the network is able to provide different levels of Quality of Service and traffic discrimination to meet the user demands, incorporate new mechanisms, and leverage security [24].

In the same context of 5G, once the RAN establishes a data flow for first time, the RAN forwards the packet to the controller which analyses the packet header. With certain configuration rules, the control plane defines the treatment of the data flow and informs the other network elements how to deal with packets that present similarities [24].

4.1.2.3 Network Slicing

The architecture proposed for 5G networks relies on network functions to assign resources and provide an SLA to the different use cases. As mentioned in [25] and [20] there are 4 slices to support 5G services which are: enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), massive Internet of Things (mIoT) and default slice. The advantage of the network slicing is that resources are provided independently within each slice, so it improves end-to-end communication.

Network Slice	Type of Services
eMBB	Ultra-High Definition Video 3D Video AR/VR Delivering to User High Definition Video Sharing
URLLC	VR machine interaction Industrial Automation Sensing
mIoT	Control of production process Health applications Real-time automation
Default	Local services

Table 8. Network Slicing classification. Source: Ericsson 2020

4.1.2.4 MIMO Aspects

5G systems implement MIMO (Multiple In, Multiple Out) technology to provide exceptional throughput by embedding a large number of antenna elements into multiple antenna panels. This arrangement improves the radiation pattern in a single cell which optimizes gains and provide better coverage in terms of user experience. This feature is widely used in stations operating in frequencies over 6 GHz, in where radiation patters is narrower than in lower bands [19].

Particularly, 5G system enables MIMO operation introducing new signals in the communication flow that are used to manage the radiation pattern. Indeed, these signals allow the network to measure and manage resources as well as report the channel state information (CSI) to the UE. The flow of information between the network and the UE establishes a dynamic interaction that lets UE to choose the beam that offers the best UP/DL conditions [19].

4.1.2.5 mmWave

The spectrum for cellular technologies under 1 GHz is saturated due to the current operation of old technologies such as GSM, UMTS and LTE, the conceptualization of 5G had to explore the spectrum in order to find suitable ranges that make possible the deployment, besides the expectation set around the ultra-high speed that the 5G network must provide led the 3GPP group to introduce the concept of mmWave to exploit the licensed bands in the 3-6 Ghz range as well as the spectrum above 26 GHz. And take advantage of the multiple channels and large bandwidth [19].

The research being conducted by regulators, operators and vendors have classified the utilization of the spectrum in function of the performance needed by the different applications that build the ecosystem [19]. Initially, the sub-1 GHz spectrum is still considered for operability of legacy technologies and the introduction of the NSA model explained in 4.1.1.2, in addition, the propagation in this range place it in the position to be considered to provide coverage in large areas. The range of 3-6 GHz is expected to be implemented in the urban landscape where mobility can be handled and provide exceptional bandwidth, while the spectrum above 26 GHz is oriented to support the implementation of fixed applications making use of massive MIMO [19].

4.1.2.6 Device-to-Device Communication

The New Radio (NR) allow devices to communicate between them without the support of infrastructure or access points to establish the communication [26]. In the 5G context, the D2D technology prototypes two scenarios. The first one enables wireless communication between

terminals which are physically close when the communication the base station is lost. The figure below illustrates this case.

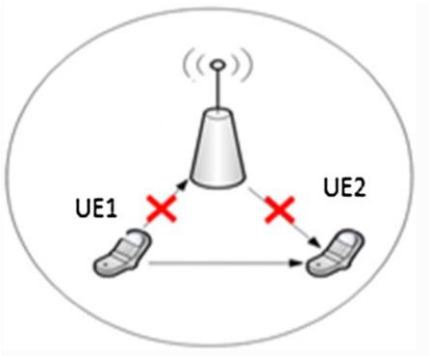

Figure 20. D2D Network Layout. Source: D2D Relay mode. Source: Hussein, Elsayed and Abs El-kader (2020)

On the other hand, the second model is oriented to extend the coverage by enlarging the footprint that a station provides making use of the transmission capabilities that the UE's have to relay the signal toward the devices that experience poor service or no signalling. This approach improves the spectrum efficiency since a range of bands can be reused in contiguous areas without interfere the smooth operation [27]. The figure below illustrates this case.

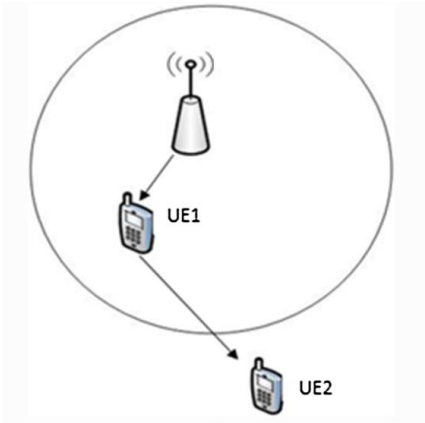

Figure 21. D2D Relay mode. Source: Hussein, Elsayed and Abs El-kader (2020)

4.1.2.7 Ultra-densification

The design of the previous generation of cellular networks relied on the RAN capacity to meet the user demands. However, the trend for this generation of mobile networks focuses its efforts on diversify the characteristics of the frontline network elements. Particularly, the technology makes use of the mmWave to introduce different base stations or gNB's in order to meet all the conditions in a given scenario.

Since the expectation is to have around 100 billion of devices connected to wireless networks by 2030, the operators need to increase the capacity in at least 1000 times in comparison with the current data rates. The approach foresaw goes through the massive deployment of macro cell stations to enlarge coverage, but also femto and picocells to support highly dense environments of 6 people per square meter [28].

As explained previously, the adoption of mmWave significantly reduces the wireless footprint, but it introduces a large broadband that can be exploited as the channel capacity increases. The implementation of several stations in relatively small areas certainly improves the efficiency of the spectral resources however, these deployments can disrupt the capacity of the network if interference occurs. For instance, UDN stipules an interference management approach to rebuilt signals that suffer overlapping, decode them, and remove the distortion from the air interface [28].

4.1.2.8 Internet of Things

With high data rates and improved reliability, the introduction of 5G is meant to be the main driver to boost the massive adoption of objects that go beyond the landscape presented by smart phones and tables. Operators must work now on the evolution of their business models to build an ecosystem of devices that includes self-driven cars, machinery sensors as well as the already known consumer electronics.

Even the industry has came up with a series of protocols to introduce IoT devices such as Zigbee or Bluetooth, the deployment of 5G systems will adopt the principle of massive IoT due to the ability to provide large high data rates, ultra-low latency, provide synchronization as a service and even more enhance the battery life of the devices. These functionalities normally run on the top of the IP protocol, so the reliability on the upper layers plays a key on the smooth quality of service to be experience by customers.

On the network side, the IoT is possible thanks to the introduction of Network Slicing, Network Exposure, and the adoption of Data Analytics. The ability to create and isolate multiple virtual networks can dedicate resources to the slices to differentiate the levels of service and meet SLA's. Moreover, the network exposure allows to monitor the performance of network as well as enable network programming. Finally, the fact of collecting data, improves the operation of IoT services by adjusting dynamically the bandwidth dedicated to each slice, performing dynamic routing to keep exceptional levels of latency, and detecting abnormal traffic patterns [29].

4.1.3 Unified Access Control

5G networks also implemented a new mechanism based on profiling to deal with congestion issues. This approach takes advantage of the slices definition, so the network identifies and grants access in function of network policies, user profiles, resources available or scenarios. In this case the CN relies on NG-RAN to define a network domain and broadcast control packets with access, categories, and identities, then the UE can figure out if conditions are given to log in into the network domain [20].

4.1.4 Service Requirements

The architecture described before opens the range of UE's that can communicate in the network, in addition, it introduces capabilities that challenge the performance of current networks. In [30] is mentioned the basic requirements to meet by new deployments among them

4.1.4.1 Mobility management

The landscape of devices and services foreseen to make up the ecosystem of 5G is highly diverse, moreover, network densification and heterogeneity represent key challenges to design 5G networks [31]. Additionally, the implementation of micro, pico and femto cells increases the quantity of gNB's in a limited area, but on the other hand, there will be a massive quantity of scenarios with different requirements of user/device experience. In [30] it is specified the following mobility management needs:

- Stationary during the entire usable life of the device.
- Stationary while active, but mobile in passive periods.
- Mobile within a specific location.
- Fully mobile.

The needs mentioned before can become more complex if the scenarios add other constrains related to applications of null interruption time, real-time visualization or simply high broadband consumption, then 5G systems allow operators to classify the UE's according to the mobility patterns. Moreover, when changes in network configuration are needed due to mobility of inter/intra networks, the loss of connection must be minimized in order to mitigate the impact over the user experience [30]. Finally, in order to deal with the scenarios mentioned previously, it is suggested that the design of the system must be flexible to allocate radio resources as well as provide efficient signalling, and dynamic self configuration of RAN [31].

4.1.4.2 Multiple access technologies

The introduction of 5G networks in the market represents an enormous business opportunity for carriers then this technology comprises the integration with legacy systems such as LTE, but also non-3GPPP technologies. Interoperability with non-3GPPP can be seem like an improvement in terms of coverage and availability, then the cellular system must provide access to devices that work in E-UTRAN, Satellite, and fixed broadband domains [30].
In a general scope, the 5G network must be able to guarantee basic network parameters such as authentication and authorization, data rate, services, radio capabilities, etc. but also must provide a smooth transition between 5G and E-URAN systems, smooth transitions between satellite and 5G networks and reach consumer through dedicated fixe broadband systems [30].

4.1.4.3 Resource efficiency

Since the landscape of devices that will be connected to 5G systems is broad and undefined, the 5G system must relied on UE classification to allocate resources efficiently. Categorization eases the traffic administration into the slicing scheme, then devices consuming highly sensitive services receive the proper treatment, then, simple IoT devices that constantly send short packets can process efficiently the characteristic burst of traffic that they generate, smartphones will receive the data flow needed for streaming services meanwhile those terminals that rely on computing capabilities of cloud, will count on very high availability and low latency [30].

4.1.4.4 Efficient content delivery

In order to provide a smooth experience to final users the 5G network has to provide caching services at ran and core network. The system must provide operators autonomy to manage resources and deal with constrains when processing multicast traffic.

4.1.4.5 Priority, QoS, and policy control

According to TS 22.261, 5G systems must allow operators to categorize and provide quality of service even if traffic have very similar requirements. The network controls parameters such as reliability, latency and bandwidth for a given traffic considering the heterogeneous characteristic of 5G networks.

4.1.4.6 Network capability exposure

5G networks can share their capabilities to other networks in order to guarantee QoS in an end-to-end communication. For instance, the TS 22.261 indicates that 5G systems must deliver enough and reliable information to their peers in order to manage the network slicing, but also peers may receive valuable information to adjust their capabilities to the requirements given by the UE.

4.1.4.7 Context aware network

Specification TS 22.261 refers this requirement to the mechanism that must be implemented in 5G systems to enhance the user experience of the diversity of applications that can be integrated in the UE. The network must optimize the usability of functionalities by analyzing the characteristics of traffic and assigning the proper quantity of resources to meet the internal policies.

4.1.4.8 Flexible broadcast/multicast service

This requirement intends to promote the usability of 5G networks as an alternative to current fixed/mobile broadband deployments. For instance, the specification TS 22.261 indicates that system must support broadcast/multicast in UHD format as well as it gives the operators the control over the radio resources to assign up to 100% of them if the environment needs it.

4.1.4.9 Subscription aspects

The 5G system must provide the traditional mechanisms to provision customers but also must consider the heterogeneous environments in where IoT devices can be enable, then the network has to implement capabilities to differentiate the large range of devices that can be connected as well as provide connectivity services as defined in a contract service.

4.1.4.10 Energy efficiency

Since the type of devices that can be connected to the 5G network is quite broad, the energy capabilities of each are also diverse, then 5G systems must implement mechanism to reduce the battery drain by enabling an energy saving mode and restricting communication to a group of users

4.1.4.11 3GPP access network selection

The new deployments of 5G network must support service types to differentiate the UE requirements and properly address the network slice needed to meet the demands. Then, the system must manage the identifiers to comply provide resources to the UE. This means that UE operating in roaming or external networks, may not experience the same behaviour the had in their home network.

4.1.4.12 eV2X aspects

The 5G network must support connectivity for Vehicle-to-Everything services then, the system has to provide exceptional services for messaging between other vehicles, cloud-based platform to get information about routes or adjust the rhythm of driving for public transportation.

4.1.5 5G key capabilities

The TS 22.261 classifies the network requirements in high data rates and traffic densities, low latency and high reliability and higher-accuracy positioning.

4.1.5.1 High data rates and traffic densities

Scenario	Data Rate (DL)	Data Rate (DL)	Area Traffic Capacity (DL)	Area Traffic Capacity (UL)	User Density	UE speed
Urban Macro	50 Mbps	25 Mbps	100 Gbps/Km^2	50 Gbps/Km^2	10000/Km^2	Up to 120 Km/h
Rural Macro	50 Mbps	25 Mbps	1 Gbps/Km^2	500 Mbps/Km^2	100/Km^2	Up to 120 Km/h
Indoor Hotspot	1 Gbps	500 Mbps	15 Tbps/Km^2	2 Tbps/Km^2	250000/Km^2	Pedestrians
Broadband in the crowd	25 Mbps	50 Mbps	4 Tbps/Km^2	7,5 Tbps/Km^2	500000/Km^2	Pedestrians
Dense Urban	300 Mbps	50 Mbps	750 Gbps/Km^2	125 Gbps/Km^2	25000/Km^2	Up to 60 Km/h
Broadcast Services	200 Mbps per channel	N/A	N/A	N/A	15 Channels of 20 Mbps	Up to 500 Km/h
High-Speed Train	50 Mbps	25 Mbps	15 Gbps/Train	7,5 Gbps/Train	1000/Train	Up to 500 Km/h
High-Speed Vehicle	50 Mbps	25 Mbps	100 Gbps/Km^2	50 Gbps/Km^2	4000/Km^2	Up to 250 Km/h
Airplanes	15 Mbps	7,5 Mbps	1,2 Gbps	600 Mbps	400/plane	Up to 1000 Km/h

Table 9. High Data Rates and Traffic Densities requirements. Source: TS 22.261

However, the data shown above is based on the definition of the standard. Third party organizations have performed different tests to understand the practical values that can be gotten with current equipment. The tests conducted by T-Mobile and Rohde & Schwarz resulted in significative improvements in comparison with the data rate handled by LTE but still away from the theoretical values indicated by the 3GPP group. The next table shows the value measured under ideal conditions.

Frequency band	SCS	Bandwidth	Practical DL	Practical UL	Efficiency DL	Efficiency UL
FR1	15 kHz	50 MHz	288.9 Mbps	309.1 Mbps	5.78 bps/Hz	6.18 bps/Hz
FR1	30 kHz	100 MHz	584.3 Mbps	625 Mbps	5.84 bps/Hz	6.25 bps/Hz
FR1	60 kHz	100 MHz	577.8 Mbps	618.1 Mbps	5.78 bps/Hz	6.18 bps/Hz
FR2	60 kHz	200 MHz	1.08 Gbps	1.18 Gbps	5.40 bps/Hz	5.90 bps/Hz
FR2	120 kHz	400 MHz	2.15 Gbps	2.37 Gbps	5.38 bps/Hz	5.93 bps/Hz
LTE	15 kHz	20 MHz	100 Mbps	100 Mbps	5.00 bps/Hz	5.00 bps/Hz

Table 10. 5G practical data rates. Source: Rohde & Schwarz 2019.

4.1.5.2 Low latency and high reliability

Scenario	Max latency allowed	Survival Time	Availability	Reliability	User Experience Data Rate	Traffic Density	Connection Density
Discrete Automation	10 ms	0 ms	99,99%	99,99%	10 Mbps	1 Tbps/Km^2	100000/Km^2
Process Automation – Remote Control	60 ms	100 ms	99,9999%	99,999%	1 Mbps up to 100 Mbps	100 Gbps/ Km^2	1000/Km^2
Process Automation – Monitoring	60 ms	100 ms	99,9%	99,9%	1 Mbps	10 Gbps/ Km^2	10000/Km^2
Electricity Distribution – Medium Voltage	40 ms	25 ms	99,9%	99,9%	10 Mbps	10 Gbps/ Km^2	1000/Km^2
Electricity Distribution – Medium Voltage*	5 ms	10 ms	99,9999%	99,999%	10 Mbps	100 Gbps/ Km^2	1000/Km^2

Intelligent Transport Systems – Infrastructure backhaul	30 ms	100 ms	99,9999%	99,999%	10 Mbps	10 Gbps/ Km^2	1000/Km^2

Table 11. Low latency and high reliability requirements. Source: TS 22.261

In terms of latency and reliability, the experiment conducted by T-Mobile tested the latency in an environment that simulated the demands of self-driving cars. The results indicated that the 5G technology reduced the latency for this kind of services reaching 3ms of delay under ideal conditions.

4.1.5.3 Higher-accuracy positioning

As specified in TS 22.261 the requirements of positioning are oriented to provide a service in which self-driven vehicles must know their location and avoid collisions. The accuracy of the service must guarantee that object in movement can transit even in narrow aisles with millimetric precision.

4.1.6 Security in cellular networks

The recent deployments of cellular networks show that each time a new technology is introduced, it coexists with the previous generation for a moderate period. Mainly due to the complexity to introduce new hardware massively as well as the elevated costs that represents to upgrade the network to its coming evolution, then from the security perspective, it is a challenge to integrate both technologies and guarantee the level of security inside the network. For this research, the security aspects of packet-based networks and LTE are considered to describe mechanisms, threats, and enhancements.

4.1.6.1 Security domains in cellular networks

The 3GPP group split the cellular architecture in several domains to identify the security measures to be applied to the network components. The Figure 22 shows the User Equipment and Infrastructure Domain which are integrated by other subdomains that define the entire architecture. In general terms, the User Equipment Domain is defined by the devices that allow users to access the network, meanwhile the Infrastructure Domain is represented by the devices that complement the radio access network service with other services needed to provide communication.

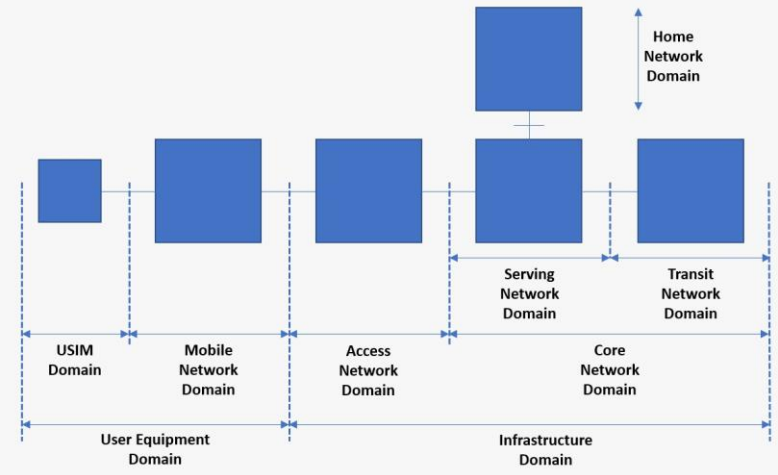

Figure 22. Security domains for cellular networks. Source: TS 23.101

User Equipment Domain

Domain	Function
USIM Domain	It contains the information that provides unique identity to user inside a network. In current networks this information is stored in the SIM card, hence, it is possible to identify the user independently of the terminal is being used.
ME Domain	It performs the transmission of the electromagnetic signals via radio as well as contain applications that are the foundations to establish communications.

Table 12. User Equipment Security Domain. Source: TS 23.101

Infrastructure Domain

Domain	Function
Access Network Domain	It manages the resources that provide access to network as well as external networks or Internet

Table 13. Infrastructure Security Domain. Source: TS 23.101

Domain	Sub Domain	Function
Core Network Domain	Home Network Domain	It performs domestic functions sus as subscription management based on USIM, however it does not take into consideration the physical location of user intending to access the network.
	Serving Network Domain	It is the bridge between the AN and CN. It performs functions of routing, shares user information to peer networks, and provides specific network services to users according to their profile.
	Transit Network Domain	It is in charge of addressing communication out of the network. If the information flows in the same network, then this domain is not activated.

Table 14. Core Network Security Domain. Source: TS 23.101

4.1.6.2 Threats in Cellular Networks.

The following list of threats is specified in [32] as the result of some academic research as well as a compilation of attacks that were address to cellular networks commercially operating.

- **Denial of Service Attack (DoS):** it consists of flooding a target network with traffic until its capacity is overflowed and does not grant access to legitimate users. The packets sent by the attackers are illegitimate request to access the network with invalid network addresses which overwhelms the server when tries to authenticate the attacker. There are four variants of this attack: the Smurf Attack, the SYN flood attack and the UDP flood attack [33].

- **Smurf Attack:** it sends ICMP broadcast packets with a spoofed source address to a given number of devices. These devices will respond to the spoofed address which is meant to be the one of the target systems [33].

- **SYN flood attack:** it occurs when the attacker abuses the 3-way handshake of the TCP protocol. The massive request of connections to different ports, leaves the target system without available ports to grant access to legitimate users [33].

- **UDP Flood Attack:** since UDP packets require less verifications than TCP, this type of attack sends a large quantity of packets to overload the servers or saturate the connections tables.

- **Distributed Denial of Service Attack (DDoS):** it follows the same principle of the DoS attack, but it is conducted by multiple devices that in most of the cases have been infected with a malware that allows attackers to trigger the network flooding increasing exponentially the quantity of requests to the target system. [33]

- **Malware attacks on UE's:** these are the attacks oriented to target the UE's with the purpose of modifying key routines of the operating system that will prevent the devices to access the network.

- **Malware attacks Impacting RAN infrastructure:** this kind of infection affects the firmware or the operating system of the devices, however, this intends to send a very large number of requests to make the base station works in an unexpected or undesirable way. This attack tends to be effective when several UE's are infected and react against a single station.

- **Malware attacks Impacting Core infrastructure:** this attack intends to infect any of the components of the core network to modify the configuration of the entities and create vulnerabilities such as traffic sniffing, user location or billing problems. Additionally, for modern networks such as LTE, it is possible to launch a DoS attack by deploying a malware on several UE's that will send a large number of invalid attach requests that can collapse the operation of the MME.

- **Unauthorized OAM Network Access:** it is referred to the unauthorized access to the management systems that can put the network in operational risk due to misconfigurations or any other malicious activity.

- **Rogue Base Stations:** since UE's tend to attach to the RBS providing the highest power level, the attacker designs and implements a fake cellular station to intercept the traffic generated between the device and an authentic cellular station.

- **Device and Identity Tracking:** now that the devices connected to the cellular networks are identified through the IMSI and IMEI, an attacker who implements a rouge base station can track the specific location of the user by capturing the signaling channels associated to geolocation.

- **Downgrade Attacks:** in this attack, an attacker implements a rouge base station to force the user to downgrade to a less secure technology such as GSM so that it would be easier to break the cryptography algorithms known as A5/1 or A5/2.

- **Preventing Emergency Phone Calls:** in the vein of the rouge stations, an attacker forwards the calls made by the UE's connected to it, then it prevents the subscribers to receive proper and on time assistance from safety services.

- **Unauthenticated REJECT Messages:** during the attach request process, a rouge station can send an unauthenticated ATTACH REJECT message to prevent the users to connect a given base station, which may also be considered as a DoS attack until the UE be rebooted and out of influence of the rouge station.

- **Air Interface Eavesdropping:** it occurs in cases where the operator does not provide encryption to the air interface, then attackers can intercept and store the radio signals which can be decoded according to the technology in operation.

- **Attacks via Compromised Femtocell:** since this kind of cells intends to provide an economical solution to provide cellular coverage in very particular areas, they don't make use of the operators backhaul infrastructure con reach the core network, instead, they make use of the wired Internet connection provided by ISP's which makes the communication vulnerable to be intercepted and decoded when tunneling or encryption is not implemented in this communication channel.

- **Radio Jamming Attacks:** this attack is characteristic for broadcasting high levels of noise in the same frequency the cellular network is operating which generates the lost of signalling and control channels and consequently the access to the network.

- **Backhaul and Core Eavesdropping:** it occurs when network operators do not provide encryption to the connection between the RAN and CN. This communication is susceptible to eavesdropping if an attacker is able to intercept the network equipment that handles the backhaul connection.

- **Physical Attacks on Network Infrastructure:** normally these types of attacks do not have origins in the cyber security premises. It is oriented to steal cooper or some other valuable elements from the station, however, this affects the operation of the RBS and prevent users to get access to the network.

4.1.7 Security in 5G networks

The evolution of cellular networks represents new business opportunities for carriers, then in order to provide an exceptional quality of service, the integration of 5G systems must enhance the protection level for well-known attacks as well as deal with a large quantity of vectors that can emerge from vulnerabilities that may be present in one of the multiple applications for which 5G in meant to be.

The 3GPP group releases in [18] a security architecture for 5G networks to protect the entities by defining network domains which can secure communication between network elements. Moreover, in [20] there are some aspects that were considered to design the technical specifications. This document considers the coexistence with LTE and defines a Non-Standalone approach, introduces the trust model, and implement important enhancements in terms of Primary and Secondary Authentication, Inter-Operator Security, Privacy, Service-Based Architecture approach (SBA), Key hierarchy and Mobility.

4.1.7.1 The Trust Model

The trust model for 5G divides the system in two blocks. The first one contains the UE, while the second one is the entities that integrate the RAN and CN. The UE has two domains which are the UICC that contains the USIM meanwhile the other one is the mobile equipment itself. Moreover, in the network level, the security is considered as decreasing as the information flows towards the core network. [30]

4.1.7.2 Security flow for NSA and SA model

As mentioned previously in 4.1.1.2, the deployments of 5G will go through a transition from an NSA model in where 4G and 5G coexist. Generally, dual-connectivity architectures rely on the existence of one Master Node (MN) and a Secondary Node (SN) to provide the cellular coverage. In this context, MN is in charge of triggering the security aspects to the SN, then when a UE is connected for first time to the NSA system, MN generates the key to secure its communication as well as the keys needed by the SN to perform similar functions [18]. The figure 23 shows the flow to activate encryption and integrity protection in dual-connectivity networks. As shown in [18], it comprises seven steps which will be described below.

1) **RRC Connection Established:** The UN and MN establish connection.
2) **SN Addition / Modification Request:** The MN sends a request to SN to negotiate resources, configuration, and algorithms for the SN. The MN generates the K_{SN} and delivers it to SN as well as the security capabilities of the UE.
3) **Capability negotiation and algorithm selection:** The SN reserve resources for the UE and set ciphering and integrity algorithms. The priority to choose them is given by the common capabilities between the UE and the system. Each time the MN delivers a new K_{SN}, the SN calculates the RRC and UP keys.
4) **SN Addition / Modification Request Acknowledge:** The SN sends an ACK message confirming the allocation of resources and indicating the algorithms chosen for the UE
5) **RRC Connection Reconfiguration (5):** The MN sends a message to the UE to adjust its configuration with the parameters given by the SN. The UE must calculate the K_{SN} to access the SN. Since this message is sent through the air interface, it is integrity protected using the K_{RRCint} of the MN.
6) **RRC Connection Reconfiguration Complete (6):** The UE accepts the message sent by the SN after validating its integrity. Then it will calculate the keys for the SN and inform the MN the RRC configuration is completed. At this point the UE enables the encryption and integrity parameters negotiated previously.
7) **SN Reconfiguration Complete (7):** MN informs the SN that the reconfiguration is completed.
8) **Activation of ciphering and integrity protection:** MN enables ciphering and integrity protection as agreed or when the UE initiates a data transfer.

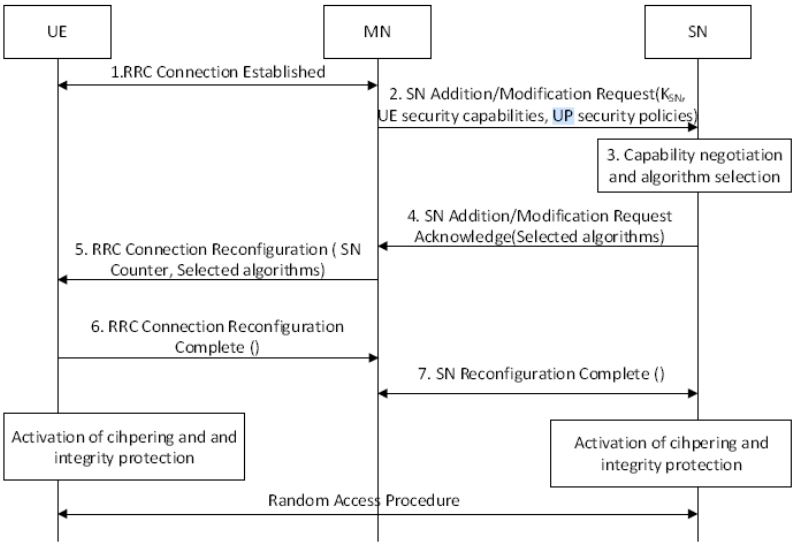

Figure 23. Description of DC procedure to activate encryption and integrity protection. Source: 33.501

4.1.7.3 Subscription Identifier Privacy

This is a global identifier that must be assigned to each 5G subscriber. The SUPI contains an IMSI and a network specific identifier [17]. The SUPI is protected over the air interface through the Subscription Concealed Identifier (SUCI) which is generated by the UE using the public keys that were provisioned in the home network (HN). The 5G system also supports another temporary identifier called 5G GUTI (Global Unique Temporary Identifier) that is used to identify the UE in the network when signalling data is being shared with the CN without revealing the permanent identity of the user.

4.1.7.4 Key Hierarchy

As indicated in TS 33.501, the implementation of 5G systems will support integrity and encryption protection for Access and Non-access stratum using keys of 128 bits but foreseeing to improve the security aspects supporting up to 256 bits in length. As it is seen in the figure below, it exists a derivation scheme that starts in the generation and storage of the private key K which is used to analyze the SUCI and deduct the SUPI.

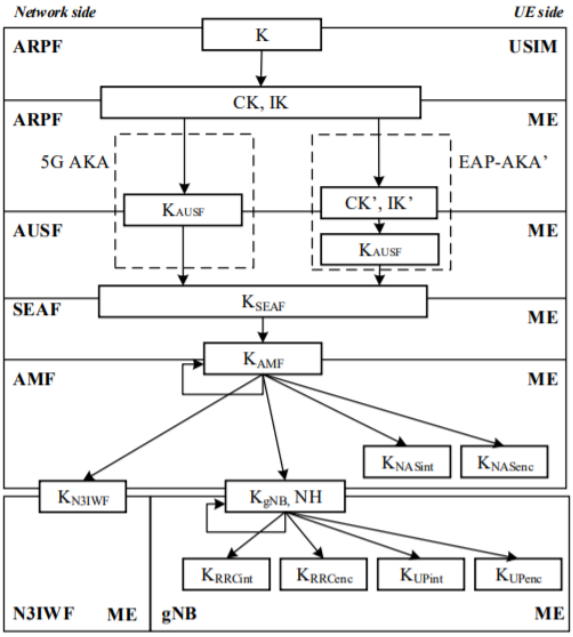

Figure 24. 5G Key Hierarchy. Source: TS 33.501

If EAP-AKA is used as authentication method the AUSF the Kausf is derived from CK', IK', if 5G AKA is implemented, then Kausf is derived from CK' and IK'. Once Kausf is generated and sent to the SEAF, it generates a token which is used by the UE to authenticate the network. If the answer sent by the UE is considered valid, the AUSF generates the Kseaf which is used by the SEAF to derivates the Kamf. To the AMF. From the Kamf, the AMF must derive the Knasint, Knasenc which are the integrity and confidentiality keys, the Kgnb, which is sent to the RBS to derivate the local keys.

4.1.7.5 Security requirements for 5G networks

The TS 33.501 presents the basic guidelines to secure 5G networks implementing specific mechanisms for each network function. The Table X shows the general requirements indicated in 3GPPP standard. Mitigation of bidding down attack pretends to avoid downgrading of security levels between UE and Network Elements by altering the exchange of credentials and forcing the system to adopt the lowest and most vulnerable level of security. Likewise, Authentication and authorization reduce the risk of Man in the middle (MITM) attack by the exchange of keys between UE and serving network that contains the Subscription Permanent Identifier (SUPI) and the serving network identifier. Afterwards, the serving network will query the home network with the SUPI before grant authorization, then connection to the RAN will be provided based on subscriber profile.

Network function	**Requirement**	**Mechanism**
General	Mitigation of bidding down attack	No clearly mentioned.
	Authentication and Authorization	- Subscription authentication - Serving network authentication - UE authorization - Serving network authorization by home network - Access network authorization - Unauthenticated emergency services

Table 15. General requirements to secure 5G networks. Source: TS 33.501

The 3GPPP standard also specified the requirements for the User Equipment (UE). It indicates that terminals must store and secure the permanent Equipment Identifier (PEI) as well as perform activities of ciphering and data integrity.

Network function	Requirement	Mechanism
UE	General	- Ciphering.
	User and signalling data confidentiality	- Ciphering of user data exchanged between UE and gNB. - Ciphering of RRC and NAS-signalling. - Algorithms: NEA0, 128-NEA1, 128-NEA2, 128-NEA3.
	User and signalling data integrity	- Data integrity of user data exchanged between UE and gNB. - Data integrity of RRC and NAS-signalling. - Algorithms: NIA0, 128-NIA1, 128-NIA2, 128-NIA3.
	Storage and processing of subscription credentials	- Subscriber credentials and long-term keys must be duly protected by a tamper resistant hardware. - Credentials and keys cannot be available outside their physical locations. - Algorithms to check subscriber credentials must run within the hardware component.
	Subscriber privacy	- Support 5G-GUTI - SUPI must not be transferred in plain text except routing information. - Home network public key must be stored in USIM - Emergency calls do not require SUPI to be sent

Table 16. User Equipment requirements to secure 5G networks. Source: TS 33.501

Network function	Requirement	Mechanism
gNB	General	Applies to all type of gNB's
	User and signalling data confidentiality	- Activate ciphering of user data as specified in security policies of SMF. - Support ciphering algorithms implemented by UE
	User and signalling data integrity	- Activate integrity protection of user data as specified in security policies of SMF. - Support ciphering algorithms implemented by UE
	gNB setup and configuration	- gNB must grant authentication to perform O&M activities. - Check TS 33.310. - Communication between O&M and gNB must meet TS 33.210 and TS 33.310. - gNB responsible for data authorized data changes.
	Keys management inside the gNB	- Plain text keys must be stored in a secure environment and cannot leave the location for any reason.
	Handling of user data plane	- Plain text keys must be stored in a secure environment and cannot leave the location for any reason.
	Handling of control plane	- Plain text keys must be stored in a secure environment and cannot leave the location for any reason.
	Secure environment of the gNB	- Support secure storage of sensitive data. - Support execution of sensitive functions. - Ensure integrity of secure environment. - Manage access to secure environment.
	Secure gNB F1 interface	- Support confidentiality, integrity and replay protection for all traffic carried over the CU-DU
	Secure gNB E1 interface	- Support confidentiality, integrity and replay protection for all traffic carried over the CU-DU

Table 17. gNB requirements to secure 5G networks. Source: TS 33.501

Network function	Requirement	Mechanism
AMF	Signalling data confidentiality	- Ciphering of NAS-signalling. - Algorithms: NEA0, 128-NEA1, 128-NEA2, 128-NEA3.
	Signalling data integrity	- Integrity protection of NAS-signalling. - Algorithms: NIA-0, 128-NIA1, 128-NIA2, 128-NIA3.
	Subscriber privacy	- Trigger primary authentication using the SUCI. - Assign 5G-GUTI to the UE. - Rellocate 5G-GUTI to the UE. - Confirm SUPI from UE and from home network. Deny service if confirmation fails.

Table 18. AMF requirements to secure 5G networks. Source: TS 33.501

Network function	Requirement	Mechanism
SEAF	General	Support primary authentication using SUCI

Table 19. SEAF requirements to secure 5G networks. Source: TS 33.501

Network function	Requirement	Mechanism
UDM	General	- Store the long-term keys for authentication and security association.
	Subscriber privacy	- Resolve the SUPI from the SUCI.
	AUSF	- Handle authentication request for 3GPPP and non-3GPPP access. - Provide SUPI to VPLMN after authentication confirmation. - Inform UDM about successful and unsuccessful authentication request.

Table 20. UDM requirements to secure 5G networks. Source: TS 33.501

Network function	Requirement	Mechanism
Core Network	Service - Based Architecture	- Provide confidentiality, integrity and replay protection to Discovery, Registration and Authorization functions. - Hide and protect network domains from different trust domains. - Support mutual authentication between NF consumer and NF producer. - Discard messages that do not meet the protocol specifications
	Network Repository Function	- All the requests to the Network Repository Function (NRF) must be mutually authenticated. - Provide authentication and authorization for communication between NF's.
	Network Exposure Function	- Provide integrity, replay and confidentiality protection for communication between NEF and AF. - Support authentication between NEF and AF Authenticate and authorize the AF before interacting with the NF's.
	E2E CN Interconnection	Provide confidentiality and integrity to e2e communications between source and destination networks - Destination network must assess credentials of source networks by implementing a Security Edge Protection Proxy. - Besides, the source and destination network must: - Implement standard security protocols. - Protect roaming interfaces. - Assess performance and overhead. - Prevent replay attacks

		- Implement mechanisms to mitigate bidding down attacks.
	Security Edge Protection Proxy (SEPP)	- Protect control messages sent by two different PLMNs over N32 interface - Authentication and negotiation of cipher suites in roaming mode - Perform key management when cryptographic keys are needed to secure messages over N32 interface. - Hide network topology limiting the visible information to external parties. - Work as a reverse proxy to provide a simple point of access and control to internal FN's. - Discard malformed N32 signaling messages. - Identify certificates sent by either peers or intermediates. - Implement rate-limiting functions to protect itself from excessive signalling. - Implement anti-spoofing mechanisms to enable cross-layer validation of source and destination identifiers.
	N32 interface	- Authentication vectors. - Cryptographic material. - Location data. - SUPI.

Table 21. CN requirements to secure 5G networks. Source: TS 33.501

Network function	**Requirement**	**Mechanism**
Visibility and configurability	Security visibility	- AS, NAS confidentiality. - AS, NAS integrity.
	Security configurability	Grant or deny access to USIM without authentication.

Table 22. Visibility and configurability requirements to secure 5G networks. Source: TS 33.501

4.1.7.6 Security on SDN/NFV

As seen in 4.1.2, the 5G system introduces a new architecture not only in terms of network functions, but also in the sense that the network functions can be integrated in a general purpose cloud-based hardware and built on the top of the stack a series of programmable network tools that eases management and drive orchestration of the entities. The figure below shows how the SDN/NFV redefine the architecture of cellular networks making use of the cloud principles.

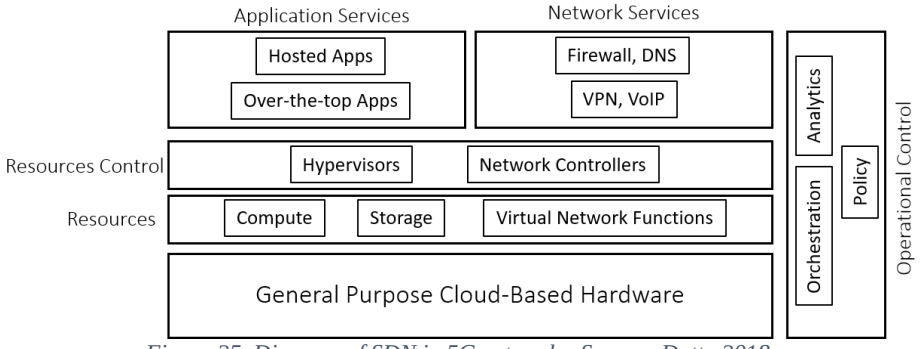

Figure 25. Diagram of SDN in 5G networks. Source: Dutta 2018.

- **Cloud RAN Security:** since the 5G systems make use of the cloud principles, the RAN as seen in 4.1.1.1 is defined not only by air interface, but also by a control and a service plane [34]. For instance, the security approach at this level must deal with the traditional incidents on the physical infrastructure such as Eavesdropping, Jamming, Impersonation attacks as well as the threats related to the control and service plane.

  The security on the control plane deals with IP spoofing, IP hijacking and Smurf attacks. To protect the network, several researchers agree on implementing cognitive radio MAC approach in where the network dynamically assigns available spectrum to users, however, this approach has the drawback that the network needs to implement an additional element to allocate resources securely.

  Another tactic that researchers have proposed to prevent the saturation on the control channel during disruptive attacks such as DoS/DDoS consists of adding a complementary validation of the source MAC addresses to verify the authenticity of the devices generating the malicious behaviour, however this theory relies on the assumption that the attacker is out of the network and ignores that valid UE's may present an inappropriate behaviour due to a massive malware infection [34].

  The introduction of C-RAN opens the opportunity to large network operators to share the radio resources with small service providers. The owner of the infrastructure split the radio resources to provide cellular service under different conditions. This implies that network operators must provide differentiation and Quality of Service to their customers. In this sense, an attacker can sense the spectrum to study how the resources are allocated, then it may be possible to inject malicious traffic in this bands to reduce the bandwidth or generate a DoS attack. Researchers have proposed an algorithm to schedule the resource allocation as the users move across the network and balance the resource allocation according to the density of the cell [34].

  There is another attack on the control plane that is known as Spectrum Sensing Data Falsification attack (SSDF). This malicious activity consists of sensing the spectrum to detect any resource allocation in process and send error messages to disrupt the integration of users to the network. In [35], there is a proposal to make use of analytics to register and classify the trust degree of users according to the past behaviours. Then, sensing and resource allocation is granted in function of the degree of trust that the interacting user has.

  Regarding the user plane, there are documented several threats which are common either for cloud computing systems or traditional cellular networks. In [34] is mentioned that the traditional threats widely discussed over the transport and application layer are still present in the cloud-based systems, moreover, there are threats associated with virtualization, privacy, intrusion prevention.

  In [36], it is recommended to make use of the virtualization technology to protect the C-RAN. Since the BBU is meant to be a centralized unit con remote connection to the RRU, the solution proposed is oriented to implement virtual machine-based intrusion detection, virtual machine-based kernel protection, virtual machine-based access control and virtual machine-based trusted computing. In this way, it is possible to mitigate the common attacks over virtualization

environments such as tampering guest or host machine, virtual machine covert channel, virtual and machine-based rootkits.

In terms of privacy, it is mentioned in [34] that cloud-based systems are particularly insecure due to the fact that users normally share resources which is well used by attackers to leak information and hit victims. In the context of 5G, since resources can be assigned following the characteristics of users, attackers will focus their attention on processes where the identity of the users is exposed in some way. Either in terms of location or identifiers.

Finally, there are concerns related to the programming practices that vendors apply over the development of their hardware. Attackers may get physical access to the hardware deployed in the base stations specifically, the BBU, hack the system, get root privileges and sniff on data in transit that revel the identity of the users or some other type of information [34].

- **SDN Controller Security:** under the scope of the SDN, there is a controller that manages the resource allocation in the network when the infrastructure is share between large carriers and Mobile Virtual Network Operator (MVNO). In the context of 5G networks, The SDN controller support the creation of network slices as required by the users' application. Moreover, it improves the efficiency of the network by classifying the slices according to their characteristics. However, in spite of the benefits of grouping the traffic flows, the network must guarantee the isolation of the different slices in order to avoid impacting the others in case of congestion or disruption [37]. Isolation on the SDN can be accomplished by establishing a set of policies to clearly define the parameters required by each client intending to make use of each slice, for instance, it is possible to define an SLA for each virtualization unit which make possible to provide smooth QoS as demanded by each slice.

  Likewise, the SDN controller represents a centralized unit in where traffic decisions are made. In consequence, it can be targeted by attackers to either gain control of the system or launch DoS/DDoS attacks to disrupt the operation of the network. The isolation discussed before is the first mitigation measure to avoid the interference on the traffic flow, however, it is valuable to implement security applications such as IDS to in the northbound interface to detect any attempt of disturb the operation of the controller.

- **Edge Security:** in the 5G context, the implementation of edge computing allows the system to improve the latency since data can be processed locally, for instance, devices connected to the same cell working in a M2M model can communicate quickly without going through the entire network entities that built the CN. However, the IEEE identified some security challenges in the implementation of this technology [38].

  Initially, one essential concern is that devices can implement mechanisms to send data securely, but it would be hard for the network to reply back with the same level of security. The second one is related to the enormous complexity the network can get as long as it grows. Experts suggests that the service providers will face serious problems to implement privacy policies to the large ecosystem of IoT devices. The third one indicates that as much as the ecosystem grows, the security treats increase in the same proportion, mainly because of flaws on the operating systems.

Now, the approaches to deal with the threats mentioned above go through the enhancement of security on IoT devices. Now they are focus on easing connectivity and power efficiency putting aside the security aspects. Additionally, operators have to implement mechanisms such as perimeter scanning, analytics-based application on edge network elements and self-patching. Another approach that is in the tableau of emerging technologies is called Security Access Service Edge (SASE) in where the network security technologies are applied to WAN network in an aaS context [39].

- **Hypervisor Security:** the implementation of hypervisors in virtualized environments enable the systems to run independently different operating systems while managing underlaying general purpose resources [40]. For instance, NIST [41] , defined a general classification of threats in this context. The first one is related to failures in keeping the isolation of processes. This occurs when there is a compromised VM that has access to memory or storage areas that belong to contiguous VM's, the second one points at the failures in isolating the network elements of VM's. This means that a rouge VM can access unauthorized network information such as MAC and IP address of other VM's which must remain concealed. The third point underlines the issue that the hypervisor as a virtual centralized unit, is target of DoS attacks, then a malicious VM can attack the system by consuming resources that must be shared with contiguous machines in the same hypervisor, for instance, the benign VM will face a DoS.

  The security recommendations for hypervisor deployment from NIST [41] indicates that it is essential to check the integrity of the components to consider them trustable. This is reachable by performing cryptography-based authentication which can be performed by a third-party authority which verifies the identity of initial; components or hardware before creating a chain of trust that starts in the components such as the core kernel, support modules, the management applications and ends in the hypervisor itself. In order to deal with the isolation issues mentioned above, the same document set the following requirements to protect the Hypervisor.

  1) The instructions sent from a guest OS to the main system must be handled in a way that the operation of the hypervisor and the controllers is maintained.
  2) The memory management function must be protected from external attacks such as buffer overflows and external code execution.
  3) Memory and CPU allocation algorithms must guarantee that the queries of resource allocation are effectively done.

- **Container Security:** under this principle, the container-based visualization approach isolates a minimalistic operating system running in the upper layers but does not virtualize the cloud-based hardware resources existing in lower layers. The NIST documentation [42] indicates that major risks on containers are associated to its main technologies such as the images, registries, orchestrators, and host OS. In general, the documentation establishes classifies several types of risks such as Image Risks, Registry Risks, Orchestrator Risks, Container Risks, Host OS Risks

  Since Containers run a partial image of the OS, they tend to be vulnerable due to the lack of support to security updates. Moreover, a non-official image can contain a malware embedded

or can support other protocols on the top which make the container exposed to the threats inherited from the protocol stack.

- **Predictive Analytics:** the implementation of analytics in SDN introduces a catalyst in the adoption of new technologies to improve detection and reaction to network attacks. In this context, the systems that make use of the virtualization can support the implementation of security solutions under the security as a service (SecaaS) paradigm which eases the standardization process and the integration of multiple players in the security ecosystem [43].

  In reference to SecaaS, the SHIELD approach provides integral services for virtualized networks that in the security regard, it collects data and logs to enrich the Intrusion Detection and Prevention System platform where algorithms can predict specific vulnerabilities or attacks. The system captures relevant traffic that defines behaviors and allow system to learn and build preventive measures [43].

  In detail, the SHIELD approach includes data analytics engines which are based on machine learning algorithms such as Naïve Bayes and Support Vector Machine to analyse and classify packets. The algorithms are empowered by processes of data collection such as networking information, IP-MAC addressing mapping, and correlation of unusual traffic patterns. Moreover, the data analytics engine is complemented by the remediation engine that is in charge of issuing recommendations which are shown in the dashboard that reflects alerts and preventive measures [43].

4.2 Machine learning for network security

Since the massive adoption of SDN and NFV technologies, the networks require sophisticated techniques to analyze in real time the statistics that usability generates. Then, Machine Learning Techniques are used to automatize the analysis of the data and adjust dynamically to the needs of the businesses [19]. The introduction of predictive models allows computers to behave like the human brain and not only analyze the data but also make decisions to adjust parameters to the changing environment. However, like humans, machines need training to define correlations between variables and make accurate predictions. At this point, machines are in training stage and need datasets to build a model based on the following algorithms: supervised machine learning, unsupervised machine learning, semi-supervised machine learning and reinforcement machine learning [44].

4.2.1 Supervised Learning

The main objective of this technique consists of labeling data to train the computer and build the prediction model. In [44], the labeled data is defined as a pair (x,y) in where x is an input vector while y is the supervisory signal or output label. In this case, algorithms find the correlation between the label y, its vector x and a new set of data to classify it. The list of supervised machine learning algorithms are as follows: logistic regression, decision trees, decision forests, support vector machines, naïve Bayes, k-nearest neighbors and neural networks [45].

4.2.1.1 Logistic Regression

This model determines the probability that a dataset belongs to a given category. It assumes that variables in vector x are all linear and independent. If the estimated probability is greater than 0.50, then the data can be classified in the given category [44].

4.2.1.2 Decision Trees

This technique is represented by a binary structured tree that establishes a set of decision rules. Each non-leaf node is a decision-making point until reaching the leaf which represents the class or label of the data in analysis [44]. The construction of the decision tree is specified in [45] and comprises the following steps:

1) At the roof of the tree the dataset is split into two binary conditions which define the branches or child subsets.
2) The child subsets are divided granularly into small subsets based on some other conditions.
3) The process of division stops when the new subdivision contains less samples than the minimal number defined previously, or when a branch has reached the maximum predefined depth or when the samples of the branch belong to the same class or are correlated with each other.
4) Finally, the outcome of the process described above is a tree in where a decision is taken at each node and each leaf represents a classification point.

4.2.1.3 Support Vector Machines

This prediction model is used to classify the dataset based on boundaries defined by the training data. SVM are oriented to find the boundaries that establish the maximum separation between classes. This technique is applied in cybersecurity to classify and detect malware attacks as well as to enhance the functionalities of the Intrusion Detection Systems [44].

4.2.1.4 Naïve Bayes

This prediction mechanism is based on Bayes theorem and analyses previous data or events to come out with new predictions. Considering the mathematical principle, the Bayes rule estimates the P(X|Y) from the training dataset where X is a data point and Y is a label. This technique is used when the size of the training dataset is moderate or large and it is assumed that the variables are conditionally independent. This classifier is used in cybersecurity to detect malware, spam, unauthorized access, DoS or DDoS and sentiment analysis.

4.2.1.5 k-Nearest Neighbors

This algorithm allows to classify a dataset by analyzing the similarity between the training data and the dataset. The value of data is classified as the k-nearest neighbor. In network security, the model is widely used to compare the real-time traffic with data collected in intrusion events as well as DoS attacks.

4.2.2 Unsupervised Learning

This technique does not require a training dataset, then the algorithms intend to define the structure of the data, analyzing patterns or classes present in the dataset. This approach assumes that values of data are independent and normally distributed, then the algorithm generates the probability density function to describe association in data. At the end, the unsupervised learning techniques intend to define groups in the data (Clustering) and find the parameters that describe better the data

(Association). The unsupervised learning algorithms are as follows: k-means clustering, hierarchical clustering, factor analysis, apriori algorithm, principal component analysis, singular value decomposition and independent component analysis [44].

4.2.3 Analysis of threats with machine learning

4.2.3.1 Spam Detection

Spam mails have characteristics that can be filtered by machine learning algorithms by analyzing the content of the email messages. Classification techniques such as naïve Bayes or SVM can be used to determine the purpose of the mail. However, the spam detection can also be oriented to analyze some other characteristics of the email such as size, presence of attachment, IP, number of recipients. In this case, SVM, Decision Trees, and Neural Network are widely used [44].

4.2.3.2 Phishing Detection

This threat is oriented to get sensitive information from people who are encouraged to click on or access webpages that sometimes are spoofed or contain malicious payloads that can capture and forward personal information such as passwords, usernames, credit card numbers, etc. Then, as specified in [44], the machine learning algorithms intend to analyze the URL features or domain features or page and content features.

To analyze this treat it is necessary to classify and label data based on real samples of phishing and secure web pages. These samples are used as training data for algorithms under the category of supervised learning such as SVM, Decision Tree, naïve Bayes etc. [44]

4.2.3.3 Malware Detection

This threat is designed to disrupt the operations of computers or systems by tampering the source code or hardware generating undesired behaviours. The malwares documented for machine learning are as follows:

- **Virus:** this malware corrupts or delete data on computers, can reproduce itself and infect other computers without explicit knowledge of users [46]
- **Worm:** this malware causes the same damage as virus but has the particularity of making use the networks to spread itself. [46]
- **Trojan:** it is a computer software that seems to be inoffensive and functional but includes a malicious payload that bypasses the security mechanisms since the program is invoked by the user and works as a legitimate request [46].
- **Adware:** this malware makes use of cookies to constantly shows advertisement on the browser or computer itself [44].
- **Spyware:** this is an unauthorized software installed in information systems to collect information of the organization and individuals without their knowledge [46].
- **Rootkit:** it is a set of files installed in on a computer that allows an attacker to gain administrative privileges on the system.
- **Backdoor:** it is a vulnerability that allows attacker to gain access to computer systems [46].
- **Keylogger:** this captures the combination of keys pressed by users when they type sensitive information [44].
- **Ransomware:** it gains control on the computers to encrypt all the data or lock the access until victim pays some money to attackers [44].

The machine learning algorithms use static analysis which is based on the intrinsic characteristics of the data to figure out the trustability of the program, however, there is a dynamic analysis that takes into consideration the runtime features of the program such as calls, CPU-Memory usage, call frequencies, etc. There are multiple algorithms to detect malwares, however, for dynamic analysis, decision trees, logistic regression, naive Bayes, artificial neuronal networks and SVM are widely used [44].

4.2.3.4 DoS and DDoS Attack Detection

As discussed before, a DoS attack exhausts the computational resources of the target systems by sending a large number of malicious packets to block the attempts of legitimate users to access the network. The mechanisms to detect and mitigate the DoS are based on Intrusion Detection Techniques (IDS) such as signature-based intrusion detection and anomaly-based intrusion detection [44]. The signature-based systems rely on known patters to predict or detect attacks, while anomaly-based implementations use statistics and metrics to detect unusual behaviors.

Machine learning techniques to detect DoS attacks can be SVM, naïve Bayes, k-means, but algorithms must analyze the number of bytes transferred from source to destination, number of connections to a host, source and destination IP addresses, byte rate, packet rate, TCP flags ratios, SYN packet statistics, SYN flag presence, classification fields and protocol fields, destination port, entropy, entropy of source port, UDP protocol occurrence and packet volume [44].

4.2.3.5 Anomaly Detection

Machine learning techniques rely on hybrid approaches to determine anomalies with high accuracy since there are cases that are not attacks but they are just representing a new behavior. Implementing k-means and decision trees stand for classification, of anomalies and normal activities. ANN and SVM are well-known in detecting U2R and U2L attacks. Basically, these cases indicate that once models are available, it worth to test them in the cyberattack landscape and assess their efficiency in combination with the existing and tested machine learning mechanisms [44].

4.2.3.6 Software Vulnerabilities

Machine learning techniques are used to detect weaknesses in software systems or applications. Attackers can take advantage of poor programming techniques to launch a code injection attack and run malicious code with exceptional privileges over the abuse program. Hence, these techniques analyze the syntax and semantics of the code as well as try to find patterns to support coding auditing. Then, the anomaly detection methods such as k-nearest neighbors are used to classify events such as API usage patterns, lack of input validation, lack of access control, etc. while algorithms such as logistic regression, random forests and neural networks are widely used to recognize patterns in defense programming [44].

CHAPTER 5

ANALYSIS AND DISCUSSION

This chapter studies the security aspects of the 5G technology as result of the analysis of the system, protocol stack, service requirements, security architecture and communication flows specified in the theoretical background. The research also considers the outcome from other researchers who have studied the application of machine learning in the cyber security context.

5.1 Security Landscape

As it can be seen in 4.1.1, the 5G system architecture makes use of the NFV (Network Function Virtualization) to split the inherit functions of the system in logical or physical entities, which in turn introduces the principles of SDN (Software-Defined Networks) separating the User and Control Plane in the centralized network elements such as gNB, AMF and UPF. The definition of a cellular system based on the principles mentioned before led this research to study the UE, the network infrastructure represented by the RAN and CN, as well as the protocol stack.

5.1.1 Attacks against the User Equipment

UE's are going to represent the largest number of network entities in the 5G ecosystem. These devices must fulfill the technical specifications required by the cellular network to have access to the network, however, the billion of gadgets connected will broaden the spectrum of operating systems (OS) that serve the UE's.

IEEE agreed in [47] that the devices that will integrate the 5G ecosystem are highly diverse. There will be a large quantity of powerful smartphones, but also a vast number of IoT gadgets with limited processing and storage capabilities. The last ones are considered the most vulnerable to malware attacks as well as the most difficult to retrieve data from in case an analysis of intrusion detection is needed. The quantity of vulnerabilities found in the most dominant operating systems totalized 9079 until 2019, however, the following chart summarizes the most critical ones.

Attack	Description
DoS	Vulnerabilities lead to Denial of Service due to local resource exhaustion, crash of internal services that black access to network, creation of internal loops or disable of security features.
Code Execution	These flaws enable remote code execution that may cause unexpected behaviours or facilitate the attacker to get additional execution privileges.
Buffer Overflow	This type of vulnerability generates a simple crash on the operating system or derivate on more complex disruptions such as DoS attacks, or memory overwriting.
Memory Corruption	These vulnerabilities allow attackers to execute remotely a malicious payload, overwrite memory allocators or modify data pointers to read unauthorized memory allocations.
SQL Injection	It exploits improper data manipulation on the OS to query information stored locally such as the list of SMS messages.
Bypass	It allows attackers to bypass permission checks and get access to authentication data, user location, or execute an unauthorize code.

Table 23. List of documented attacks on UE. Source: CVE

Besides the flaws mentioned before, the company JSOF in collaboration with Treck disclosed in August 2020 a set of 19 vulnerabilities [48], that affect the TCP/IP library developed by Treck for its multiple clients. As indicated in [49], there are four vulnerabilities that are considered as critical because they allow attackers to get remote access to the target devices and run malicious code. There are other 15 flaws with different degrees of criticality, however, most of them lead to improper handling of malicious packets. The next table shows the description of the vulnerabilities documented by the CVE.

CVE ID	Vulnerability Score	Impact
CVE-2020-11896	10	Devices may enable remote code execution due to improper input validation
CVE-2020-11897	10	Malformed IPv6 packets can generate a buffer overflow or edit unauthorized memory allocations.
CVE-2020-11898	9.1	Devices running the Treck TCP/IP stack improper handle the length parameter in IPv4/ICMP packets. The attackers can play with the length of the ICMP Echo request to receive a response that contains additional information stored in buffer.
CVE-2020-11901	9	Devices may enable remote code execution due to an improper validation with a single invalid DNS response.
CVE-2020-11900	8.2	Devices running the TCP/IP stack improperly handles the ICMPv4 length parameters which leads to information leak.
CVE-2020-11902	7.3	Encapsulation of IPv6 packets within IPv4 headers allow attackers to read unauthorized memory areas.
CVE-2020-11904	5.6	Devices running the Treck TCP/IP stack can suffer an integer overflow during the memory allocation process which enables edition over unauthorized memory spaces.
CVE-2020-11899	5.4	Devices working in IPv6 mode may perform an improper input validation when packets are sent by an external entity which may lead to a DoS attack.
CVE-2020-11903	5.3	Devices running the TCP/IP stack are vulnerable to attacks that intents to read the memory stack. Due to improper input validation, the attacker can get access to the DHCP component.
CVE-2020-11905	5.3	Devices running the TCP/IP stack are vulnerable to attacks that intents to read the memory stack. Due to improper input validation, the attacker can get access to the DHCPv6 component.
CVE-2020-11906	5	Devices running the TCP/IP stack are vulnerable to attacks that intents to hit the Ethernet Link Layer. If the malicious activity is successful, the attack may cause an integer underflow and allocate information in wrong memory spaces.
CVE-2020-11907	5	Devices running the TCP/IP stack improper handle the length parameter of the TCP packets. This leads to generate Integer overflow.
CVE-2020-11909	3.7	Devices running the TCP/IP stack improper handle the length parameter of the IPv4 packets. This leads to generate Integer overflow.
CVE-2020-11910	3.7	Devices running the Treck TCP/IP stack improper handle the length parameter in IPv4/ICMP packets. This leads to overwrite contiguos memory allocation.
CVE-2020-11911	3.7	Devices running the Treck TCP/IP stack improper handle the length parameter in IPv4/ICMP packets. This leads to incorrect permission assignment for critical resource.
CVE-2020-11912	3.7	Devices running the TCP/IP stack improper handle the length parameter of the TCP packets. This leads to overwrite contiguous memory allocation.
CVE-2020-11913	3.7	Devices running the TCP/IP stack improper handle the IPv6 packet which may lead to read contiguous memory allocation.
CVE-2020-11914	3.1	Devices running the TCP/IP stack improper handle the ARP frame which may lead to read contiguous memory allocation.
CVE-2020-11908	3.1	Devices running the TCP/IP stack improper handle the Null termination in DHCP. This may lead to exposure of sensitive information.

Table 24. Description of Ripple20 vulnerabilities. Source: National Vulnerability Database (2021)

The disclosure of the Ripple20 set, represents an important threat for the devices that make up the IoT ecosystem since problems are not going to be exclusive for mobile devices running OS1 or OS2, but these weaknesses are going to be present in billions of devices across 12 sectors.

5.1.2 Attacks against the RAN

One of the most concerning issues for operators is the fact that 5G networks have to coexist with legacy networks, especially with 4G. This means that the vulnerabilities existing in this technology will remain there while the 5G network is fully deployed in terms of RAN and CN. Previously, the privacy issues were studied in [50]. That research identified eleven type of attacks that would disclose the identity or location of the user as well as tracking the UE of the victim all over the network. The table 20 summarizes the risks present in 4G networks in terms of privacy exposure which are described below [50].

- **IMSI-Catching:** an active attacker sends authentication requests to devices located in a given area. 4G networks sends the IMSI/GUTI to initiate the attachment, while the secure channel is established, there are cases in where the network is not able to resolve the temporary identifier, then the attacker capture the traffic on the air interface and break the encryption applying IMSI-Cracking attack [50].

- **IMSI-Probing:** once the attacker knows the IMSI of the victim, he/she can send multiple queries in a given area to determine is the victim is present in the same area the attacker in polling [50].

- **IMEI Request:** it is valid for 2G/3G networks, but 5G devices operating in poor performance environment can downgrade the operating technology and receive unauthorized IMEI requests and reply successfully with the information [50].

- **GUTI Persistence:** either 4G or 5G specifications indicate that the temporary identifiers should be refreshed when certain network activities are performed. However, there are evidences that network operators have implemented poor practices in this aspect in order to avoid signalling storms, then attackers can track users more easily during longer periods of time [50].

- **C-RNTI based tracking:** when a new user is joining a cell, the RBS assigns a layer 1 temporary identifier called Cell Random Network Temporary Identifier. Several traffic analyses have shown that this parameter is sent unencrypted to the air interface in every single packet. Hence, an attacker may be able to track a victim in this level, even more, during the handover process, this random parameter can be linked to the new one that receiving cell will generate, then traceability is possible across the network [50].
- **GUTI Relocation Replay Attack:** this attack targets a vulnerability on 4G networks that consist of abusing an unfinished handshake when GUTI is being refreshed. Since the GUTI_Reallocation command does not include an automatic replay mechanism, the network is able to register the new temporary identifier, but the UE can continue operating with the old parameters as long as an ACK is sent by the UE [50].

- **ToRPEDO Attack:** it consists of triggering a serie of paging events such as calls in very short time, the RBS would update the GUTI very often as well. In consequence, the attacker would be able to deduct the last 7 digits of victim's IMSI. Since IMSI is a 15 digits number, the computationally challenge to deduct the other numbers is less significant [50].

- **Linkability of AKA Failure Messages:** it takes advantage of the fact that the attacker manages to capture the failure messages in case of an errors occurs during the authentication challenge. To conduct this malicious activity, the attacker registers the first authentication challenge exchanged between the network and the UE. Later, to do traceability of the user, the attacker polls the network by sending the authentication challenge to the network and analyses the answer. If it gets "MAC_failure", it means that the user is not longer in the cell but if the answer is "Sync_Failure", it means the victim is the area under observation [50].

Attack	Type		
	Identity Disclosure	Location Leak	User Traceability
IMSI-catching	X	X	X
IMSI-probing		X	X
Unauthenticated IMEI Request	X	X	X
GUTI Persistence		X	X
C-RNTI based tracking		X	X
GUTI reallocation replay			X
ToRPEDO	X	X	X
AKA Protocol Linkability			X

Table 25. Source: Summary of documented attacks on RAN. Khan, Martin (2020)

The security requirements mentioned in 4.1.9.8 can be considered as technology enhancements oriented to provide confidentiality and integrity to the end-to-end communication established by the subscriber. In the same vein, the 3GPP group designed several improvements which partially fixed the vulnerabilities associated to the list of attacks mentioned before. There are attacks present in the 4G RAN that are also inherited by the stand-alone model of the 5G architecture such as IMSI-probing, C-RNTI-based tracking, AKA Protocol Linkability. [50]

In the same vein of temporary identifiers, there is significant difference between 4G and 5G, hence the NSA and SA models. Networks operating in 4G initiates the registration process by sending an Attach Request that includes the IMSI/GUTI in an encrypted format, while the 5G network introduces the SUPI and SUCI which are temporary identifiers. The first one is generated on the UE and is equivalent to IMSI but the second one represents a concealed identifier that encrypts SUPI using ECIES algorithm and the public key of the home network. Certainly, this represents an improvement in terms of privacy for SA deployments, however, the implementation of 5G through the NSA model is still a problem in this aspect.

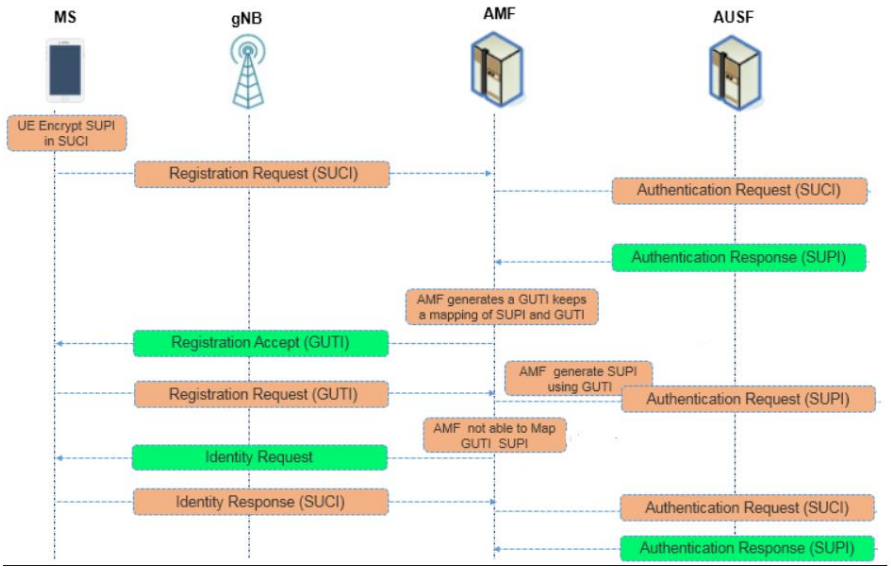

Figure 26. 5G SUPI and SUCI flow exchange. Source: TS 23.501

Additional weaknesses that can be exploited in 5G networks as well as in the NSA model is the lack of encryption during the pre-authentication stage. In 4G networks, attackers exploit the exposure of capabilities of UE, RAN and CN [51], while in 5G the registration request message is sent without integrity and encryption protection when there is not NAS security context [52]. In both technologies this flaw is used to launch bidding down attacks.

Particularly in the case of 4G/5G, the RAN functionalities are concentrated in the eNB/gNB, this network entity can be attacked either in the radio interface, or the interfaces N3 and N2 towards the UPF or AMF in the case of 5G. The attacks on the air interface exploit the vulnerabilities of wireless communications, while the weaknesses in the protocol stack can be used to gain control of the system, especially when there are hybrid architectures like the NSA model.

Another attack that can be conducted in the air interface for most of the cellular networks is called jamming attack. In [53], it is mentioned that this malicious activity can be launched by transmitting amplified noise in the same frequency band that the gNB is operating. It will interfere the messages to be sent to CP and UP, generating a local DoS attack.

5.1.3 Attacks against the core network

In 5G networks, communication from RAN to CN circulates through the N2 and N3 interfaces towards the AMF and UPF, respectively. These two network entities are designed to be agnostic in L1 and L2, however, they both implement the IP protocol in L3 and a couple of variants for upper layer protocols. AMF implements Stream Control Transmission Protocol (SCTP) and Next Generation Application Protocol (NG-AP) while UPF employs User Datagram Protocol (UDP) and GPRS Tunnelling Protocol (GTP-U). The next figures show the comparison of the protocol stack for each interface.

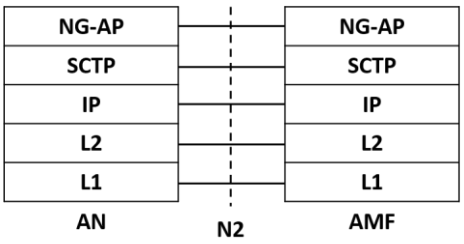

Figure 27. AN-AMF protocol stack

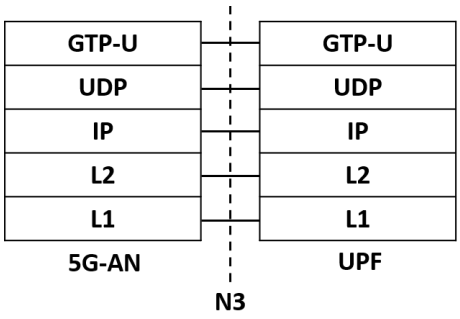

Figure 28. AN-UPF protocol stack

The implementation of SCTP protocol in the transport layer intended to improve the operation of peer protocols such as UDP and TCP. Even some vulnerabilities that led to amplification attacks were exposed in [54], these weaknesses were fixed in [55]. Even this release made the protocol more robust in terms of memory administration, there are other critical points that can be exploited through a DoS attack such as INIT Flooding, Long INIT Flooding, Real Cookie Flooding, and Fake Cookie Flooding. The description as follows.

- **INIT Flooding:** this attack is oriented to overwhelm the computational capacity of the systems by sending a large number of initiation packets (INIT) as attempts to begin association between hosts. The system under attack collapses when the quantity of cookies to calculate saturate the processing capacity [56]. In the context of 5G networks, this attack can be launched to gNB's or AMF.

- **Long INIT Flooding:** this attack exploits the multi-homing capability to support multiple IP addresses that leads to a different sub-nets and network paths. The attack consists of sending a very large list of client IP addresses that should be registered in a given endpoint. When the quantity of malicious INIT messages is large, the processing capacity overwhelms due to the calculation of cookies and IP addresses registration [56]. This attack can be launched in a 5G network by sending the corrupted INIT packet to gNB or AMF.

- **Real Cookie Flooding:** this attack needs a large number of devices to send a legitim INIT message to the endpoint. Then, the server has to calculate the cookie to each of them and reply back. Once the zombies receive the cookie, they send a large number of COOKIE/ECHO messages to make server to believe that the 4-way handshake procedure is lost, so the attacked machine restarts the association process with its peers [56]. This attack seems to be unlikely to occur in a 5G network since the zombies machines have to send the INIT message from real

IP addresses in order to get validated cookie [56]. Since the family of IP addresses configured for the N2 interface should be relatively small, this fact leaves the attacker with few options to connect the zombies' machine.

- **Fake Cookie Flooding:** similar to the Real Cookie Attack, the attacker sends a large number of COOKIE/ECHO messages to overwhelm the processing capacity of the endpoint, however, since the COOKIE/ECHO does not contain a valid IP address, the message will be discarded. The attack can be materialized if the aggressor recruits multiple zombies' machine with fake IP address, configured to send the malicious message [56].

Now, analyzing the communication protocols for the user plane, it is shown in the protocol stack that GTP over UDP is used for the transport layer. This protocol is not only used in 5G networks, but also it was implemented in 4G networks to support data services over the air interface. Since the early implementation of 5G networks goes through the transition from the NSA architecture until reaching a complete deployment of the technology presented in the SA model, the vulnerabilities associated to the GTP protocol present in 4G can also be replicated to the 5G network design. The descriptions of the GTP flaws are described below:

- **Confidentiality:** since GTP protocol does not specify encryption for communication between peers, an eavesdropping attack can get access to sensitive information in transit [57]. An attacker can force a 5G UE to downgrade its operation to 4G during the registration process to capture the IMSI that will be sent to the CP of the CN using the GTP-C protocol. Or in 5G, some other sensitive information that can be sent to the UPF using the GTP-U protocol.

- **Integrity protection:** the TS 29.281 [58] does not include any consideration in terms of integrity protection. Then, an attacker can tamper signalling messages or unencrypted data sent to the UPF. Moreover, the attacker can also generate malformed GTP packets with the purpose of detecting flaws on the systems that will lead to buffer overflow due to poor exception handling [57].

- **Sender authentication:** as indicated in [57] GTP protocol does not implement mechanisms to verify the identity of the senders, then an attacker can make use of a spoofed IP address to send corrupted information to the UPF that can cause service disruptions as DDoS attacks.

- **Leak of Network Information:** For topologies using the 4G CN, there are evidences that some systems exposed their IP addresses when a network scanning attack was launch against the network entities. The attack exploited the lack of sender authentication to send echo request messages which were successfully answered by the entities.

5.2 Artificial Intelligence in Denial-of-Service attack detection

The literature review suggests that the Denial-of-Service attack can be detected by implementing a machine learning classifier to analyze the traffic signatures generated by either regular traffic or DoS attack. By contrast, the clustering techniques tend to be less efficient for cybersecurity tasks since they increase the technical complexity of the implementation and provide similar results. In [44], it is extended that clustering algorithms perform better when they work with numerical data.

There are significative contributions about the criteria to choose the proper algorithm to detect DoS attacks. In [45], it is considered, the computational and mathematical complexity, as the main factors to consider across the implementation, while [59] analyzes the inherent characteristics of the supervised algorithms in the DoS context. However, in [60] there is a comprehensive framework that explains the general characteristics of the algorithms. The following table shows the summary for each of these techniques.

Algorithm	Accuracy	Training Time	Linearity
Logistic Regression	Good	Fast	Yes
Support Vector Machine	Good	Fast	Yes
Gaussian Naïve Bayes	Good	Moderate	Yes
k-NN	Excellent	Moderate	No
Decision Tree	Excellent	Moderate	No

Table 26. Preliminary assessment of ML algorithm. Source:

5.3 Model Definition

After studying the network architecture shown in 4.1.1. as well as the communication flow during the attachment procedure, this research concentrated its attention on the message flow that circulates over the S1 interface for the EN-DC model and the N3 in the SA model. Legacy implementations made use of the GTP protocol, however, in spite of the multiple flaws mentioned before, the protocol is still present in the newest architecture.

5.3.1 GTP protocol on the S1 interface

The implementation of the Multi-RAT DC with EPC implies that the eNB, working as a Master Node (MN), is in charge of handling the initial interactions with the non-access stratum, while the gNB, working as secondary node (SN), has to the process the uplink/downlink data generated between the UE and PGW.

5.3.2 GTP protocol on the N3 interface

The technical specification TS 29.281 [58] explains the treatment of data for the different messages that circulate between the gNB and UPF. The documentation indicates that gNB and UPF can share GTPv1-U packets that transport the T-PDU data, but also peers must monitor and maintain communication by sending Echo Request/Echo Response messages between them.

The first set of GTPv1-U messages is encapsulated data that is generated by UE's and send it to Internet through the CN entities. The messages associated with signalling support entities to verify the status of the path in a similar way as traditional networking devices test the availability of peers sending ICMP ECHO_REQUEST. The management messages help entities to inform its peers that it received a malformed packet either for problems in the communication process or malicious activities.

5.3.3 Protocol attack definition

As mentioned before, this research intends to study the behavior of the DoS attack on the different implementations of the 5G network. The definition of this attack as indicated in 4.1.8.2 falls short of depth to cover the diversity of scenarios that lead to a disruptive attack. The description given

by Canadian Institute for Cybersecurity [61], enlarge the pool of protocols that can be involved in a DoS attack, hence more scenarios can be studied. The figure shows protocols considered by CIC. Since this research studies the GTP protocol, which is UDP based, the UDP exploitation attacks are going to be considered for the experimental phase.

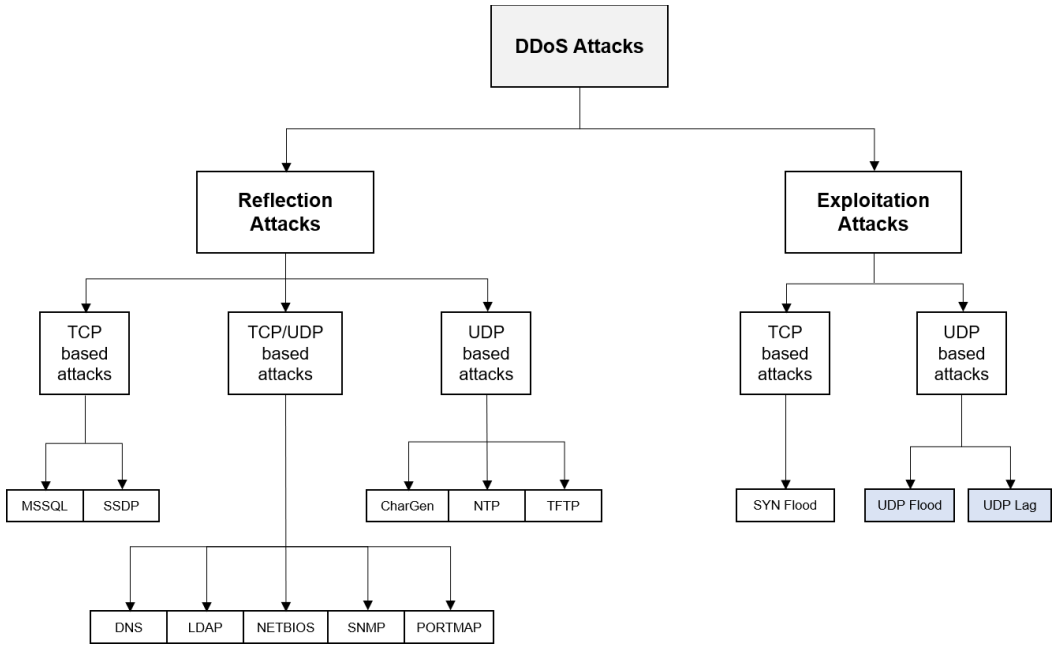

Figure 29. Definition of DoS attack according to the Canadian Institute for Cybersecurity. Source: CIC (2019)

- **UDP Flood:** this attack sends large quantity of packets at very high rate to the target machine. As a result, the network capabilities as well as the system performance get exhausted and unavailable to accept new connections.

- **UDP-Lag:** this attack also floods the network sending a large quantity of UDP packets with the purpose of consuming bandwidth and reduce the performance of the entire network. In general, this attack is launch against networks.

5.3.4 Data Set Definition

In order to assess the performance of the machine learning algorithms in the DoS attack context, the dataset extracted from the Canadian Institute for Cybersecurity contains 3 signatures such as UDP-Lag, WebDoS, DrDoS and one set of Benign data. The file was downloaded in .CSV and included 1032445 registries that were generated in a timeframe of 52 min, 13 seconds. The distribution of labels is described in Table 27.

Label	# of packets
UDP DrDoS	660242
UDP-Lag	366461
Benign	4772
WebDoS	439
Total	1031914

Table 27. Packet distribution in CICDDoS2019

The attacks mentioned previously were generated in a non-tunneled environment, in consequence the samples were adjusted to the technical specifications of the GTPv1 protocol as specified in [58], in order to make the dataset suitable for the 5G context. The TS 29.281 also indicates that GTP peers must generate path management traffic in intervals of at least 60 seconds, then control data must be generated and added to the dataset.

From the dataset can also be deducted that the attack is launched from one IP address that hits a network with 4 active and benign elements. This distribution led this research to define an experimental topology that comprises the same quantity of benign elements plus one malign entity that generated the different labels of DoS attack. The figure below shows the architecture in analogy to the dataset chosen.

The tunneling provided by the GTPv1 protocol in 5G network defines that peers must set the Source Port and Destination Port as 2152, hence all benign and control traffic must meet these specifications while the malign traffic must keep the destination port as 2152. As a result, 530 packets were added to the dataset with the label of Control. The total distribution of data throughout the timeframe is illustrate in Figure 30.

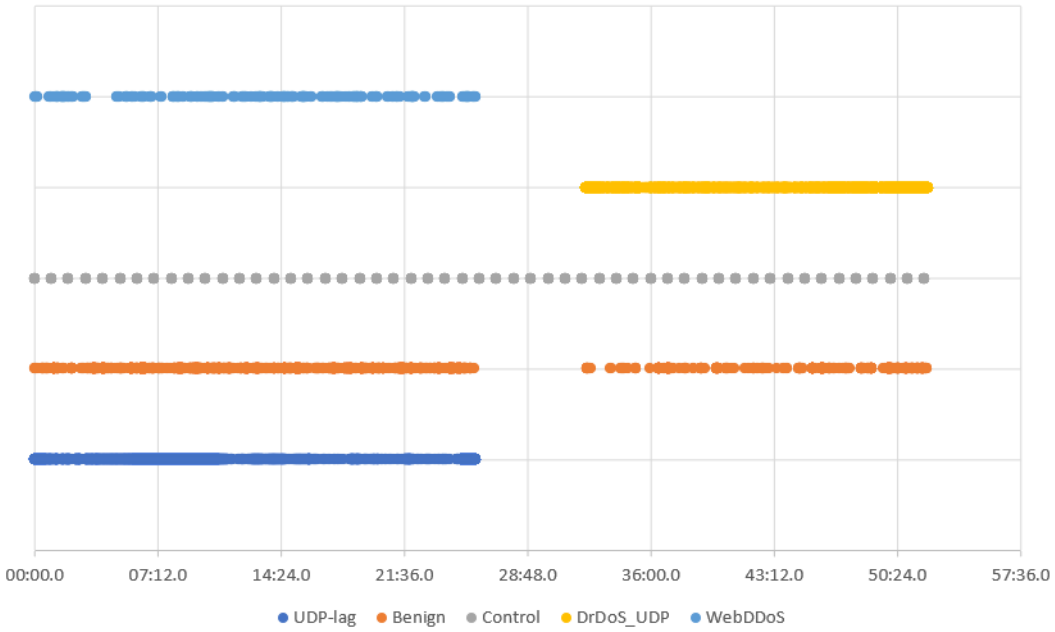

Figure 30. Packet distribution across the capture.

One of the main characteristics of the flooding attacks is that they saturate the network resources by sending large a quantity of packets within a specific timeframe. Then the timestamp is used to understand the behaviour of traffic throughout the test. Even the dataset includes some other parameters, this research considers studying the fields of the outer GTP packet such as Source IP, Source Port, Destination IP, Destination Port, Protocol and Packet Size. The inner GTP packet as well as its payload may be interested to analyze in order to detect some other anomalies in the traffic flow, however, it would be out of discussion in this research since the DoS attacks under

study are protocol-based volumetric attacks. The next figure shows the packet structure of the GTP-Uv1 packet.

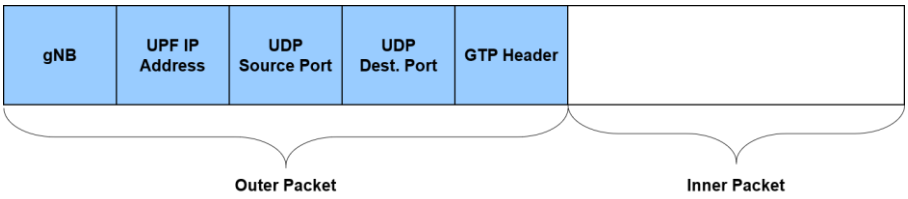

Figure 31. Structure of the GTP-Uv1 packet. Source:

From the following figures it possible to deduct the shape of the samples included in the dataset. Some researchers indicated that malign packets may had a small size since they are easier to send over the wire and challenge the network and computational resources by adding more headers to process in a time unit. However, the representation of the patterns below shows similarities in size between benign and malign data throughout the packet capture.

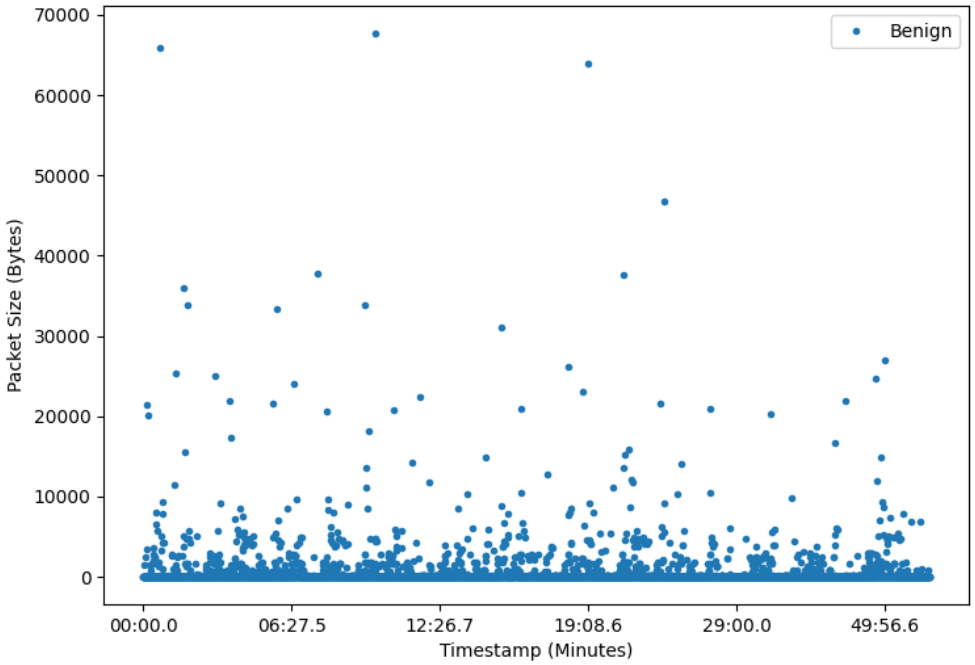

Figure 32. Packet Size vs Timestamp - Benign

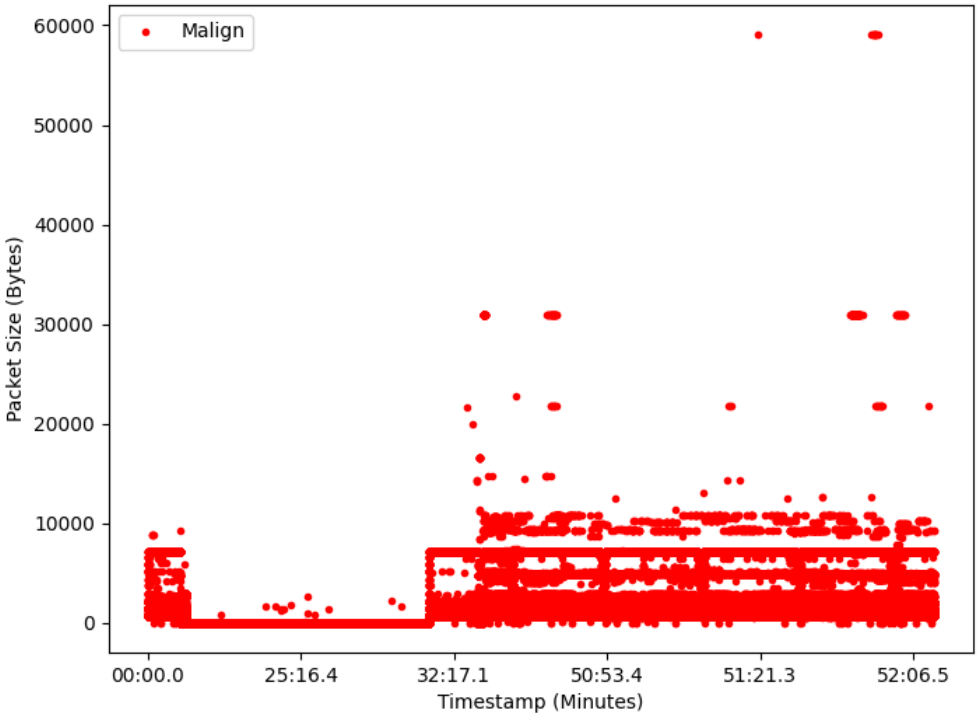

Figure 33. Packet Size vs Timestamp - Malign

On the other hand, when the analysis is conducted in function of source ports, the characteristics of the GTP protocol led to classify the benign traffic as any packet that has Source Port and Destination Port as 2152. The rest of the traffic can be considered as malign, even though there are cases in where traffic is sent from well known and ports such as 80.

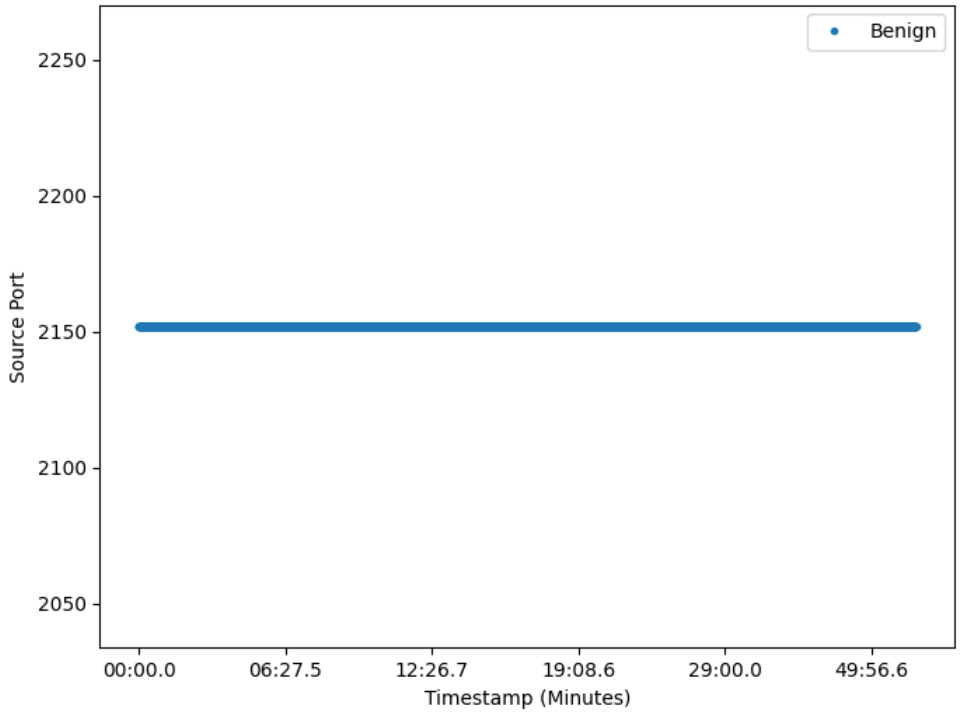

Figure 34. Source Port vs Timestamp - Benign

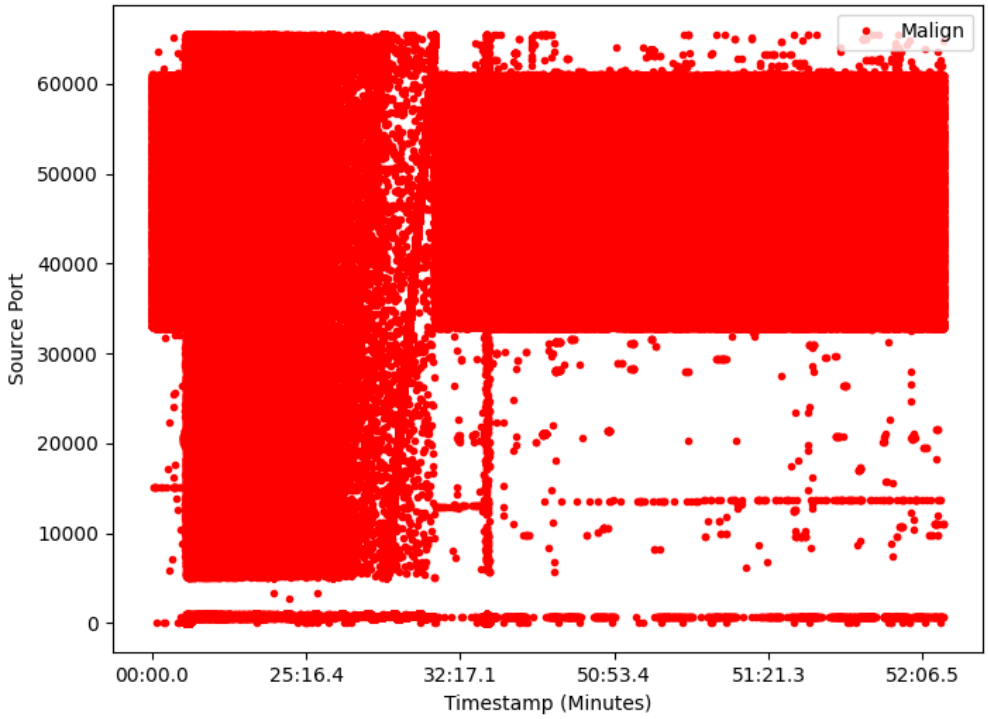

Figure 35. Source Port vs Timestamp - Malign

5.4 Testing

The environment that is represented in the dataset is illustrated in the next figure. As mentioned before, the evaluation of ML algorithms is based on several assumptions that simulate the architecture to test. The first assumption is that the attacker has already gained access to the CN, then it pretends to be a rouge base station with physical access to the N3 interface that connect to the UPF. In addition, there are four gNB's exchanging benign traffic into the network.

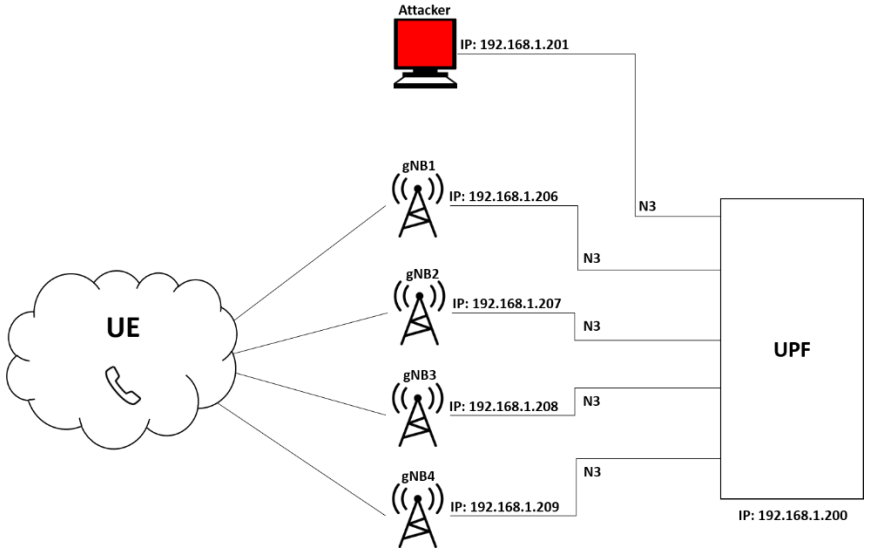

Figure 36. Network environment for data generation. Source: CIC

Traffic	Src IP	Src Port	Dest IP	Dest Port	Protocol	Packet Size
UDP-Lag	192.168.1.201	Variable	192.168.1.200	2152	UDP	Variable
UDP DrDoS	192.168.1.201					
WebDoS	192.168.1.201					
Control	192.168.1.201	2152			GTP	50 bytes
Benign	192.168.1.206	2152	192.168.1.200	2152	UDP	Variable
Control	192.168.1.206				GTP	50 bytes
Benign	192.168.1.207	2152	192.168.1.200	2152	UDP	Variable
Control	192.168.1.207				GTP	50 bytes
Benign	192.168.1.208	2152	192.168.1.200	2152	UDP	Variable
Control	192.168.1.208				GTP	50 bytes
Benign	192.168.1.209	2152	192.168.1.200	2152	UDP	Variable
Control	192.168.1.209				GTP	50 bytes

Table 28. Network parameters considered in dataset CICDDoS2019.

As suggested in the literature review, the best technique to detect DDoS attacks is the classification approach as mentioned in 4.2.1. Hence, the ML techniques to assess are Logistic Regression, Support Vector Machine, Naïve Bayes, K-Nearest Neighbor, and Decision Tree. Since the UPF is the network entity to be flooded, the classifiers must be implemented in the centralized unit. If an attack is detected, the UPF can block the IP address and raise a flag to the other network entities such as AMF to disconnect the elements associated to malicious activities.

The machine learning algorithms are implemented in Python3.8 making use of the set of features included in scikit-learn library. Previously, the datasets were manipulated using pandas library for data analysis. The scatters were created by making use of the matplotlib library which is specific for Python programming language.

5.5 Performance of algorithms

In order to assess the performance of the machine learning algorithms, this research relies on the classification metrics published in [62]. The evaluation starts with the plotting of the Confusion Matrix and continues with of metrics commonly used such as Accuracy, Precision, Recall, and F1 score.

- **Confusion Matrix:** is the graphical representation of how the ML algorithm performs the classification. The matrix shows how many samples were classified correctly by plotting diagonally the combination of True vs Predicted labels. In the case of multi-class classification, the rows illustrate the value of the predicted labels while the columns represent the value of the true labels.
- **Accuracy:** in general terms represent the percentage of correct predictions. In the case of multi-class studies, it represents the average number of correct predictions.
- **Precision:** shows the ability of the classifier to choose the right labels across the different classes
- **Recall:** shows the ability of the classifier to find the right labels across the different classes
- **f1-Score:** represents the harmonic mean of recall and precision. It is used to assess the results in unbalanced datasets.

5.5.1 Logistic Regression

The distribution shown in the following confusion matrix represents the predictions made by the algorithm when it processes the dataset mentioned previously in this chapter. The results show high precision for dominant classes such as DrDoS_UDP and UDP-lag, however the regression shows a very poor performance when the quantity of packets in a given class is very low. For Control and WebDDoS classes the predictor could not classify any packet correctly, this is consistent with the classification report presented below which shows 0% of precision for Control and WebDDoS and 10% for Benign label. The accuracy of the model is 99,0513% mainly influenced by the large quantity of data of DrDoS_UDP and UDP_lag classes that was classified correctly.

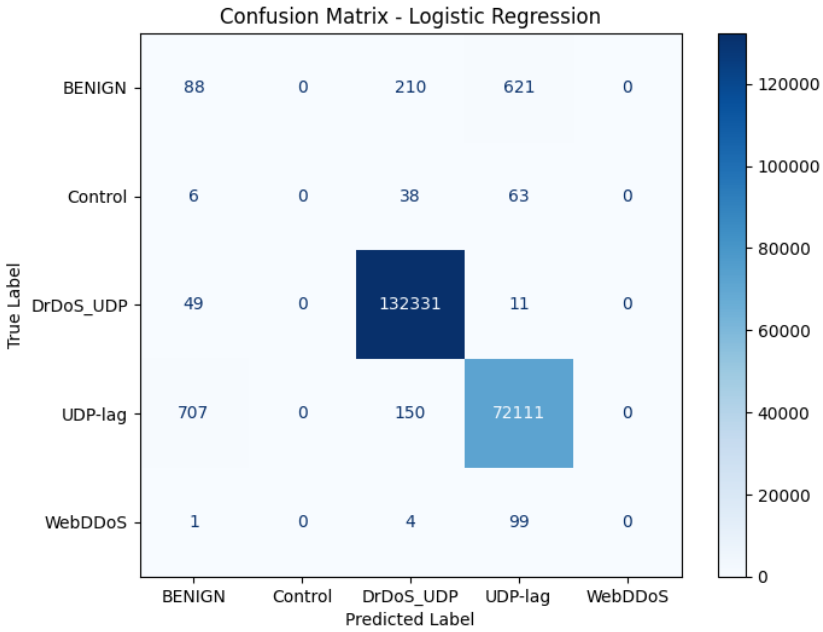

Figure 37. Logistic regression confusion matrix.

```
The Logistic Regression classification report:
              precision    recall  f1-score   support

      BENIGN       0.10      0.10      0.10       919
     Control       0.00      0.00      0.00       107
   DrDoS_UDP       1.00      1.00      1.00    132391
     UDP-lag       0.99      0.99      0.99     72968
     WebDDoS       0.00      0.00      0.00       104

    accuracy                           0.99    206489
   macro avg       0.42      0.42      0.42    206489
weighted avg       0.99      0.99      0.99    206489

The accuracy score is: 0.9905128118204843
root@Thinkbook:/home/alijose14/Documents/Capstone#
```

Figure 38. Logistic regression classification report.

5.5.2 Support Vector Machine

As suggested in sklearn documentation for SVM, the implementation of this algorithm is not recommendable for datasets larger then tens of thousand samples. Then this implementation reduced the original dataset to 20% of its larger size and proceeded to run the classifier. The confusion matrix shown below reflects a poor performance across the five labels studied. The accuracy of the model is around 91,7672% and precision does not reach 100% for any of the labels studied. The classification report shows values of 100% due to the approximation of values.

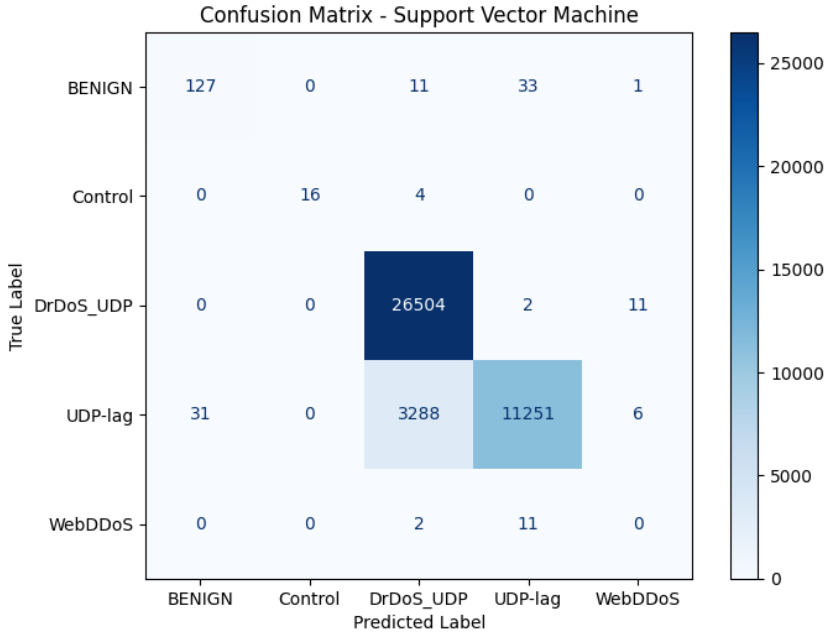

Figure 39. Support vector machine confusion matrix.

```
The SVM classification report:
              precision    recall  f1-score   support

      BENIGN       0.80      0.74      0.77       172
     Control       1.00      0.80      0.89        20
   DrDoS_UDP       0.89      1.00      0.94     26517
     UDP-lag       1.00      0.77      0.87     14576
     WebDDoS       0.00      0.00      0.00        13

    accuracy                           0.92     41298
   macro avg       0.74      0.66      0.69     41298
weighted avg       0.93      0.92      0.91     41298

The accuracy score is: 0.9176715579446947
```

Figure 40. Support vector machine classification report.

5.5.3 Naïve Bayes

The algorithm in this case could classify Benign and Control packets correctly but lacked precision to identify some packets of three malign signatures. The accuracy of the model is high since it predicted correctly 205185 out of 206489 packets which converges in 99,3684% as shown in the classification report below.

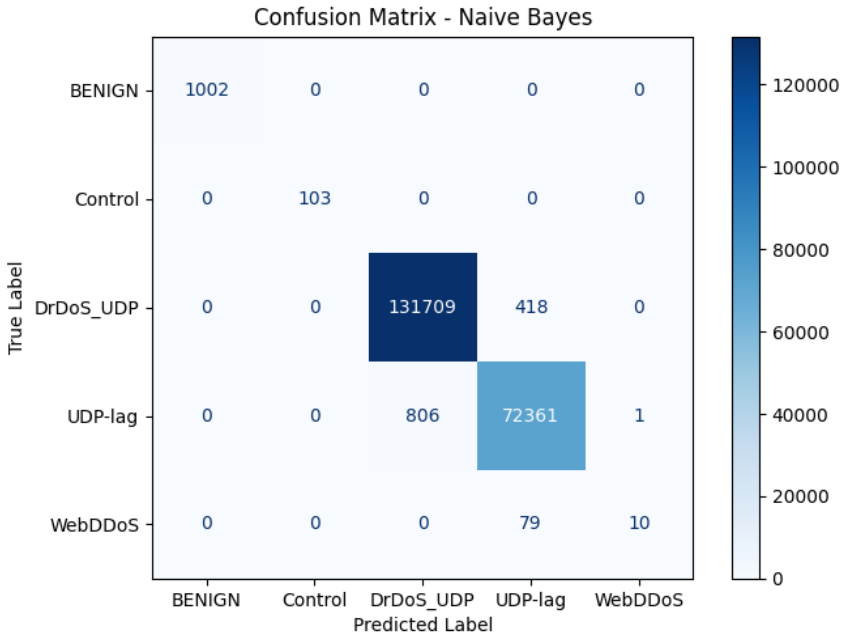

Figure 41. Naive Bayes confusion matrix

```
The Naive Bayes classification report:
              precision    recall  f1-score   support

      BENIGN       1.00      1.00      1.00      1002
     Control       1.00      1.00      1.00       103
   DrDoS_UDP       0.99      1.00      1.00    132127
     UDP-lag       0.99      0.99      0.99     73168
     WebDDoS       0.91      0.11      0.20        89

    accuracy                           0.99    206489
   macro avg       0.98      0.82      0.84    206489
weighted avg       0.99      0.99      0.99    206489

The accuracy score is: 0.9936848936262949
root@Thinkbook:/home/alijose14/Documents/Capstone#
```

Figure 42. Naive Bayes classification report.

5.5.4 k-Nearest Neighbors

This classifier shows pretty good precision to predict the values of each class, however, as evidenced in the confusion matrix, no class reached 100% of samples classified correctly. The accuracy of the model tends to be high since the algorithm could process correctly 206385 out of 206489 samples which generates 99,9496% as shown in the classification report below.

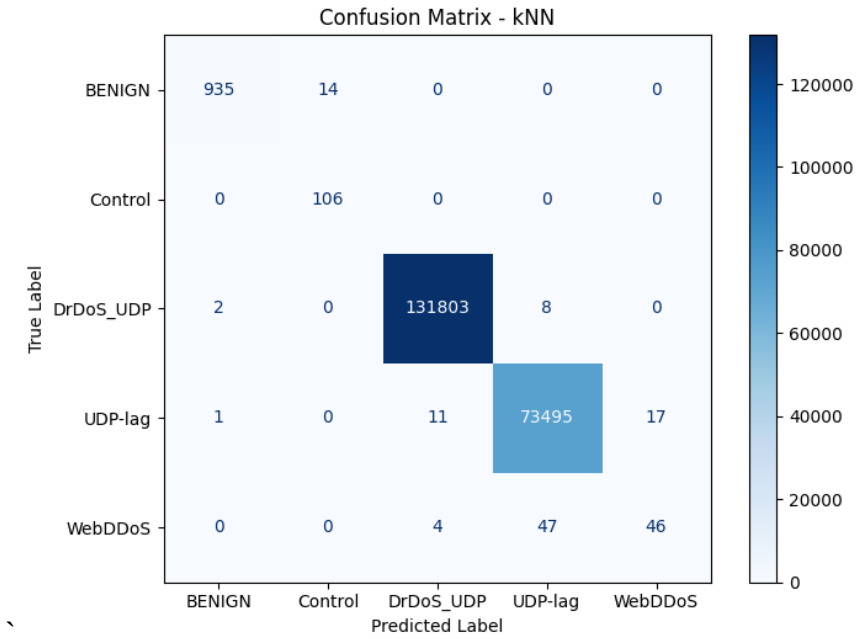

Figure 43. k-NN confusion matrix

```
The k-NN classification report:
              precision    recall  f1-score   support

      BENIGN       1.00      0.99      0.99       949
     Control       0.88      1.00      0.94       106
   DrDoS_UDP       1.00      1.00      1.00    131813
     UDP-lag       1.00      1.00      1.00     73524
     WebDDoS       0.73      0.47      0.58        97

    accuracy                           1.00    206489
   macro avg       0.92      0.89      0.90    206489
weighted avg       1.00      1.00      1.00    206489

The accuracy score is: 0.9994963412094591
root@Thinkbook:/home/alijose14/Documents/Capstone#
```

Figure 44. k-NN classification report.

5.5.5 Decision Tree

This algorithm presented very values of precision and accuracy. The model managed to predict correctly 206464 out of 206489 with an accuracy of 99.9880% and high precision for 4 out of 5 classes.

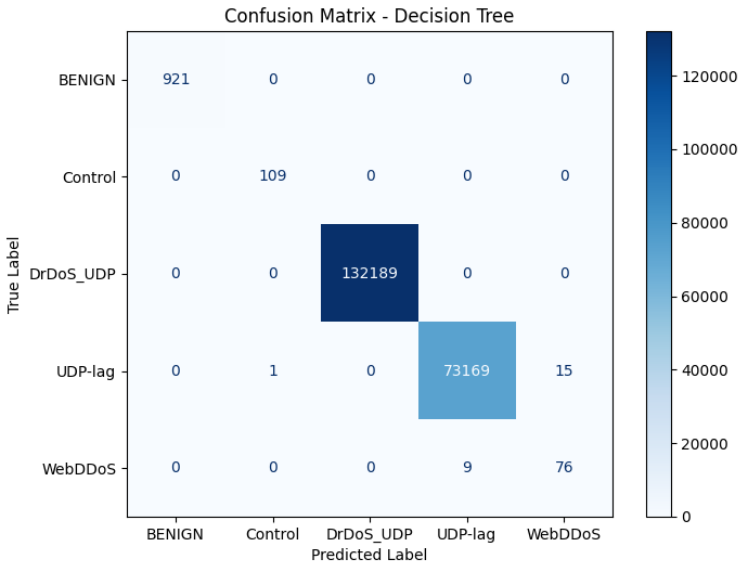

Figure 45. Decision tree confusion matrix

```
The Decision Tree classification report:
              precision    recall  f1-score   support

      BENIGN       1.00      1.00      1.00       921
     Control       0.99      1.00      1.00       109
   DrDoS_UDP       1.00      1.00      1.00    132189
     UDP-lag       1.00      1.00      1.00     73185
     WebDDoS       0.84      0.89      0.86        85

    accuracy                           1.00    206489
   macro avg       0.97      0.98      0.97    206489
weighted avg       1.00      1.00      1.00    206489

The accuracy score is: 0.9998789281753507
root@Thinkbook:/home/alijose14/Documents/Capstone#
```

Figure 46. Decision tree classification report.

CHAPTER 6

RESULTS

6.1 Interpretation of findings

After going through the technical specifications of the 5G network, the security concepts, and the machine learning theory this research assessed the security landscape on the basis of the UE's and the protocol stack. Afterwards, one 5G scenario was defined to assess the performance of classifiers making use of data that was initially generated by the Canadian Institute for Cybersecurity but modified to make suitable to the tunneling conditions of the GTP protocol.

6.1.1 The Cellular Network

The outcome of the previous chapter points to a large list of vulnerabilities, most of them present in the outer layer of the network which in some way is consistent with the preliminaries of security for 5G networks. The TR 29.915 specifies in the description of the trust model that it decreases as long as the data moves from core network towards the RAN and UE. That explains why the UE's are the first on the list when the disruptions occur.

In the same vein, the security landscape has shown that the UE's reported the largest quantity of flaws in comparison with the other network elements such as RAN and CN. The analysis considered the most dominant players in the value chain; however, it is expected to grow exponentially due to the introduction of IoT and new UE's vendors.

Along with the analysis of vendors, the findings indicate that the root cause that makes UE's less secure is the lack of rigour in programming or poor programming techniques to develop either operating systems or compatible applications. Moreover, the complexity of applications that will be launched in the 5G ecosystem will force vendors to integrate libraries developed by third-parties which will create security holes with unforeseen consequences.

Regarding the RAN, there are two scenarios to consider within an operational network. In the first instance, the early deployments of 5G represents a challenge for ISP's who have to provide reliable and innovative services while they deal with the vulnerability existing on legacy systems. On one side, the NSA model, while the SA architecture represents an improvement in terms of privacy since IMSI is not longer sent. In consequence, the flow of information during the initial attachment illustrates an improvement in terms of privacy and security for final users.

The CN shows its vulnerabilities in both NSA and SA model keeping GTPv1 on the top of the protocol stack. As this research explained in the previous chapter, an attacker can abuse the system by scanning the network with the purpose of receiving critical information such as the IP address of the GTP peers. Once the attacker maps the network entities, it would be simple to exploit the lack of sender authentication to launch a DoS/DDoS or the lack of encryption and integrity to tamper tunneling information such as TEID's or User Identifiers.

In the case of the AMF, as a centralized unit, it tends to be vulnerable to DoS/DDoS attacks. Certainly, the implementation of the SCTP protocol represents an improvement to avoid TCP-based attacks, but the entity is still prone to receive malicious traffic such as the INIT flooding attack that would overwhelm the processing capacity of the device since it has to compute a large number of cookies. Hence, it becomes a DoS/DDoS attack.

AMF and UPF are frontline entities that can be reached to exploit the vulnerabilities present in the protocol stack. However, the CN performs some other functions that can be impacted indirectly in case the AMF receives a malicious flood of Registration Requests. The AUSF can receive a request to validate SUCI, the AUSF would forward the SUCI to UDM, UDM then replies to AMF either with positive or negative answers. This flow generates amplification of malicious and invalid traffic over the network which impacts its performance.

6.1.2 The Machine Learning Techniques.

The data captured reflected a non-linear behaviour throughout the time. It seems coherent to think that in real conditions, non-linearity would be a characteristic for data generated by subscribers. From the results gotten in the previous assessment, the analysis of metrics defines what method performs better in the detection of the DoS attacks. Initially, the accuracy seems to be very high for every model, however, the Decision Tree algorithm resulted to be the winner in this segment since showed the highest accuracy in comparison with the other algorithms. On the other hand, SVM performs worst due to the limitations of the system to process datasets larger than tens of thousands of entities.

Table 29 shows the Accuracy value for each model. Decision tree performs better than the others since it partitions the data as explained in 4.2.1.2. k-NN model got the second place in this segment because it easy to find the neighbours in a set of data represented in Figure 23 which is consistent with the approximation approach to predict values in well defined boundaries. The family of linear classifiers tends to have inferior results since samples are dispersed and these algorithms do not have the flexibility to study all the samples as presented in this study.

Metric	Logistic Regression	SVM	Naïve Bayes	k-NN	Decision Tree
Accuracy	0.9905128118	0.9176715579	0.9936848936	0.9994963412	0.9998789281

Table 29. Accuracy comparative table.

6.1.3 The Security of 5G Networks and Machine Learning

To design the cybersecurity framework, this research takes into consideration 3 principles exposed throughout the development of the theoretical perspective. In 4.1.8.1 is said that the 3GPP group defined security domains for the entire network, in second place, it been said that the DoS attacks tend to hit the centralized network elements to disrupt the entire operation of the system and finally, the X.805 framework indicated that the user and control plane must be protected but also the management plane.

Regarding the User Equipment Domain, it is possible to enhance security in this domain if ISP's manage implement mechanisms in the access network that would detect anomalies in the traffic patterns that the subscribers generate. If an event occurs, the CRM can send a push or simple notification that the normal operation of the system has been abused. According to our results and

the characteristics of the traffic that the subscribers generate, k-NN or Decision Tree are good options to deal with non-linear patterns.

To protect the Access Network Domain, the implementation of classifiers is also helpful to detect anomalies in traffic coming from the User Equipment Domain, however, the gNB's must be tagged as a local centralized unit and can suffer attacks of different kinds, for instance the classifier to use must be flexible to received different traffic patterns that in some case can present a non-linear behaviour. Regarding the interface that handles the traffic to/from CN, the solution may be straightforward. Since communication flow is supported by IP protocol with variants of SCTP for the control plane and UDP in the transport layer, the complexity is higher in terms of pattern recognition, in the same vein, a hybrid implementation of linear and non-linear models would be useful to get more accuracy on predictions. Naïve Bayes can be implemented to process Control and Management data, while Decision Tree can be used for the rest of traffic.

Finally, the management plane specified in X.805 can be protected by implementations of ML, also analyzing traffic patterns related to the O&M activities. Normally, the activities that impact the operation of the network in this plane are scheduled in time and requires some levels of approval before being executed. In this case the classifiers can take into consideration not only the IP or Ports, but also the time frame in which these operations are performed.

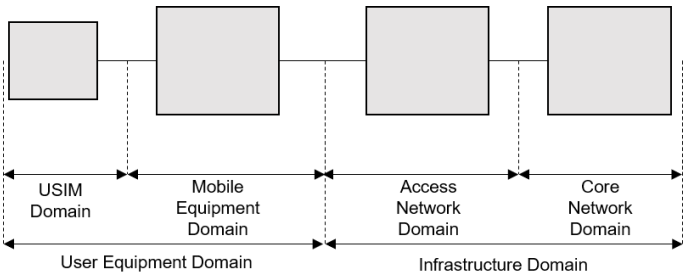

Table 30. Security Domain

6.2 Limitations

This project considered to use NetSIM to simulate the traffic circulating over the 5G network, however, the dataset generated by the CIC included proper interactions of human behaviour, while the proof of concept in NetSIM would include only control data.

The dataset used in this research shows a small proportion of benign traffic generated by legitimate elements. Even the CIC states that to generate this data they made used of the B-profile system to simulate the behaviour of human interactions on Internet, in a real environment, the volume of benign packets could be significantly high. Since the signatures studied are associated to volumetric attacks, this study considers that the dataset used is valid to reach the purpose of this research. However, a data collection on the N3 interface would generate more accurate results.

The implementation of ML in Python through the library scikit-learn showed limitations to compute the prediction using the SVM algorithm. As it stated in the documentation, the datasets of more than tens of thousand of samples must be resized in order to ease the calculations.

CHAPTER 7

CONCLUSIONS

In order to summarize the findings, it is important to mention that this request went through three technical areas such as 5G cellular networks, internet security and machine learning. Certainly, the approach conducted, led this research to put the pieces together and give a broad perspective about the benefits of analytics for 5G networks in a security context.

- The implementation of cybersecurity measures in 5G networks deserves special attention due to the different perspective it can take when the architecture is analyzed. On one side the design proposed by the 3GPP exploits the system in granular elements with well defined network functions, however, the introduction of the SDN/NFV gives another dimension in terms of cybersecurity. Beyond the configuration that vendors and operators can implement in this regard, researchers, operators, and suppliers agree on the idea that the centralized elements are the most likely to be hit by any attempt to disrupt the network operation.

- Beyond the different vulnerabilities that the 5G systems drags from the legacy networks, the large source of threats is condensed in the UE. The flaws on the network itself can be patched or inspected by implemented analytics, but the massive adoption of IoT brings with it an unknown quantity of zero-day vulnerabilities as a result of poor programming practices and less smart devices.

- In the DoS/DDoS context, every network function works in collaboration with the others either in terms of authentication or signalling. Even concepts of D2D and Edge Computing intend to minimize the dependency on the CN, every single network element can be hit by any of the variants of the Denial-of-Service attack.

- The implementation of machine learning algorithms in a case study that simulated the traffic flow through the N3 interface showed that with proper characterization the algorithms can classify the behaviours if patters are properly labeled in the train set.

- The study of the classifiers in a supervised learning approach demonstrated that non-linear classifiers tend to perform better with the signatures of the DoS attack. With the random characteristic of Internet data, it is suggested to used non-linear models such as decision trees or Naïve Bayes.

CHAPTER 8

GLOSSARY

3GPP 3rd Generation Partnership Project
5GMM 5G Mobility Management
AES Advanced Encryption Standard
AF Application Function
AI Artificial Intelligence
AKA Authentication and Key Agreement
AMF Access and Mobility Management
AMPS Advanced Mobile Phone System
AUC Authentication Centre
AUSF Authentication Sever Function
BBU Band Base Unit
BSC Base Station Controller
BSS Base Station Subsystem
BTS Base Transceiver Station
CDMA Code Division Multiple Access
CN Core Network
CP Control Plane
C-RAN Cloud Radio Access Network
CS Circuit-Switched
CSI Channel State Information
CUPS Control and User Plane Separation
D2D Device-to-Device
DDoS Distributed Denial-of-Service
DHCP Dynamic Host Configuration Protocol
DoS Denial-of-service attack
EAP Extensible Authentication Protocol
EIR Equipment Identity Register
EN-DC E-UTRA-NR Dual Connectivity
EN-DC E-UTRAN New Radio – Dual Connectivity
eV2X Enhanced Vehicle-to-Everything
GSM Global System for Mobile Communications
GTP GPRS Tunnelling Protocol
GUTI Global Unique Temporary Identifier
HLR Home Location Registry
HN Home Network
HSS Home Subscriber Server
IDS Intrusion Detection
IMEI International Mobile Equipment Identity
IMSI International Mobile Subscriber Identity
IoT Internet of things
ISDN Integrated Services Digital Network
ISP Internet service provider

LPN Low Power Node
LS-CSSP Large-Scale Cooperative Spatial Signal Processing
M2M Machine to machine
MAC Medium Access Control
MANO Management and Orchestration
mBB Mobile Broadband
MBS Macro Base Stations
MIMO Multiple In, Multiple Out
ML Machine Learning
MME Mobile Management Entity
mmWave millimeter Wave
MN Master Node
MR-DC Multi-Rat Dual Connectivity
MS Mobile Station
MSC Mobile Services Switching
MVNO Mobile Virtual Network Operator
NAS Non-access stratum
NAS-MM Non-Access Network Mobility Management
NF Network Functions
NFV Network Function Virtualization
NFVI Network Function Virtualization Infrastructure
ng-eNB Next-Generation eNodeB
NG-RAN Next-Generation Radio Access Network
NIST National Institute of Standards and Technology
NOC Network Operation Center
NR New radio
NRF Network Repository Function
NSSF Network Slice Selection Function
PCF Policy Control Function
PCRF Policy and Charging Rules Function
PDCP Packet Data Convergence Protocol
PDN Public data network
PEI Permanent Equipmnet Identifier
P-GW Packet Data Network Gateway
PS Packet-Switched
PSTN Public Switched Telephone Network
QoS Quality of Service
RAN Radio Access Network
RBAC Role-Based Access Control
RLC Radio Link Control
RRU Radio Remote Unit
SASE Security Access Service Edge
SBA Service-Based Architecture
SCS Subcarrier Spacing
SDAP Service Data Adaptation Protocol
SDN Software Defined Networking

SecaaS Security as a Service
SEPP Security Edge Protection Proxy
S-GW Serving Gateway
SIM Subscriber identification module
SLA Service Level Agreement
SME Short Message Entity
SMF Session Management Function
SMS Short Message Service
SN Secondary Node
SSDF Spectrum Sensing Data Falsification
SUCI Subscription Concealed Identifier
SUPI Subscription Permanent Identifier
SVM Support Vector Machine
U2L User to Local
U2R User to Root
UDM Unified Data Management
UDR Unified Data Repository
UDSF Unstructured Data Storage Function
UE User Equipment
UHD Ultra High Definition
UICC Universal Integrated Circuit Card
UIM User Identity Module
UMTS Universal Mobile Telecommunications System
UP User Plane
UPF User Plane Function
URLLC Ultra-Reliable Low Latency Communications
UTRAN UMTS Terrestrial Radio Access Network
VIM Virtualized Infrastructure Manager
VLR Visitor Location Register
VM Virtual Machine

CHAPTER 9

REFERENCES

[1] World Economic Forum, 01 01 2020. [Online]. Available: http://www3.weforum.org/docs/WEF_Cybercrime_Prevention_ISP_Principles.pdf. [Accessed 20 09 2020].

[2] "International Telecommunication Union," [Online]. Available: https://www.itu.int/osg/spu/ni/3G/technology/index.html. [Accessed 23 September 2020].

[3] Z. F. a. P. Porter, "Advance Mobile Phone Service," *The Bell System Technical Journal*, vol. 58, no. 1, pp. 43-69, 1979.

[4] R. S. C. L. P. Gould, GSM, cdmaOne and 3G Systems, West Sussex: John Wiley & Sons, 2001.

[5] C.-C. L. P. G. Raymond Steele, GSM, cdmaOne, and 3G systems, Chichester [England]: John Wiley, 2001.

[6] J. Eberspächer, GSM : architecture, protocols and services, Chichester, U.K.: Wiley, 2009.

[7] V. Vanghi, The cdma2000 system for mobile communications, Upper Saddle River, N.J: Prentice Hall PTR, 2004.

[8] P. Lescuyer, UMTS: Origins, Architecture and the Standard, London: Springer, 2004.

[9] C. Cox, An introduction to LTE : LTE, LTE-advanced, SAE, VoLTE and 4G mobile communications, Second edition., Chichester, West Sussex, United Kingdon: John Wiley & Sons, Inc, 2014.

[10] E. Hajlaoui, A. Zaier, A. Khlifi, J. Ghodhbane, M. B. Hamed and L. Sbita, "4G and 5G technologies: A Comparative Study," in *5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Sousse, Tunisia, 2020.

[11] Huawei Technologies Co., LTD, "5G Network Architecture-A High Level View," Huawei, Shenzhen, P.R. China, 2016.

[12] ETSI, "WHY DO WE NEED 5G?," ETSI, [Online]. Available: https://www.etsi.org/technologies/5g#:~:text=So%205G%20should%20deliver%20significantly,offering%20full%20mobility%20and%20coverage).. [Accessed 01 02 2021].

[13] D. M. T. N. Eoin O'Connell, "Challenges Associated with Implementing 5G," MDPI, Ireland, 2020.

[14] 3GPP, 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 15.4.0 Release 15), Sophia Antipolis, France: ETSI.

[15] ETSI, "3GPP TS 23.401 version 12.6.0 Release 12," ETSI, Sophia Antipolis, France, 2014.

[16] K. N. Noomene Ben Henda, "Formal Analysis of Security Procedures in LTE - A Feasibility Study," Springer International Publishing, Stockholm, Sweden, 2014.

[17] 3GPP TS 23.501, "System Architecture for the 5G System," ETSI, Sophia Antipolis, France, 2018.

[18] 3. T. 33.501, "Security architecture and procedures for 5G System," ETSI, Sophia Antipolis, 2018.

[19] S. Ahmadi, 5G NR : architecture, technology, implementation, and operation of 3GPP New Radio standards, London, United Kingdom: Academic Press, 2019.

[20] 3GPP TR 21.915, V15.0.0, "Release 15 Description," ETSI, Sophia Antipolis, France, 2019.

[21] N. H. Zeineb Guizani, "CRAN, H-CRAN, and F-RAN for 5G systems: Key capabilitiesand recent advances," Wiley, 2017.

[22] A. M. M. P. O. S. a. W. Y. Osvaldo Simeone, "Cloud Radio Access Network: Virtualizing Wireless Access for Dense Heterogeneous Systems," *JOURNAL OF COMMUNICATIONS AND NETWORKS*, vol. 18, no. 2, pp. 135-149, 2016.

[23] Y. L. Z. Z. C. W. Mugen Peng, "System Architecture and Key Technologies for 5G Heterogeneous Cloud Radio Access Networks," *IEEE Network*, December 2014.

[24] N. C. R. L. E. A. F. M. José Quaresma Filho, "A Software Defined Wireless Networking Approach for Managing Handoff in IEEE 802.11 Networks," João Pessoa, Brazil, 2018.

[25] A. X. John Kaippallimalil, "5G System Design," in *5G System Architecture*, Cham, Switzerland, Springer, 2020, pp. 273-298.

[26] IEEE Spectrum, "Applications of Device-to-Device Communication in 5G Networks," National Instruments, [Online]. Available: https://spectrum.ieee.org/computing/networks/applications-of-devicetodevice-communication-in-5g-networks. [Accessed 01 02 2021].

[27] H. A. E. &. S. M. A. E.-k. Hanan H. Hussein, "Intensive Benchmarking of D2D communication over 5G cellular networks: prototype, integrated features, challenges, and main applications," Springer, 2020.

[28] J. Liu, M. Sheng, L. Liu and J. Li, "Network Densification in 5G: From the Short-Range Communications Perspective," IEEE Communications Magazine, United States, 2017.

[29] Ericsson, "Cellular IoT in the 5G era," Ericsson, Stockholm, Sweden, 2020.

[30] 3. T. 22.261, "Service requirements for next generation new services and markets," ETSI, Sophia Antipolis, 2018.

[31] Ö. B. E. T. A. K. T. S. Michał Maternia, "Interference management, mobility management, and dynamic reconfiguration," in *5G Mobile and Wireless Communications Technology*, Cambridge, Cambridge University Press, 2016, pp. 381-400.

[32] J. M. F. M. B. Jeffrey Cichonski, "Guide to LTE Security," National Institute of Standards and Technology, Gaithersburg: USA., 2017.

[33] Cybersecurity and Infrastructure Security Agency, "Security Tip (ST04-015). Understanding Denial-of-Service Attacks," [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-015#:~:text=What%20is%20a%20denial%2Dof,a%20malicious%20cyber%20threat%20actor.. [Accessed 06 11 2020].

[34] F. Tian, P. Zhang and Z. Yan, "A Survey on C-RAN Security," IEEE Access, 2017.

[35] M. Z. L. X. K. W. a. J. L. H. Chen, "Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack," IEEE Trans, 2016.

[36] Q. W. X. H. a. J. L. X. Wang, "Security technology in virtualization system: State of the art and future direction," ICISCE, Changsha, China, 2012.

[37] A. A. R. M. A. H. Alcardo Alex Barakabitze, 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges, Elsevier, 2020.

[38] IEEE innovation at work, "Edge Computing: Security Issues and Trends to Watch in 2020," [Online]. Available: https://innovationatwork.ieee.org/edge-computing-security-issues-and-trends-to-watch-in-2020/. [Accessed 01 02 2021].

[39] S. Bocetta, "Deploying Edge Cloud Solutions without Sacrificing Security," [Online]. Available: https://www.infoq.com/articles/secure-edge-systems/. [Accessed 03 02 2021].

[40] B. C. M. S. a. C. L. Y. Huang, "Security Impacts of Virtualization on a Network Testbed," IEEE, Gaithersburg, USA., 2012.

[41] R. Chandramouli, "Security Recommendations for Hypervisor Deployment on Servers," National Institute of Standards and Technology, Gaithersburg, USA, 2018.

[42] J. M. K. S. Murugiah Souppaya, "Application Container Security Guide," NIST, Gaithersburg, USA, 2017.

[43] S. S.-H. L. J. R. H. Shao Ying Zhu, Guide to Security in SDN and NFV, Leicester, UK: Springer, 2017.

[44] A. P. V. E. Tony Thomas, "Introduction to Machine Learning," in *Machine Learning Approaches in Cyber Security Analytics*, Singapore, Springer, 2020, pp. 17-36.

[45] C. C. a. D. Freeman., Machine learning and security : protecting systems with data and algorithms, First edition., Sebastopol, CA: O'Reilly Media, 2018.

[46] National Institute of Standards and Technology, "Computer Security Resource Center," [Online]. Available: https://csrc.nist.gov/glossary/term/virus#:~:text=Definition(s)%3A,See%20malicious%20code.. [Accessed 09 11 2020].

[47] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015.

[48] Treck, "Vulnerability Response Information," [Online]. Available: https://treck.com/vulnerability-response-information/. [Accessed 03 12 2020].

[49] JSOF Research Lab, "https://www.jsof-tech.com/ripple20/," [Online]. Available: https://www.jsof-tech.com/wp-content/uploads/2020/08/Ripple20_CVE-2020-11901-August20.pdf. [Accessed 03 12 2020].

[50] K. M. M. Haibat Khan, "A Survey of Subscription Privacy on the 5G Radio Interface - The Past, Present and Future," University of London, Surrey, UK, 2020.

[51] R. B. S. P. J.-P. S. Altaf Shaik, "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, NY, United States, 2019.

[52] 3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS)," ETSI, Sophia Antipolis, 2018.

[53] T. M. Hafida Amgoune, "5G: Interconnection of Services and Security Approaches," Association for Computing Machinery, Tetouan, Morocco, 2018.

[54] G. C. M. T. R. Stewart, "RFC 5062. Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures," IETF, 2007.

[55] R. Stewart, "RFC 4960. Stream Control Transmission Protocol," IETF, 2007.

[5 6] C. H. M. N. Erwin P. Rathgeb, "On the Robustness of SCTP against DoS Attacks.," in *Third 2008 International Conference on Convergence and Hybrid Information Technology*, Busan, South Korea, 2008.

[5 7] J. Sau, "Securing the GPRS Network Infrastructure – a Network Operator's Perspective," SANS Institute, Bethesda, USA, 2005.

[5 8] 3GPP TS 29.281 version 16.1.0 Release 16, "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)," ETSI, Sophia Antipolis, France, 2020.

[5 9] M. S. Naveen Bindra, "Detecting DDoS Attacks using Machine Learning Techniques and Contemporary Intrusion Detection Dataset," *Automatic Control and Computer Sciences*, vol. 53, no. 5, p. 419–428, 2019.

[6 0] Microsoft, "How to select algorithms for Azure Machine Learning," Microsoft Azure, 07 05 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/machine-learning/how-to-select-algorithms. [Accessed 21 12 2020].

[6 1] Canadian Institute for Cybersecurity, "DDoS Evaluation Dataset (CIC-DDoS2019)," University of New Brunswick, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html. [Accessed 3 12 2020].

[6 2] M. Harrison, Machine Learning Pocket Reference, O'Reilly Media, Inc., 2019.

[6 3] M. Sauter, From GSM to LTE : an introduction to mobile networks and mobile broadband, Cichester, UK: Wiley, 2011.

[6 4] X. Z. H. V. P. Trung Q. Duong, Trusted Communications with Physical Layer Security for 5G and Beyond, London, UK: London: Institution of Engineering and Technology, 2017.

[6 5] 3GPP TS 38.321 , Medium Access Control (MAC) protocol specification, Sophia Antipolis: ETSI, 2018.

[6 6] F. Y. Rashid, "IEEE Spectrum," 20 Jun 2020. [Online]. Available: https://spectrum.ieee.org/tech-talk/telecom/security/5g-networks-will-juggle-legacy-security-issues-for-years. [Accessed 22 11 2020].

[6 7] "CVE Details," [Online]. Available: https://www.cvedetails.com/index.php. [Accessed 24 11 2020].

[6 8]