
Politecnico di Torino

POLITECNICO DI TORINO

Master Degree course in Communications and Computer Networks Engineering

Master Degree Thesis

# A survey on Cybersecurity in 5G.

**Supervisors**
Prof. Roberto GARELLO

**Candidate**
Seyed Mohammad MOUSAVI

ACADEMIC YEAR 2020-2021

# Dedication

*This thesis is dedicated to:*

- ♥ *My God for everything that I have and what I am.*
- ♥ *My parents and my sister for their unlimited love, support, and encouragement.*

# Acknowledgments

I want to thank my thesis supervisor, Professor Roberto Garello, for his excellent guidance, constant support, and patience during writing my thesis.
Finally, I would like to thank my parents and my sister for helping me with my studies and supporting me throughout my life. I would never have reached this level without their love and guidance.

# Table of Contents

# Chapter 1

# Introduction

In today's era, mobile communications play an important role in our modern life. In recent years, mobile technology attracted the focus of industry attention. In the last four decades, by the evolution of mobile wireless technology from 1G in 1980 to 5G in 2019 by introducing new features and capabilities in each mobile network generation and growth of them, the number of demands for using these new technologies also has gradually increased, and the mobile interaction has become an important part of our life [1].
Through the big leap in mobile networks, new opportunities and challenges for mobile wireless networks have emerged. On one side, 5G technology claims can make a dramatic change in mobile broadband networks. 5G would guarantee bigger channels (to accelerate data transfer), less latency (to be increasingly responsive), and also the ability to link more devices at once (for sensors and intelligent devices) [2].
On another side, with the dramatic advancement of new technologies and the emergence of concepts such as the Internet of Things, as well as the proliferation of wireless network users, the security of users of these technologies seems obvious and important. For example, global operators started launching 5G networks in early 2019, but this enables the movement and access of vastly higher quantities of data especially through the Internet of things (IoT). As a result, it broadens attack surfaces, and new cyber threats will emerge. Thus, it is clear that the infrastructure equipment providers should pay more attention to the Cybersecurity of 5G mobile networks by finding the latest tactics to deal with threats and be one step ahead of attackers to protect our digital communications world.
This chapter begins with an explanation of the aim of the thesis. Next, in the Motivation and research questions section, problem statements and research questions are pinpointed to specify the current problems. Then the research Limitations are described. This chapter ends with a brief description of the audience and readers to point out the thesis structure and methodology.

## 1.1 Aim of the thesis

The purpose of this thesis is to research and study the 5G networks to gain a close understanding of this newborn technology and check out its security from different aspects. Both security improvements and new vulnerabilities that 5G brings are reviewed.

## 1.2 Motivation and research questions

The first phase of inquiry is to pose the initial research questions, which this thesis aims to answer. The thesis will address the following research questions:
• What are or what would be the possible attacks to 5G networks?
• What are the available cyber-attack detections techniques in 5G networks?
• What is the minimum acceptable level of cyber security in 5G?
• What are the latest tactics to make the 5G networks more secure?
• Has cybersecurity succeeded effectively in its mission to prevent cybercrimes and mitigate cybercrimes in telecom networks, especially 5G networks?

## 1.3 Limitations

As has been mentioned so far, the 5G is the newest generation of wireless technology, and it isn't officially launched in many countries. Hence, the real vulnerabilities of this technology and its sub-disciplines are still undiscovered and aren't documented fully. Therefore, to fulfill the requirements of

this thesis, I used the available resources like peer-reviewed journal articles, books, white papers, reports, and online articles, which were sourced from the internet and online databases.

## 1.4 Thesis structure and methodology

The research methodology deployed in this paper involves the review and analysis of relevant and related literature.
The thesis is organized into six chapters. Chapter 1 introduces the research problem and describes the research objectives, research questions, limitations, and methodology. Chapter 2 presents the literature review on the subjects of cybersecurity, 5G, and cybersecurity in 5G. Chapter 3 has a review on risk management in 5G. Chapter 4 will focus on the status of 5G and its security in Italy. Chapter 5 will provide some information about the upcoming mobile communications generation (6G) and related security concerns. Finally, Chapter 6 concludes the findings in previous chapters.

# Chapter 2

# Literature study

## 2.1 A brief history of mobile communication generations:

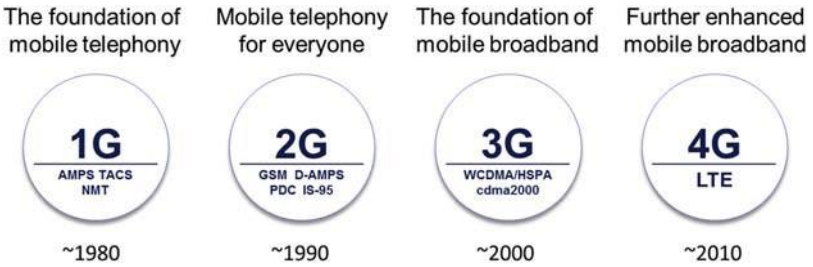

Fig 1: The different generations of mobile communication [3].

The first generation of international mobile communication(Known as 1G) systems was NMT (Nordic Mobile telephony) system and AMPS (Advanced Mobile Phone System), which were introduced in Nordic countries and North America respectively in 1981. Other analog communication systems were TACS (Total Access Communication System) used in the United Kingdom and Japan, known as Japan Total Access Communications System (JTACS). All the communication systems mentioned above were based on analog transmission, and they had voice quality problems like cross-talk between users. In addition, first-generation technology-based mobile communications systems were limited to voice services, making mobile phones available to the general public for the first time[1][4].

The second generation of mobile communications(2G) emerged in the early 1990s. Initially, there were several different technologies of the second generation, including GSM (Global System for Mobile Communication), developed jointly by a large number of European countries, D-AMPS (Digital AMPS), PDC (Personal Digital Cellular) developed and used only in Japan and after on, CDMA-based IS-95 technology was developed. The main evolvement compared to 1G was digital transmission over radio links. Although the service is still voice, using digital transmission for second-generation mobile communication systems allows it to provide limited circuit-switched data services at sped up to 14.4kbps. 2G provided services such as a short message service known as SMS and Multimedia Messaging Service known as MMS. The security feature in 2G has improved compared to 1G, such a way that all text messages are encrypting for both sender and receiver.
Implementing a packet-switched domain in addition to a circuit-switched domain led to the emergence of a new concept called GPRS(General Packet Radio Service), in which provided data rates improved from 56 Kbps up to 384 Kbps. It provides services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for internet communication services like E-mail and the possibility of access to the World Wide Wireless Web (WWW). The way of billing the data rate is another difference between GPRS traditional circuit switching. The term 2.5G is an informal name that refers to GPRS.
Then EDGE(Enhanced Data rates for GSM Evolution)(2.75G)was deployed on GSM networks in 2003 by Cingular (now AT & T) in the United States.EDGE is standardized by 3GPP(The 3rd Generation Partnership Project).GPRS networks evolved to EDGE networks with the introduction of 8PSK encoding, which helps to achieve higher data –rates (up to 236.8Kbits/s) by switching to more sophisticated methods of coding (8PSK), within existing GSM timeslots[1] [4].

The third generation of mobile communications, often referred to as just 3G, was introduced. With 3G, a real step has been taken for high-quality mobile bandwidth, enabling fast wireless internet access. This was made especially possible by the evolution of 3G known as HSPA (High-Speed Packet Access).

The 3G technology, developed by the ITU (International Telecommunication Union) in early 2000. It was a big step to establish a global standard for wireless data networks, known as the IMT-2000 standard. IMT-2000's fundamental goal was implementing an international frequency band in the 2000 MHZ range. It also aimed to bring transmission speeds of up to 394 Kbps and 2 Mbps for mobile stations and fixed stations, respectively. Existing CDMA experienced upgrades that led to CDMA2000 for cellular phone systems mainly used in North America and some parts of Asia. In Europe, it was called UMTS (Universal Terrestrial Mobile System), which is an ETSI (European Telecommunications Standards Institute) -driven technology. W-CDMA (wideband CDMA) is the air-interface technology for the UMTS in Japan and Europe. High-Speed Downlink Packet Access(HSDPA) and High-Speed Uplink Packet Access(HSUPA) were two divisions of the HSPA (High-Speed Packet Access) concept and two advancements in 3G technology. HSDPA is also known as 3.5G allowing for higher data transfer speed in W-CDMA downlink with data transmission up to 8-10 Mbit/s (and 20 Mbit/s for MIMO systems) over a 5MHz bandwidth in WCDMA downlink. On the other hand, HSUPAwhich known as 3.75G, boosts the transmission rate of the UMTS / WCDMA uplink up to 1.4Mbps and in later releases up to 5.8Mbps.3G allows operators to provide users with a wide range of the latest services, including wide-area wireless voice calls, video calls, broadband wireless data, mobile TV(IPTV) and media streaming, GPS (global positioning system), and video conferencing[5].

The development of mobile communications continued by introducing LTE to meet the requirements(improving possible end-user data rates) of increased mobile broadband subscribers and implementing infrastructure to provide more services. Orthogonal Frequency Division Multiplexing (OFDM), SC-FDE and SC-FDMA, and Multi-antenna Technique are three main LTE features. As we mentioned so far, traditional 3G systems were based on UMTS and CDMA2000, in which CDM techniques were used. OFDMA was the solution for having more probabilities of intersymbol interference because of multipath in high data rates. SC-FDMA allows multiple users to use parts of the frequency spectrum, especially in uplink communications, to achieve better battery life. Multi-antenna techniques take advantage of using multiple antennas at the receiver and/or the transmitter with the combination of advanced signal processing algorithms to achieve improved system performance, including enhanced system capacity and improved coverage, higher per-user data rates, etc. [5].

The evolution of LTE technology continued by defining some requirements by the International Telecommunications Union-Radio communications sector (ITU-R) in 2008, known as International Mobile Telecommunications Advanced (IMT-Advanced) specification. Minimum Requirements for an IMT-Advanced cellular system to be considered as 4G are listed below:

- Interoperability with other radio access networks as well as internetworking compatibility within the IMT.
- The peak data rate should be up to 100 Mbps for high mobility users and 1 Gbps for users with low mobility or stationary users.
- Be able to dynamically share and use the network resources to support more simultaneous users per cell.
- User-plane latency of less than 10 ms. Scalable bandwidth up to 40 MHz, extendable to 100 MHz.
- Downlink peak spectral efficiency (SE) of 15 bps/Hz and 6.75 bps/Hz for Uplink.
- Supporting smooth handovers across heterogeneous networks(having capability of worldwide roaming).

Although the WiMAX and LTE as two candidates of 4G weren't fully IMT-Advanced compliant, finally, they were accepted as IMT-Advanced 4G technology in November 2010[5][6].

## 2.1.1 Main radio features of LTE Advanced

### 2.1.1.1 Carrier Aggregation(Known as 4G+ or 4GPLUS):

With carrier aggregation (CA), multiple component carriers (CC) are aggregated and jointly used for transmission to/from a single terminal. Maximum five component carriers, possibly each of different bandwidths, can be aggregated, allowing for transmission bandwidths up to 100 MHz.
Carrier Aggregation has some benefits, including:

- Higher speeds: Aggregation of carriers increases spectrum resources, which provides higher data rates across the cell coverage.
- Capacity gain: Aggregating multiple carriers increases the spectrum but also includes trunking gains from dynamically scheduling traffic across the entire spectrum. This, in turn, increases cell capacity and network efficiency and improves the experience for all users.
- Optimum utilization of an operator's spectrum resources: The majority of operators have a fragmented spectrum covering different bands and bandwidths; carrier Aggregation helps combine these into more valuable spectrum resources.

### 2.1.1.2 LTE Broadcast: Evolved Multimedia Broadcast Multicast Services (eMBMS)

### In Unicast scenario:

- One data channel for device
- Limit on the maximum number of users
- Variable quality to the user, depending on the channel and the number of users

### In Broadcast scenario:

- One data channel for content
- Unlimited number of users
- High quality for everybody

### 2.1.1.3 Enhanced MIMO: Multi-User MIMO and Higher Order MIMO

Refers to a technology in which throughput could be increased through simultaneous transmission/reception by exploiting a higher number of antennas at both eNB and/or UE. MIMO 4x4 and 8x8 configurations require radiating systems with increasing dimension and complexity in both the UE side (impacting the device engineering) and the BS side (impacting site design). MIMO 2x2, MIMO 4x4, and MIMO 8x8, all on 10MHz, can reach the data rate of 75 Mbps, 150 Mbps, and 300 Mbps, respectively. MIMO experienced some advancements(Multi User-MIMO) in Release 8, 9, and 10 in which the data rate can be reached 3 Gbps through MIMO 8x8 with CA on 100MHz.

### 2.1.1.4 CoMP: Coordinated Multi-Point transmission/reception

Coordinated multi-point (CoMP) transmission and reception is considered for LTE-Advanced Rel. 11 as a tool to improve the coverage of high data rates, the cell-edge throughput, and also to increase system throughput. With CoMP, different eNBs coordinate their transmissions to reduce interference or even cooperate to increase received signal quality. Coordination can be particularly beneficial for the cell edge users who are typically affected by the interference of neighboring cells.

## 2.2 What is 5G?

The advent of the 5G network has revolutionized mobile networks. The 5G technology has begun to commence in full from 2020, and it is creating huge opportunities for consumers, enterprises, operators, vendors, and all stakeholders day by day. The fifth generation of telecommunications networks, known as 5G, is a major step forward in mobile networks and exponentially increasing Dl/Up rates and sharing of real-time data. To meet these requirements and to exploit the potential of new technologies, 3GPP developed a new radio-access technology known as NR (New Radio). Although NR reuses many of the structures and features of LTE but also unlike the LTE evolution, is not restricted by a need to retain backward compatibility. The most important difference between 4G and 5G is that the 5G is the gateway to the Internet of Things(IoT) technology. In IoT technology, all humans, devices, and even animals are connected to each other on a large scale. The latest generation of communications is expected to revolutionize Data-Driven Industries, Smart Cities, and Infrastructure Management; Because this type of telecommunication network is able to host more devices in an area with more security and reliability and with much less interruption and disruption.

In general, due to the new technologies as well as the millimeter wave spectrum(mmWave) used in the 5G generation, higher speeds, lower latency, more capacity, less interference, and higher efficiency are the features of these networks.

An example of a very important application of 5G is in remote surgical robots. In these robots, despite the fact that the robot and the user are miles apart, the use of 5G leads to increased system reliability. However, in such applications, the network latency must be less than two milliseconds.

A fast, reliable, and real-time network can make various industries independent of the need for cable connections to connect to the network. Such networks equip industries with wireless communications for more autonomous and flexible operation. Wireless and fast communication also reduces costs and increases productivity. In Addition, the spread of 5G communication generation provides the necessary infrastructure network for the areas of Smart City and Connected Car.

### 2.2.1 Usage scenarios of 5G:

The ITU-R has defined three main usage scenarios for the enhanced capabilities of IMT systems in the IMT-2020 platform: enhanced mobile broadband (eMBB), massive machine-type communication(mMTC), and ultra-reliable and low-latency communication (URLLC).

**eMBB** Refers to the improvement of the current mobile broadband services, with faster connections, higher end-user throughput, and more capacity.

**mMTC** This usage scenario is used to connect a large number of connected devices such as remote sensors, actuators, smart metering, inventory control, smart city, etc., which are usually used to transmit a small amount of data. Minimum requirements for such devices are to be low-cost and have a long battery life to make these devices operable for a long time(typically several years).

**URLLC** refers to supporting very low latency and extremely high reliability, and high availability, which guarantees robust data exchange between different entities. Examples of 5G services in this category are autonomous driving cars, smart grids, eHealth, remote surgery, industrial automation, and control, etc.

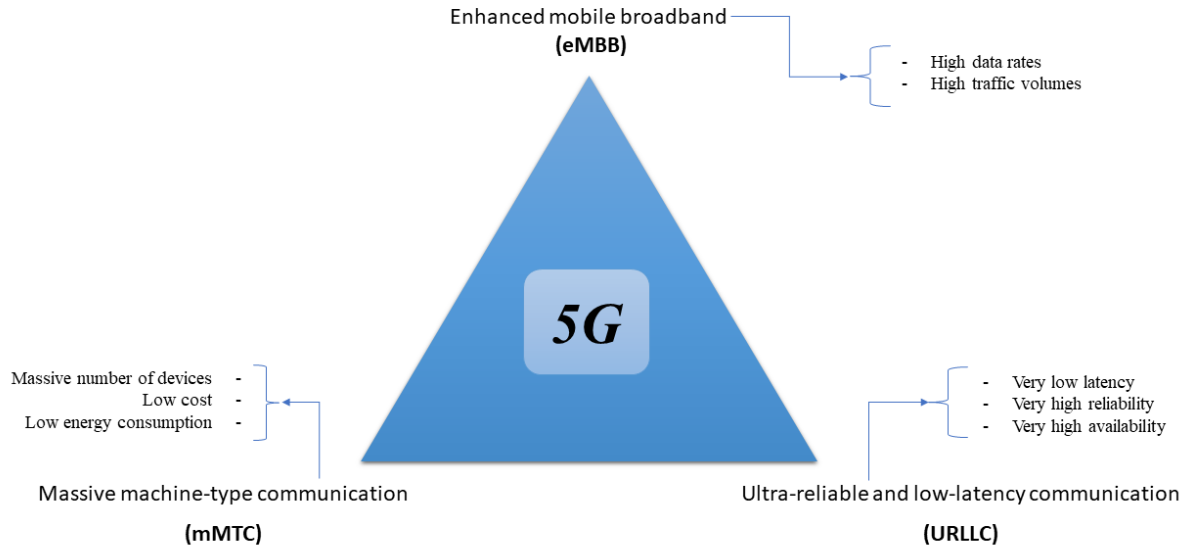


Figure1. Three main use case categories as defined by ITU in [7]and 3GPP in [8].

Report ITU-R M.2410 November 2017 defines 13 requirements related to technical performance for IMT-2020 radio interface(s).

- **Bandwidth** is the maximum aggregated system bandwidth.
- **Mobility interruption time** the shortest time duration supported by the system during which a user terminal cannot exchange user plane packets with any base station during transitions.
- **Mobility** is the maximum mobile station speed at which a defined QoS can be achieved (in km/h).
- **Reliability** relates to the capability of transmitting a given amount of traffic within a predetermined time duration with a high success probability.
- **Efficiency** is the capability of a RIT/SRIT to minimize the radio access network energy consumption in relation to the traffic capacity provided.
- **Connection density** is the total number of devices fulfilling a specific quality of service (QoS) per unit area (per $km^2$).
- **Latency: User plane latency** is the contribution of the radio network to the time from when the source sends a packet to when the destination receives it (in ms). **Control plane latency** refers to the transition time from a most "battery efficient" state (e.g., Idle state) to the start of continuous data transfer (e.g., Active state).
- **Area traffic capacity** is the total traffic throughput served per geographic area (in $Mbit/s/m^2$).
- **Average spectral efficiency** is the aggregate throughput of all users (the number of correctly received bits, i.e. the number of bits contained in the SDUs delivered to Layer 3, over a certain period of time) divided by the channel bandwidth of a specific band divided by the number of TRxPs and is measured in bit/s/Hz/TRxP.
- **5th percentile user spectral efficiency** is the 5% point of the CDF of the normalized user throughput.
- **User experienced data rate** is the 5% point of the cumulative distribution function (CDF) of the user throughput

- **Peak spectral efficiency** is the maximum data rate under ideal conditions normalized by channel bandwidth (in bit/s/Hz).
- **Peak data rate** is the maximum achievable data rate under ideal conditions (in bit/s).

These technical parameters and the corresponding minimum requirements are summarized in Table 1.

| Parameter | Minimum Technical Performance Requirement |
|---|---|
| Peak data rate | Downlink: 20 Gbit/s<br>Uplink: 10 Gbit/s |
| Peak spectral efficiency | Downlink: 30 bit/s/Hz<br>Uplink: 10 bit/s/Hz |
| User-experienced data rate | Downlink: 100 Mbit/s<br>Uplink: 50 Mbit/s |
| Fifth percentile user spectral efficiency | 3× IMT-Advanced |
| Average spectral efficiency | 3× IMT-Advanced |
| Area traffic capacity | 10 Mbit/s/$m^2$ (indoor hotspot for eMBB) |
| User plane latency | 4 ms for eMBB<br>1 ms for URLLC |
| Control plane latency | 20 ms |
| Connection density | 1,000,000 devices per $km^2$ |
| Energy efficiency | Related to two aspects for eMBB:<br>a. Efficient data transmission in a loaded case<br>b. Low energy consumption when there is no data<br>The technology shall have the capability to support a high sleep ratio and long sleep duration |
| Reliability | $1-10^{-5}$ success probability of transmitting a layer 2 PDU (Protocol Data Unit) of 32 bytes within 1 ms, at coverage edge in Urban Macro for URLLC |
| Mobility | Normalized traffic channel data rates defined for 10, 30, and 120 km/h at ~1.5× IMT-Advanced numbers<br>Requirement for high-speed vehicular defined for 500 km/h (compared to 350 km/h for IMT-Advanced) |
| Mobility interruption time | 0 ms |
| Bandwidth | At least 100 MHz and up to 1 GHz in higher-frequency bands. Scalable bandwidth shall be supported |

Table 1 Overview of Minimum Technical Performance Requirements for IMT-2020 [9].

## 2.2.2 5G NR SYSTEM ARCHITECTURE

System architectures of both the Radio-Access Network (RAN) and the Core Network (CN) experienced some changes in terms of splitting the functionality between the two networks.

### Radio-Access Network (RAN)

The RAN is responsible for all radio-related functionality of the overall network including connection of user equipment to a core network (all radio-related functionalities) is done by RAN. Scheduling, radio-resource handling, retransmission protocols, coding, and various multi-antenna schemes are examples of RAN responsibilities.

### Core Network (CN)

The 5G core network is one of the main parts of the overall mobile network. Handling some functions like authentication, charging functionality, and setup of end-to-end connections are some of the responsibilities of this part of the mobile network. There are different modes to connect the NR radio-access network to the core network. In the first case, known as non-standalone mode, the NR radio access network is connected to the legacy LTE (Long-Term Evolution) core network known as the Evolved Packet Core(EPC). And in the second case, which would be standalone mode, in which NR connecting to the 5G core, as well as LTE connecting to the 5G core(Later releases). It should be noted the first version of NR operates in a non-standalone mode where NR is connected to the EPC.

## 2.2.2.1 5G CORE NETWORK:

The 5G core network had three new areas of enhancement compared to EPC:
A service-based architecture is an architecture in which all of the services are delivered as a set of interconnected Network Functions (NFs). These NFs are authorized to access each other's services.
5G network slicing is a network architecture that enables the multiplexing of virtualized and independent logical networks(slices) on the same physical network infrastructure, while from the end-user application perspective, they appear as independent networks or entities.
Control and User Plane Separation of EPC nodes (CUPS) offer the ability to separate between control plane functions and user plane functions on an as-needed basis and in real time[10].

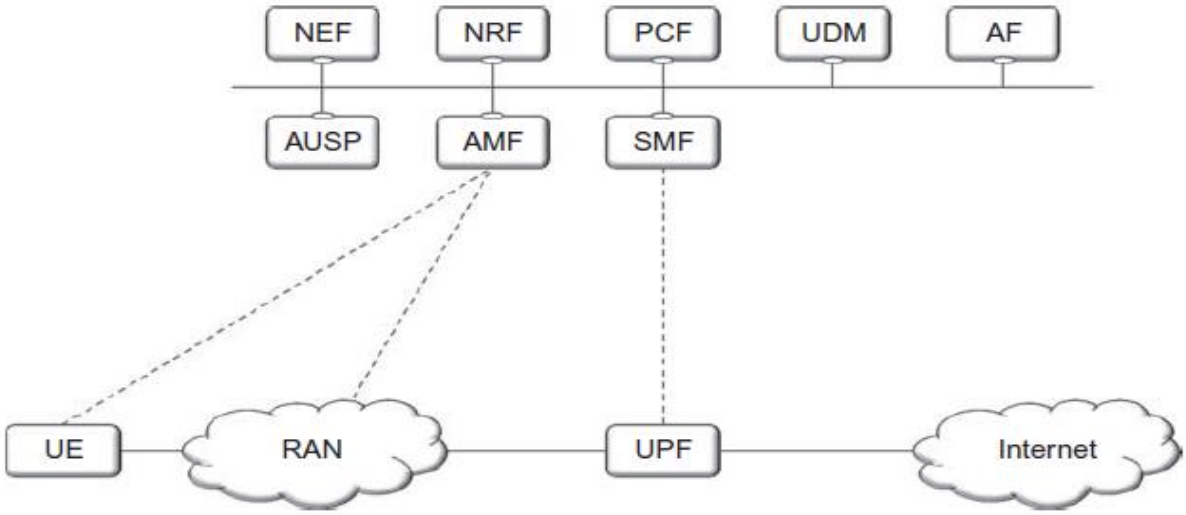


Figure 2. shows a service-based representation of high-level core network architecture[11].

### The user-plane function consists of:

- User Plane Function (UPF) is a gateway between the RAN and external networks such as the Internet (responsible for data plane handling).

The control-plane functions consist of several parts.

- Session Management Function (SMF) handles the UE's data sessions (i.e., session establishment and management), formerly part of MME. It supports allocation of UE's IP address, UPF selection, and control of policy enforcement.
- The Access and Mobility Management Function (AMF) is for control signaling to/from UE, similarly to MME in EPC but only managing UE registration, reachability, connection, and mobility. It also performs access authentication and authorization.
- Policy Control Function (PCF) responsible for policy rules
- Unified Data Management (UDM) is responsible for authentication credentials and access authorization.

- Network Exposure Function (NEF) is a function that provides a means to securely expose the services and capabilities provided by 3GPP network functions.
- NR Repository Function (NRF) supports the service discovery function. As such, it is able to receive NF Discovery Request from a NF instance and can provide information about discovered NF instances.
- Authentication Server Function (AUSF) handles authentication functionality.
- Application Function (AF) provides session-related information to the PCRF in support of PCC rule generation[11][12].

### 2.2.2.2 5G RADIO-ACCESS NETWORK

The radio-access network can have two types of nodes connected to the 5G core network. A NG-RAN node is either a gNB, providing NR User Plane (UP) and Control Plane (CP) protocol terminations towards the UE or a ng-eNB, providing E-UTRA (i.e., LTE like) UP and CP protocol terminations towards the UE. gNBs and ng-eNBs are interconnected via Xn interface.NG-RAN nodes connect to 5G Core network (5GC) nodes known as Access and Mobility management Function (AMF) and User Plane Function (UPF) via NG-C and NG-U interfaces, respectively. There is also a standardized way to split the gNB into two parts, a central unit(gNB-CU) and one or more distributed units (gNB-DU) using the F1 interface. In the case of a split gNB, the RRC, PDCP, and SDAP protocols, described in more detail below, reside in the gNB-CU and the remaining protocol entities (RLC, MAC, PHY) in the gNB-DU. The interface between the gNB (or the gNB-DU) and the device is known as the Uu interface.

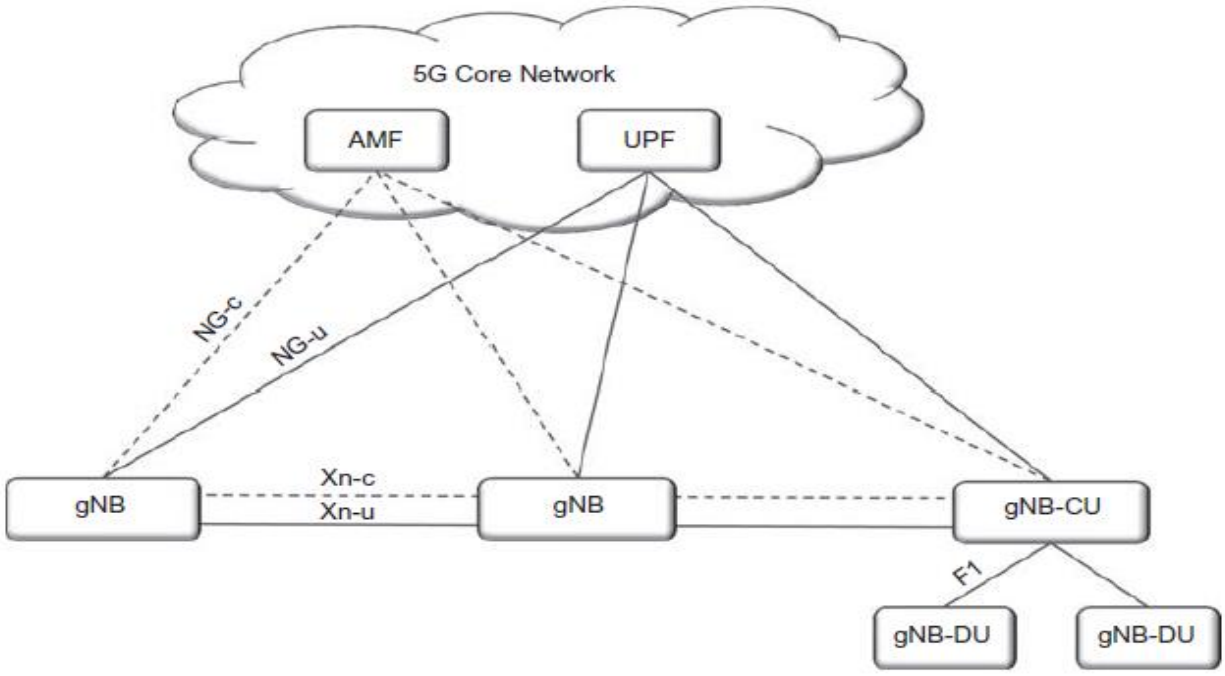


Figure 3. Radio-access network interfaces[11].

## 2.3 Cybersecurity in 5G:

### 2.3.1 Definition and comparison of cybersecurity and information security:

According to NISTIR 7298 Rev. 3[13], cybersecurity and information security are defined as follows:

**Information Security**: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

**Cybersecurity**: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Confidentiality, integrity, and availability are three principles known as the CIA Triad.

**Confidentiality**: which is similar or equivalent to privacy. More clearly, confidentiality means access to resources or data must be restricted to only authorized subjects or entities. Data encryption is a common method of ensuring confidentiality.

**Integrity**: on the other hand, integrity involves maintaining the consistency and accuracy of data over its entire life cycle. Data must not be changed in transit, for example, when it is sent over the Internet or using a local area network, and steps must be taken to ensure that no one or an unauthorized person or subject makes any changes to our data, so it cannot be altered by unauthorized people. It is very common to use hash values for data integrity verification, for example, when you download a new operating system from the Internet. One of the first things to do once the download is ready is to compare the hash values that there are provided by the author of the operating system and the hash value of the downloaded file. They must match to make sure that the integrity is accurate.

**Availability**: Ensuring availability requires maintenance and upgrading of hardware and software and operating system environments. So basically, it is about keeping the business operations up and running, firewalls, proxies, computers everything has to be up and running 24 by 7, 365 days. Now business continuity plans, disaster recovery, redundancy, all those are best practices consider for availability to guarantee that the business is always running.

In summary, cybersecurity focuses on the protection of cyberspace against any sort of crime, but Information Security is a wider field and is the protection of information from any kind, physical or digitalized. Since most of the information nowadays is saved electronically and most of the cyber-attacks are executed to information systems infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, we use the cybersecurity term.

### 2.3.2 A brief history of cybersecurity from 1G to 4G

The fifth generation of telecommunication networks(5G) is revolutionizing the Internet of Things and smart cities, paving the way for a fully connected environment that contributes greatly to economic prosperity. Industrial Internet and smart control systems, autonomous vehicles and drones, life-critical e-health and remote surgery, virtual reality and augmented reality, remote diagnostic and preventive maintenance are just some of the application areas of this new technology. Increasing data transfer speeds, reducing latency, fast network response, and increasing network reliability and stability are just some of the benefits of fifth-generation Internet. However, the emergence of such a powerful technology is not without its security risks; that's why companies are preparing themselves to overcome the challenges of 5G security.
Sensitive data from the organization and customers using the organization's services may be compromised by a 5G-based cyber-attack. Hackers can exploit the high speed and unrecognized vulnerabilities in 5G-based products and the technology's infrastructure to infect IoT equipment and

speed up the spread of malware. Infection of just one IoT gadget can pose a serious security risk to network infrastructure. By controlling IoT equipment, hackers can infiltrate the network, alter information within databases, and disrupt the operation of a data center.
In this chapter, after a brief cybersecurity review in various generations of cellular systems, we will focus on cybersecurity in 5G and the relevant major approaches and challenges, including discussing novel threats.

#### 2.3.2.1 Security in 1G

As we mentioned so far, the first generation (1G) cellular system used analog communication. Due to the vulnerable nature of analog signal processing, it was difficult to provide efficient security services for 1G. For example, eavesdropping was a pressing concern for 1G phones, as it was possible for anyone to listen in to private communication between two users, so there was absolutely no confidentiality in communication in 1G networks. Furthermore, in AMPS and TACS, the identity of the cellphone could easily be duplicated (phone cloning), and all the call charges made from the duplicate phone could be directed to the original owner. Even though the information about the number being dialed could be encrypted, the major problem was the transmission through the air, as signals could easily be received by using any FM receiver since the transmission used frequency modulation. NMT employed voice scrambling at the mobile phone and the base station; this was not a robust encryption method, but it prevented attackers who intercepted calls[5][14].

#### 2.3.2.2 Security in 2G

GSM (the second generation) introduced user authentication and encryption solutions at the radio interface level, unlike the first-generation system. SIM (subscriber identity module), known as a SIM card, is one of the distinguishing features of 2G cellular networks. It is an integrated circuit running a card operating system (COS) that securely stores some subscriber information and is used for proving its identity with the operator and some information about the allowance of access to some services for each specific user. In the GSM authentication procedure, users must prove their identity to a particular operator to be served by offered services. Ciphering takes care of the interception of all the data and signaling. International mobile subscriber identity (IMSIs) and Temporary Mobile Subscriber Identity(TMSI) are used to ensuring that the information is not disclosed to anyone to avoid any intrusion of confidentiality of the user. The SIM card uses symmetric A3 and A8 algorithms to establish a secure connection with the operator to carry out safe communication where the same key is used for encryption and decryption. These algorithms have a one - way function, meaning that output could be found if the inputs are known, but the opposite is impossible. Even if an unauthorized person tries to use the SIM, there is still a PIN code to avoid.

#### 2.3.2.2.1 Entities in GSM authentication procedure:

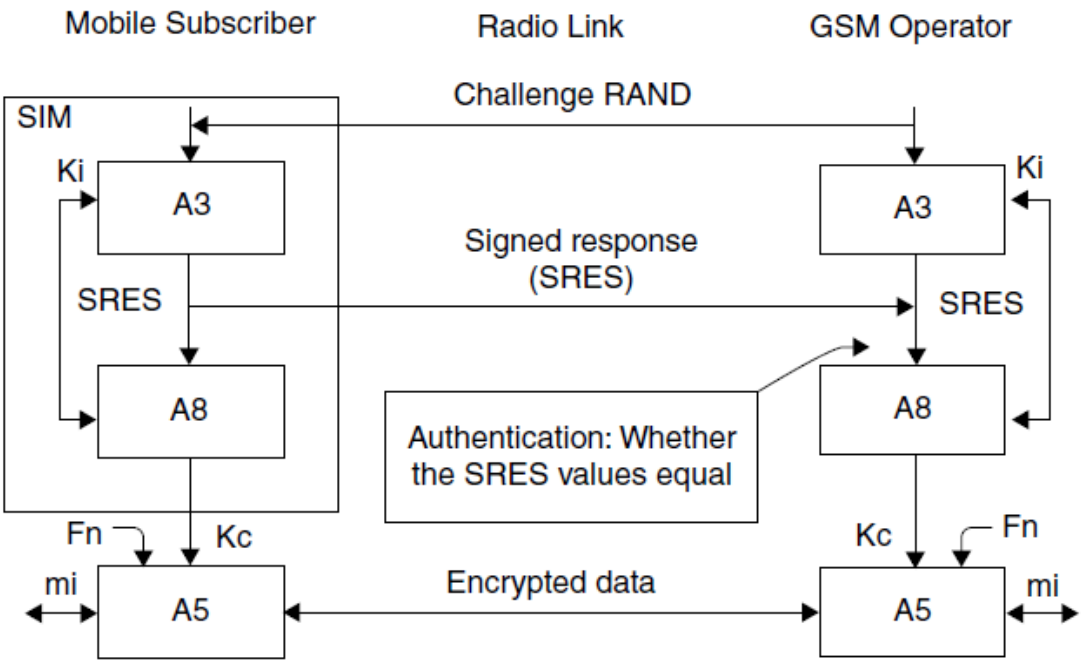


Figure 4. GSM authentication process[5].

##### 2.3.2.2.1.1 A3 algorithm

The A3 authentication algorithm is used in conjunction with $K_i$, the authentication key, and RAND, the random number generated in the AuC (Authentication Centre) to produce the SRES (Signed Response). This variable is used by the network to authenticate a MS (Mobile Station) requesting network resources. First, a subscriber initiates a signaling connection with the network. The Mobile Switching Centre (MSC) sends the International Mobile Subscriber Identity (IMSI) to AuC to requests an authentication triplet from it, which then retrieves $K_i$ of the subscriber and the A3 authentication algorithm based on the subscriber IMSI. Then this 128-bit number (RAND) challenge is transmitted from the network to the subscriber through the air interface. The SIM card processes RAND and the secret 128-bit key $K_i$ through the A3 algorithm to produce a 32-bit signed response (SRES). SRES as the outcome of the A3 algorithm transmitted back to the network from the subscriber again through the air interface. Finally, the AuC compares its SRES value with the received SRES from the subscriber. If the two values match, authentication is considered successful, and the subscriber gets permission to attach to the network. The AuC does not store the copy of SRES but takes the help of the home location register (HLR) or visitor location register (VLR) whenever required[5].

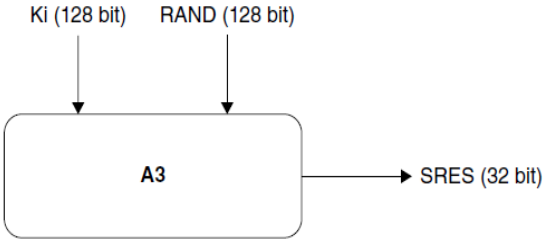


Figure 5. The A3 algorithm[5].

#### 2.3.2.2.1.2 A8 Algorithm

This algorithm uses $K_i$, the authentication key, and RAND (Random Number) to generate $K_c$ (Cipher Key). This is used with A5/X to cipher the data stream between the MS (Mobile Station) and the GSM network[12].

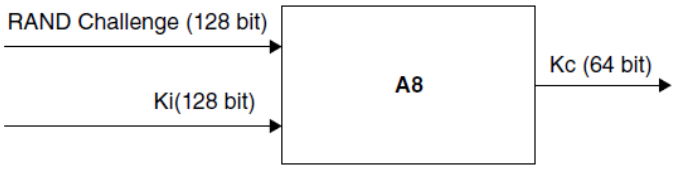


Figure 6. The A8 algorithm[5].

#### 2.3.2.2.1.3 COMP128

COMP128 is technically a hash function that consists of A3 and A8 algorithms in the GSM standard. It is used to provide authentication and helps derive the cipher key (A3/A8).In summary, since A3 and A8 algorithms rely on the same inputs, they are executed simultaneously. COMP128 takes in a 256-bit sequence and gives out a 96-bit output consisting of the SRES and $K_c$[5].

#### 2.3.2.2.1.4 A5 Algorithm

The A5 algorithm is a stream cipher and can be efficiently implemented on a hardware platform. To achieve encryption, $Kc$(64 BIT) and a unique frame number (22-bit) act as input parameters to an A5/$x$ algorithm, where '$x$' denotes a number 1, 2, 3, and so on. The choice of the algorithm depends on the mobile device capabilities (in which the mobile device will let the network know about the algorithm it supports) and laws governing the sale of ciphering algorithms in some countries. A5/1 is the most widely used, mainly in Western Europe and America, while A5/2 is commonly used in Asia. A5/0 is used in so-called third-world countries and countries under UN sanctions, which provides no encryption. The output of the algorithm is a 114-bit sequence that is XORed with a 114-bit sequence of the original data stream. The ciphertext is then sent to the modulator. The frame number changes for every frame transmitted on the air interface[5].

## 2.3.2.3 Security in 3G

3G or UMTS (Universal Mobile Telecommunications), or in particular IMT-2000, supports both packet-switched and circuit-switched data communication.

### 2.3.2.3.1 Security in CDMA2000

In CDMA 2000, authentication and key management (AKA) protocol is used as the security mechanism in two execution stages. The first stage involves the transfer of security credentials (authentication vector, AV) from the home environment (HE) to the serving network (SN). The HE mainly contains the HLR and AC, and the SN consists of the parts of the core network that are directly involved in setting up connections. In terms of access security, the SN network elements of interest are the PDSN, which handles packet-switched traffic, and the circuit-switched nodes VLR/MSC.

### 2.3.2.3.2 Security in UMTS

The UMTS security architecture is in five different sets of features, as mentioned below:

1) **Network access security**: providing secure access for subscribers to the 3G services and protects the radio interface(link) against attacks;

2) **Network domain security**: is a set of features that provides protection against different attacks on the wireline network and also the possibility of exchanging signaling data in a secure manner;
3) **User domain security**: some security features to secure the access to mobile stations;
4) **Application domain security**: provides the possibility of securely exchange messages between applications in the user and provider domain;
5) **Visibility and configurability of security**: provide the possibility of checking the activation status of specific security features.

**2.3.2.3.2.1 UMTS AKA**: is the term given to the mechanism based on challenge-response, which performs authentication and session key distribution in UMTS, IMS, and LTE networks using symmetric cryptography. A challenge-response protocol is a security measure used by one entity to verify the identity of another entity without revealing a secret password shared by the two entities involved. Each entity must prove to the other entity that it knows the password without actually revealing the related information.

## 2.3.2.4 Security in 4G Cellular Systems

With the advent of new technologies, ensuring users' security is also very important. Credentials, identity, certificates, username, and password are used to authenticate different users to access these new technologies.

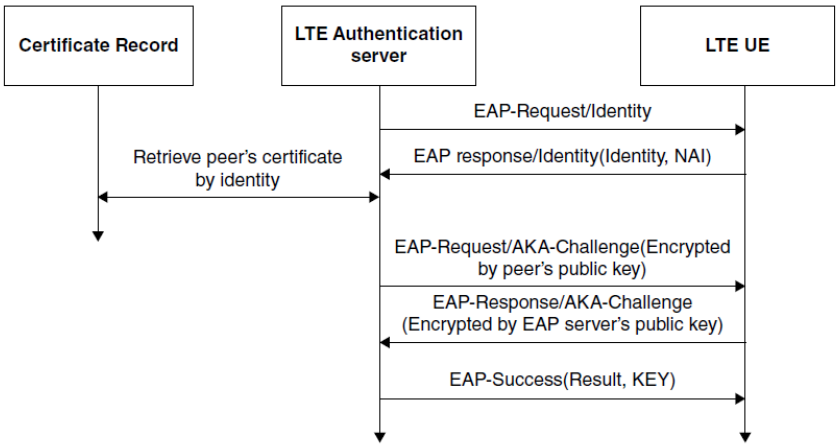


Figure 7. The authentication method of LTE[5].

The authentication process in LTE is started by the authentication server when it sends Enhance Authentication Protocol request/Identity message (EAP) to the UE. The UE responds by a message containing the identity message and Network Access Identifier (NAI). Then the authentication server tries to retrieve the UE's certificate from its records. The authentication server generates the EAP-Request/Authentication and Key Agreement (AKA)-Challenge message using the standard AKA process and sends the EAP-Request/AKA-Challenge message Encrypted by the UE's public key to the UE side. After reception of the mentioned message by UE, it decrypts the EAP Request/AKAChallenge message using its private key then sends the response to the authentication server. The authentication server decrypts the information using the server's private key and verifies the EAP-response/AKAChallenge message using the AKA algorithm. If the message is correct, the EAP server sends the EAP success message to the UE[5].

## 2.3.3 Cybersecurity in 5G

From now on, I will focus on the latest available reports and white papers which concentrate on Cybersecurity in 5G. Following researches are ordered from A to L.

# A

### Security Threats and Protection for 5G

It is obvious that 5G, with its variety of applications and services threat vector for 5G, can be wide, and Motivations to threaten and attack to that would be higher than previous mobile communication networks. The most important motivations which lead the 5G to become the target of criminal activities are state-sponsored political motives, adversaries, organized crime cartels, espionage, and cyberwarfare. Furthermore, the evolution of cryptocurrencies like Bitcoin helped attackers a lot to stay under the blanket and keep gaining financial benefits. The 5G threat vector will have no borders and will range from the end-user equipment such as mobile phones, industrial items, sensors, smart homes, automated vehicles, enterprise networks to mobile networks; therefore, it will be a serious challenge for security practitioners to step up and build a protection system that can defend 5G networks end to end[15].

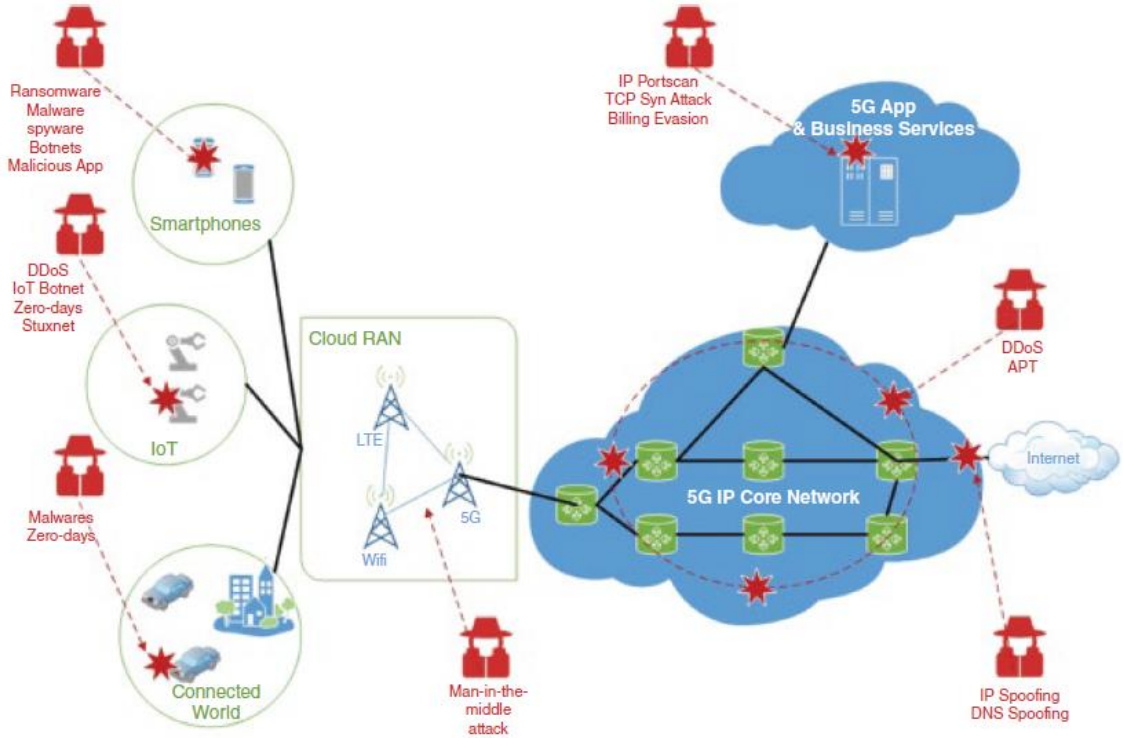


Figure 8. 5G security threat landscape[15]

The current security and privacy solutions to 5G networks are not impressive and, hopefully, unable to handle massive connections. We can clearly visualize a potential scope for developing latency-aware protocols along with security awareness that must consider secure data transmission, end-to-end security, secure and private storage, threats resistant UEs, and valid network and software access.

In this section, we present security and privacy-related challenges and a discussion of security and privacy protocols in the context of 5G networks.

Challenges in security and privacy in 5G networks: Authentication is a vital issue in any network. Due to the zero latency guarantee of 5G networks, authentication of UEs and network devices is very challenging.

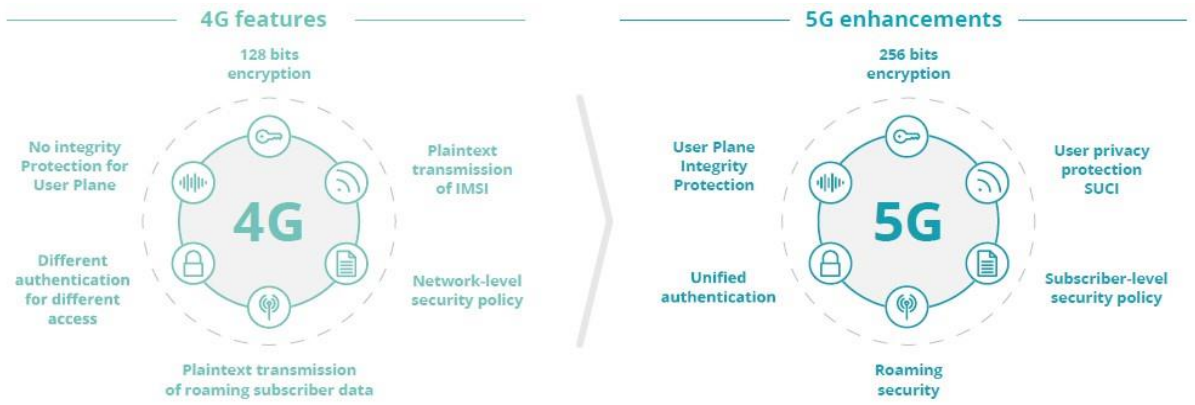


Figure 9. Evolution of different network security features that will be enhanced with 5G[16].

# B

According to [16], ensuring 5G security is all about establishing an effective security management process. This report claims most of 5G attacks would be on four new technology domains:

### Use of Internet technologies:

The 5G network core is built on web resources, where well-known Internet protocols such as HTTP and TLS are used, and 67 percent of web applications contain high-risk vulnerabilities.

### Network slicing:

Nowadays, instead of configuring just one network, operators will have to configure a larger number of slices with greater complexity and service requirements, especially when 5G network infrastructure is built jointly by several operators or when several virtual mobile operators share a single 5G network. Although network slicing is supposed to promote security, increasing the number of slices on a 5G network may lead to more configuration errors and even deterioration of operator awareness, adversely impacting security overall. According to this report, one out of every three successful attacks on 4G networks resulted from the incorrect configuration of equipment.

### SDN and NFV:

Switching to SDN/NFV entails a change in network infrastructure and the appearance of new elements, such as an orchestrator and various control components. Using SDN/NFV reduces the isolation of the networks, increases the risk of sharing resources, and increases access control issues.

### Internet of Things:

The behavior of IoT devices is different from device to device, so the threat model for identifying suspicious activity in the context of a human subscriber will not work for IoT devices, which are the majority of 5G users.

# C

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), had a phased approach in the form of a project[17] to secure cellular networks and, in particular, 5G deployments. This project divides the development of 5G into three phases: Phase 1 - Preparing a Secure 5G Infrastructure & Architecture, Phase 2: Secure 5G Infrastructure &

Architecture, and Future Phases. In each phase, some capabilities are proposed as a roadmap to implement a complete and robust 5G network. The summary of proposed capabilities is listed in the table below.

| Proposed Capability | Phase 1: Preparing a Secure 5G Infrastructure & Architecture | Phase 2: Secure 5G Infrastructure & Architecture | Future Phases |
|---|---|---|---|
| Trusted hardware | X | X | X |
| Isolation and policy enforcement | X | X | X |
| Visibility and compliance | X | X | X |
| VM and container orchestration | | X | X |
| TLS recommended practice | | X | X |
| EPC-based security feature enablement | X | X | X |
| False base station protections | X | X | X |
| Downgrade to legacy technology protections | X | X | X |
| Subscriber privacy | | X | X |
| User plane integrity protection | | X | X |
| CU/DU split | | X | X |
| Authentication enhancements | | X | X |
| Roaming security | | X | X |
| Network exposure function | | X | X |

Table 2. Proposed Capabilities in different development phases of securing 5G

# D

GSMA published a report [18] that provides an overview of the important security topics for the mobile industry. Some of them are mentioned below because of their close relation to this topic.

**Cyber & Operational Security:**
In addition to telecoms infrastructure, there are often a number of corporate information technology systems that enable the broader business operations like the corporate intranet, email, instant messaging, and staff systems such as timesheets and sales systems. Additionally, a range of wider corporate partner connections are often in place to provide access to wider IT and cloud services but also can provide access to the operator network to enable managed service providers. As a result, we have to protect both the operational mobile network and the associated IT. They are a threat vector for cyber-attack because any connection between the corporate systems and the operator network can provide an operational network attack route through associated IT Networks.
Some of the attack vectors presented below:
**Phishing attacks:** Well-engineered and styled phishing attacks continue to have a finite success rate in penetrating perimeter defenses. Consequently, anti-phishing campaigns and well-architected internal network controls making lateral movement more difficult are important activities.

**Malicious Insider / Compromised Access:** Internal controls, least privilege, and strong authentication make it harder for a malicious insider to gain traction.

**Managed Service Provider attack:** Remote compromise of a managed service provider offers a potential attack vector. Strong vetting, least privilege, and trust domains form part of any defense.

**Inter-connect / Roaming / Internet Signalling and DDOS attack:** The exploitation of control signaling is a well-known attack vector that is comprehensively documented.

**Exposed routers and servers:** A network operator will have a significant estate of vendor equipment, router, and server infrastructure. It is important to have a strong grasp of the inventory of equipment so that it can be managed and protected. Additionally, legacy equipment can use protocols with limited in-built security. These exposed interfaces must be configured to secure protocols or have additional security controls such as Virtual Private Network protection. This applies to virtualized deployments in the same sense, in that bare metal compute, storage, and network devices must be protected. Additionally, unused management protocols, internet services, and accounts can be disabled to limit attack opportunities.

**Infrastructure Attack:** Physical attack of network infrastructures, such as at Cell sites or Data Centres, has been seen this year in the UK where conspiracy theorists attacked 5G Mast sites.

**Device attack:** with increasing access bandwidth and a range of malware attacks on the device, protection must be considered against device-based network attacks back into the network.

**Supply Chain** where equipment/software experiences interference in the process of supply/deployment, this also includes where third-party service providers may also be exploited to compromise the network operator.

Strong security controls can significantly reduce the attack surface; all techniques are exploited by phishing attacks, malware, identity theft, malicious insiders, and external attacks via corporate partner arrangements. Good security practices can mitigate this risk through secure networks, strong authentication, least privilege practices alongside strong privileged access management (PAM). In addition, approaches such as Zero trust, Roots of trust, and Trust Domain Separation are also important security concepts.

A security strategy may be composed of multiple layers, as mentioned below.

- Risk-driven bespoke Controls
- Company Security Practices (e.g., company SDLC, Security Practices, Service Introduction Strategy)
- National Regulations
- Industry Best Practice
- Security Standards

**Signalling & Inter-connect:**
The traffic between operators relies on the underlying signaling protocols like SS7(Signaling System No. 7), GTP(GPRS Tunnelling Protocol), BGP(Border Gateway Protocol), and Diameter for effective and secure operation. Therefore, it requires monitoring because if signaling is compromised, integrity, privacy, and service availability are risked. Some legacy signaling threats are listed below:
**legacy signaling threats:**

- Location tracking
- Financial fraud and theft
- Denial of service
- Digital identify theft
- Data, call, email, and SMS intercept

The SEPP(Security Edge Protection Proxy) is a new network function(made for 5G) that protects the home network edge, acting as the security gateway on interconnections between the home network and visited networks. Since 5G still relies on previous generations of telecommunication networks like 2G and 3G, current signaling protocols will remain in use within the industry for many years; as a result, the GSMA recommends that operators implement compensating controls, specifically:

- Guide consumers and enterprises on the risks of using SMS as a multi-factor authentication mechanism

- Implement signaling controls outlined in the GSMA Fraud and Security Group(FASG) guidelines on securing interconnect protocols.
- Have a fraud management system (FMS) to identify, detect and prevent potential fraud transactions within the signaling messages.
- Deploy signaling firewall or similar technologies to support the monitoring and blocking of signaling traffic.
- Prepare for realistic threat scenarios
- Use 5G deployment programs to implement new security specifications such as SEPP and user plane protection
- Use 5G deployment programs to rationalize and close down 2G/3G networks

**Securing 5G:**

Newer and more complex systems like 5G will introduce new vulnerabilities. There has been much focus to identify the critical threats within 5G networks. There is a range of critically sensitive functions identified as follow:

- Virtualisation infrastructure
- Controllers
- Orchestrators
- Internet gateways
- Network slicing
- Mobile Edge Computing
- Routing and switching of IP traffic at the core
- Database functions
- Authentication, access control, and other security functions

5G needs to use current technologies and processes like:

- Apply security considerations identified in the GSMA report.
- Using Network Equipment Security Assurance Scheme (NESAS), which is defined by 3GPP and GSMA. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, and 3GPP defined security test cases for the security evaluation of network equipment.
- Having a zero-trust approach for creating Trust Relationships between trust domains, between and within the system.
- Supply chain risk assessment and product testing
- Using Security Orchestration, Automation and Response (SOAR) and embedding 5G data into protective monitoring capabilities.
- Using Management and network orchestration (MANO) and building of secure templates for server deployments and management. Especially in network slicing, network function virtualization, and container management.
- Considering the cloud security arrangements.
- Consider the whole lifecycle through design, development, procurement, deployment, operations, and decommissioning and implement appropriate security for each stage.

Operators should:

- Build 5G networks that fulfill 5G standards
- Source network equipment from vendors that have demonstrated a commitment to security and an ability to comply with security requirements defined by schemes such as NESAS
- Ensure equipment is deployed at a network level according to 3GPP in its security assurance specifications.
- Try to isolate or close down less secure 2G/3G networks

- Join industry initiatives currently developing the implementation models for 5GC(5G Core) and 5G Non-Stand Alone (NSA) like
- GSMA Fraud and Security Group (FASG) for the development of the Security Edge Protection Proxy (SEPP), secure roaming development through GSMA Networks, and disclosing vulnerabilities impacting the industry by GSMA CVD (Coordinated Vulnerability Disclosure)

# E

In its report [19], Cisco introduced six key cybersecurity recommendations to reducing the attack surface, continuously mitigating threats, and protecting data and privacy.

## Zero Trust

Considering the 5G infrastructure as an untrusted environment and trying to minimize the attack surface by following actions:

**Asset Hardening**: Reduce the attack surface for each asset by following best practices to lock down local access controls, configurations, and services.

**Intrinsic Authentication and Authorization**: Authenticate and authorize access between all entities, considering contextual factors that include user identity, device type, and geographical and/or network access location.

**Multi-Factor Authentication (MFA)**: Using mixed and robust methods to authenticate and authorize user access in addition to contextual factors that include device type and geographical and/or network location.

**Asset Profiling**: allowing or denying access based on assessed risk.(intelligent protection)

**Traffic Encryption**: using robust encryption technologies to secure communications between all properties

## Integrity

Validation of secure development practices, products' trustworthiness, and monitoring different assets integrity to minimize the infrastructure and service tampering like:
**Vendor Security Assessment**: verifying product security through direct assessment and testing the vendor's design and implementation in vendor-managed facilities.
**Secure Boot and Runtime**: guaranty the authenticity and integrity of hardware and software components by using secure boot processes based on anti-tamper to avoid attacks such as buffer overflows and code injection.
**Integrity Assurance**: Interminably monitor hardware and software to validate the integrity and detect tampering issues.
**Operational Integrity**: Detect and prevent insider abuse by implementing appropriate policies, governance, and operational practices.

## Visibility

Providing complete visibility across the infrastructure and repeatedly monitor asset security logs and strange behavior and communications patterns to decrease potential security risks:
**Asset Monitoring**: Enable security tracking, logging, telemetry, and centralized monitoring of all entities.
**Anomaly Analysis**: applying machine learning techniques(system pattern recognition) to monitor and detect anomalous behavior. As decryption of network traffic for threat inspection may impose unacceptable latency or violate privacy requirements, machine learning techniques should be tuned to detect anomalies in encrypted traffic flows as well.

## Segmentation

Implement end-to-end segmentation to partition asset groups, reduce the attack surface, and limit the impact of a compromise.
Key capabilities include:
• **Software-Defined Segmentation:** Place assets into logical security groups that leverage network integrated access controls and policy services to limit communication flows between groups. 5G network slicing features should be leveraged as a component of an end-toend segmentation strategy.
• **Network and Application Firewalls:** Implement firewall gateways to inspect and explicitly allow or deny transactions between critical assets or asset groups.

## Threat Protection

Refers to applying some defensive security controls and continuous monitoring of the whole system with the help of ML techniques to minimize the threat:

- **Vulnerability Management**: Apply international standards and best practices to manage the vulnerabilities and control their surface.
- **Denial-of-Service Defense Systems**: Decreasing network flooding attacks by monitoring the network traffic.
- **Intrusion Detection and Prevention Systems**: A kind of system to monitor and control unauthorized access or attempts to exploit system vulnerabilities.
- **Malicious Traffic Filtering Systems**: the ability to block malicious or unwanted traffic such as spam or attempts to interact with malicious domains and websites.
- **Anti-Malware Systems**: Detects and blocks malware files or malware execution.
- **Security Operations Center**: Rapidly detecting and mitigating security breaches by establishing a centralized security monitoring, incident response, and threat intelligence unit.

# F

5G Americas, as an industry trade organization, published a white paper[20] that specifies the differences between 5G and other wireless architectures, different threats, vulnerabilities, and attacks that are threatening it. This paper looks into threats, Vulnerabilities, and Attacks of both Pre-Full 5G Standalone (LTE and 5G Non-Standalone networks.

## Threats, Vulnerabilities, and Attack of non-standalone 5G:

**Attacks to legacy networks:**

This type of attack allows the attacker to force the LTE-connected UE to switch to legacy networks like 2G and 3G to make it easier to perform man-in-the-middle (MiTM) active attacks and/or passive (e.g., eavesdropping) attacks to collect sensitive information.

**IMSI Tracking (Privacy):**

The IMSI (International Mobile Subscriber Identity) is a unique number that can be captured by software-defined radios (SDRs). Attackers could use it to track higher-value targets which visit secret facilities.

**Man-in-the-Middle Attacks:**

Integrity Protection security algorithms do not adequately protect the Access Stratum (AS) over-the-air User Plane traffic. It refers to a type of attack where a customer's message and/or communication flow could be intercepted in the middle between the UE and the server, so to make it impossible for attackers,

the customer's communication should be protected by end-to-end security encryption protocols (e.g., SSL, TLS, IPSec, VPN, etc.).

**LTE Roaming:**

LTE is dependent on SS7 and Diameter protocols. Many operators have deployed voice over LTE (VoLTE), which uses Session Initiation Protocol / Real-time Transport Protocol (SIP-RTP) instead of SS7. Still, VoLTE is not supported in some areas, so home networks must use SS7 for voice services for that roaming customer. The important point is that Diameter, and SS7 are vulnerable to eavesdropping, including voice calls, reading text messages, and tracking phones. Many operators have implemented SS7 and/or Diameter firewalls, but these firewalls are also subject to several cross-protocol attacks.

## Threats, Vulnerabilities, and Attack of standalone 5G:

**Service-Based Architecture:**

5G network is composed of software that could run on general-purpose hardware that communicates with application programming interfaces (APIs). Therefore the integrity of the software, especially from open-source locations and the overall software supply chain, is an area of vulnerability. As a result, all systems and subsystems must be authenticated with protected communication to prevent unauthorized instructions or unauthorized access to resources.

**SDN:**

5G systems consist of programmable software modules. it's crucial that only authorized entities have the ability to change or program the network by programmability; the provider there must be a way like a verification to control any behavior related to applied policies.

**NFV:**

Opensource software is considered a concern in any environment where it is used. The virtualized elements must communicate with each other in a standardized, API-style environment. Safeguards should be implemented to avoid any threats.

**Hardware and Software Supply Chain:**

**Hardware and Software Supply Chain** are vulnerable areas for most operators and OEMs Original Equipment Manufacturer /ODMs(Original Design Manufacturing). Therefore they need to be viewed with a zero-trust approach from a Network Operations Center perspective that is vertically implemented into the supply chain. So operators and OEMs must be sure they follow best practices towards secure software development and secure the end-to-end supply chain by the corporation of internal and external auditors.

**User Plane Integrity Protection_Man-in-the-Middle :**

Many of the OEMs have not implemented User Plane (UP) Integrity Protection (IP) because it requires considerable computing resources and adds the overhead that directly impacts the user experience in downloading and uploading throughput. Integrity Protection has been enabled on Control Plane messages, but it is still vulnerable because of the segregation of UP and CP. To solve this gap, Some 5G radio OEMs are developing hardware-based encryption acceleration to mitigate the negative impacts on the user's download and upload data experience.

**SUPI/SUCI Privacy:**

Subscription Permanent Identifier (SUPI) is a concept that refers to IMSI in LTE, which was vulnerable to tracking. In 5G Subscription Concealed Identifier (SUCI) is sent over-the-air rather than the SUPI, which prevents an adversary from tracking an important value but it is was not successful in following three scenarios:

1. An emergency call has taken by unauthenticated devices
2. A UE which still uses a legacy SIM that is not compatible with the 5G public key and didn't update via an OTA update
3. mobile subscribers who have their own devices and un-updated SIMs.

**5G NSA and SA Roaming:**

Unlike the vulnerabilities we had in 5G NSA, 5G SA will be considerably different, as HTTP/2 and JavaScript Object Notation (JSON) will be used versus the legacy Diameter protocol.
Voice over New Radio (VoNR) would be a replacement for VoLTE. In 5G, a Security Edge Protection Proxy (SEPP) is used, which will establish a secure, encrypted connection with the roaming partner's SEPP. The SEPPs will then pass HTTP/2 SBA control plane flows for authentication and authorization. For the data flows, there are two options available:
1. Securely between the VPLMN (Visited Public Land Mobile Network) and the HPLMN (Home Public Land Mobile Network) UPFs(User Plane Function) (aka Home Routed)
2. Through the VPLMN's UPF (aka Local Breakout)
the N32 interface is used to pass securely the Control-Plane messages between the VPLMN and HPLMN Security Edge Protection Proxies (SEPPs).in the other hand, The User Plane traffic is carried over GTP-U. But the main issue is For Option (1), the security of user's data traffic is not guaranteed by GTP-U. To overcome this issue, a secured tunnel between VPLMN and HPLMN should be used to maximize the protection of user data flows on the N9 interface.

**5G Security Capabilities:**

In this section, 5G Americas had an overview of some of the most important security capabilities offered by 3GPP standards to improve the security in 5G. The 3GPP SA3 Group has defined the security architecture of 5G mobile networks in specification document TS 33.501.

**Security Functions**

**Enhanced Confidentiality**

In 5G, the base station is logically split in the interface between the CU and DU elements. Security is provided for the CU-DU interface. The DUs are typically deployed at some edge of the network and do not have access to any user data when confidentiality protection is enabled.

**Enhanced Integrity**

As we mentioned so far in the previous generations of mobile networks 5G, mobile architectures did not have a trust model using integrity protection at the User Plane. 5G enables the ability to introduce integrity protection of the User Plane at UE and gNB, but the drawback is that it would add overhead on packet sizes and increases processing load at both the gNB and the UE and results to have lower data rate.

**Enhanced Authentication**

In 5G, the primary protection of UE traffic is assured between the UE and the AMF(Access and Mobility Management Function). Secondary protection is based on Extensible Authentication Protocol(EAP) which is established between the UE and the AAA(Authentication, Authorization, and Accounting) server in external data networks, where the core network element SMF(Session

Management Function) plays the role of an authenticator. AMF triggers primary authentication of the UE using the Subscription Concealed Identifier called SUCI, which is a one-time temporary user identifier. Then, it assigns a 5G-GUTI(Global Unique Temporary Identifier) to the UE and supports reallocating the 5G-GUTI to the UE when necessary (e.g., roaming). This is performed on both 3GPP (e.g., gNB) and non-3GPP (e.g., WiFi) access. The Security Anchor Function (SEAF) at the AMF performs primary authentication procedures and stores the security profile on a per-subscriber basis for the duration of the registration. The IMSI has not managed to keep its name in 5G, as is the case with previous generations of mobile networks. Rather than the IMSI in 5G, the SUPI is used for UE authentication and key agreement. The SUPI is transferred in a ciphertext form over the 5G RAN. Security Edge Protection Proxy performs mutual authentication and negotiation of cipher suites in the roaming network. This prevents third-party operators' devices from tampering with sensitive data such as user IDs exchanged between core networks.

**Enhanced Privacy**

In 5G, subscriber privacy is improved by encryption of subscriber identifier (SUPI). Furthermore, mutual authentication exists between the UE and the network entities. As we mentioned so far, there are a few cases(three cases) where SUPI is sent in the clear. So operators should apply some rules to limit subscribers to use updated with 5G credentials devices.

**Anti-Bidding-down Between Architectures**

ABBA (Anti-Bidding-down Between Architectures) parameter defined in the is 5G to force the UE to use new mechanism for accessing the network instead of old mechanism which had vulnerabilities. This value is defined from 3GPP release 15, which adds new security algorithms to attach to the network. In summary, it is a Parameter that provides anti-bidding down protection of security features against security features introduced in higher release to a lower release and indicates the security features that are enabled in the current network. To ensure forward compatibility, the ABBA parameter is a variable-length parameter. 0x0000 is the value that has been defined for this parameter which means "the Initial set of security features defined for 5GS".

Up to here, we checked out available reports and white papers to specify the 5G threat landscape, and risks, and possible solutions. Then, we will focus on some available published papers on this domain which are published since 2019.

# G

Altaf Shaik et al. in [21] mentioned that device capabilities which are exchanged with the network during the device registration phase are vulnerable to attacks because it is done before the authentication stage without any protection and verification by the network. Consequently, the device capability information can be misused by an adversary to perform several attacks against the mobile subscriber. They classified threats into three groups: identification attacks(which allows the attacker to discover devices on the mobile network and reveal their hardware and software characteristics such as model, manufacturer, version, and applications running on them), bidding down attacks(which allows the attacker to force the device to operate with lower data rate, denying the UE to use VoLTE services and also forces the UE to operate only in 3G/2G ), and battery drain attacks(which targets NB-IoT and LTE-M devices to breakdown their power-saving abilities and drain their battery life five times faster than the expected lifetime).

Discovered threats and possible solutions could be found in the table below:

| Vulnerability | Problem in | Impact | Mitigation |
|---|---|---|---|
| UE capabilities are accessible without authentication | 3GPP LTE protocols | Identification of devices (Model, OS) | Mandatory security protection for UE capabilities |
| UE radio capabilities could be accessed before security setup | operator's eNodeB Configuration or implementation | decreases the data rate, downgrades to 3G/2G for voice calls | |
| UE (NB-IoT) core capabilities are not protected | 3GPP LTE protocols | Increases the power consumption on the device | Core network capabilities mutually verified after NAS security setup |

Table 3. Threats in 5G and their Mitigations[21].

# H

Ijaz Ahmad et al. in[22] highlight the present and future security challenges in wireless networks, mainly in 5G, and future directions to secure wireless networks beyond 5G. According to this paper, affected areas by different threads are divided into three segments 1) access networks, 2) backhaul network, and 3) the core network. Security threats of these segments are listed in the table below.

| Security threats | Potential targets | Affected network segments | | |
|---|---|---|---|---|
| | | HetNet Access | Backhaul | Core Network |
| DoS attack on signaling plane | Centralized control elements | | | ✓ |
| Hijacking attacks | SDN controller, hypervisor | ✓ | ✓ | |
| Signaling storms | 5G core network elements | | | ✓ |
| Un-authorized access | Low-power access points | ✓ | | |
| Configuration attacks | Low-power access points | ✓ | | |
| Saturation attacks | Ping-pong behavior in access points, and MME | ✓ | | ✓ |
| Penetration attacks | Subscriber information | | | ✓ |
| User identity theft | User information data bases | | | ✓ |
| Man-in-the middle attack | Un-encrypted channels, e.g. in IoT | ✓ | | |
| TCP level attacks | Gateways, router and switches | | ✓ | |
| Key exposure | Radio interfaces | ✓ | | |
| Session replay attacks | Session keys in non-3GPP access | ✓ | | |
| Reset and IP spoofing | Control channels | ✓ | | |
| Scanning attacks | Radio interfaces interfaces | ✓ | | |
| IMSI catching attacks | Roaming and UE | ✓ | | |
| Jamming attacks | Wireless channels | ✓ | | |
| Channel prediction attacks | Radio interfaces | ✓ | | |
| Active eavesdropping | Control channels | ✓ | | ✓ |
| Passive eavesdropping | Control channels | ✓ | | ✓ |
| NAS signaling storms | Bearer activation in core network elements | | | ✓ |
| Traffic bursts by IoT | Saturation of GTP end-points | | ✓ | ✓ |

Table 4. Security challenges in 5G network segments[22].

The table below lists a list of available threats and technologies which are suffering from these threats. More detailed descriptions of available threats of each specific technology have been listed in [23].

| Security Threat | Target Point/Network Element | Effected Technology | | | |
|---|---|---|---|---|---|
| | | SDN | NFV | Cloud | MIMO |
| DoS attack | Centralized control elements | ✓ | ✓ | ✓ | |
| Hijacking attacks | SDN controller, hypervisor | ✓ | ✓ | | |
| Signaling storms | 5G core network elements | | | ✓ | |
| Resource (slice) theft | Hypervisor, shared cloud resources | | ✓ | ✓ | |
| Configuration attacks | SDN (virtual) switches, routers | ✓ | ✓ | | |
| Saturation attacks | SDN controller and switches | ✓ | | | |
| Penetration attacks | Virtual resources, clouds | ✓ | | ✓ | |
| User identity theft | User information data bases | | | ✓ | |
| SPIDAS DoS attacks | Cyber-Physical clouds | | | ✓ | |
| TCP level attacks | SDN controller-switch communication | ✓ | | | |
| Man-in-the-middle attack | SDN controller-switch communication | ✓ | | | |
| Reset and IP spoofing | Control channels | ✓ | | | |
| Scanning attacks | SDN controller interfaces | ✓ | | | |
| Insider attacks | Cloud and virtual systems | | ✓ | ✓ | |
| Data leakage | Cloud storage systems | | | ✓ | |
| Cloud intrusion | Overall cloud systems | | | ✓ | |
| Active eavesdropping | Control channels | ✓ | | | ✓ |
| Passive eavesdropping | Control channels | ✓ | | | ✓ |
| VM manipulation | Clouds and virtual systems | | ✓ | ✓ | |

Table 5. Security challenges in key 5g technologies[23].

Finally, they have listed possible solutions to the presented threats in table 6.

| Solution | Security type | Effected Technology | | | |
|---|---|---|---|---|---|
| | | SDN | NFV | Cloud | MIMO |
| Controller Replication | Control plane security through scalability | ✓ | | | |
| SEFloodlight | Control plane access authorization | ✓ | | | |
| DoS detection | DoS and DDoS detection techniques | ✓ | | ✓ | |
| NetServ | Self-protection of control plane from DoS attacks | ✓ | ✓ | ✓ | |
| FRESCO | Composable security for SDN | ✓ | | | |
| PermOF | Application authorization in SDN | ✓ | | | |
| FlowChecker | Flow rules verification in SDN switches | ✓ | | | |
| VeriFlow | Flow rules verification in SDN switches | ✓ | | | |
| Flow admission | Flow-based access control in SDN | ✓ | | | |
| Resonance | Control access to SDN and core network elements | ✓ | | | |
| Splendid Isolation | Ensures traffic isolation for VNFs and virtual slices | | ✓ | | |
| TLS protocol | Provide security to control channels | ✓ | | | |
| IBC protocol | Provide security to control channels | ✓ | | | |
| Capacity sharing | Security in sharing of resources | ✓ | | ✓ | |
| DDoS Defender | Defence from IP spoofing and DDoS | ✓ | | ✓ | |
| OpenHIP | User identity verification for roaming and clouds services | ✓ | | ✓ | |
| ECOS | Privacy and trust in offloading | ✓ | | | |
| OF-RHM | Ensure identity security of users | ✓ | | | |
| mMIMO security | Active attack detection methods | | | | ✓ |
| OSPR | Active eavesdropping detection | | | | ✓ |
| Physical layer security | Passive eavesdropping detection | | | | ✓ |
| Security principles | NFV security challenges and best practices | | ✓ | | |
| Policy manager | NFV security configurations | | ✓ | | |
| Xoar | NFV and VM security platform | | ✓ | | |
| OpenVirteX | NFV hypervisor security | | ✓ | | |
| SecMANO | NFV orchestration and MVNO security | | ✓ | | |
| NFVITP | MVNO security principles and practices | ✓ | ✓ | | |
| Security proposals | Integrity verification, security of data and storage systems | | | ✓ | |
| ENDER | HX-DoS mitigation Security for cloud web services | | | ✓ | |
| Secure protocol | Service-based access control security | ✓ | | ✓ | |
| CSA proposal | Cloud Security Alliance (CSA) proposal for security | | | ✓ | |

Table 6. Security solutions for key 5g technologies[23].

# I.

Rabia Khan et al.in[24] have looked at this area more broadly. They have divided threats domains into seven domains, including Network Slicing, Access Network, DoS Attack, MEC (Mobile edge computing), Latency, and Consistent User Experience. Different available threats to these domains and possible recommendations are listed in the table below.

| Domain | Threats | Recommendations |
|---|---|---|
| **Network Slicing** | Communication between inter-network slices is not secure. | Controlled and secure communication between all slices, function and interfaces between them. |
| | Impersonation attack against physical host platform and network slice manager. | Mutual authentication between host platform and network slice manager. |
| | Within an operator network impersonation attack against a Network Slice instance. | Authenticity and integrity of Network Slice instance need to be verified. |
| | Within an operator network impersonation attack against multiple Network Slice Managers. | Mutual authentication between all Network Slice Managers. |
| | Variance of policies and protocols for different slices. | Proper isolation between slices and separate authentication of each slice for a UE or authentication at a lower security slice. |
| | Denial of service attack to other slices. | Capping for slices individually for provisioning maximum resources. |
| | Affect of other slices' resources exhaustion. | Ring-fencing provide flexibility to run in all conditions. |
| | Side channel attacks due to same set of primary hardware. | Avoid co-hosting with different level of sensitivity and strong isolation of virtual machines. |
| | Combination of vitualized and regular function in a hybrid deployment model offers new threats. | Maintenance of same 5G security level. |
| | Service for UE with multiple slices at the same time provides risk of security. | Sealing between slices with a security mechanism in both UE and network. |
| **Access Network** | Expected high traffic either malicious or accidental. | Reduce traffic changers whenever possible and be flexible for maintaining system performance. |
| | Risk of key leakage between operator's links. | Strong security link between operators or a new method for key sharing. |
| | Optional security implementation offers security threat. | Study for mandating security. |
| | Subscriber device level security in 5G due to roaming routed IP traffic in 5G. | Virtualization and network slicing. |
| **DoS Attack** | Exhaustion of signaling plane with a number of devices that gain access simultaneously. | Stop new unknown access through access control when network is exhausted or check the novelty and standardization of signal patter and requires to find a new method to overcome DOS attack. |
| | Exhaustion of signaling plane with a number of simultaneously and intermittently data transfer devices. | Avoid time synchronized data transfer, Use of analytical techniques for consistent and persistent communication devices, access control and designing of new techniques. |
| | Stopping services for a number of devices due to traffic overload is sometimes a trick by an attacker. | Series of overload defenses, defense overload mechanism and designing of new mechanism that limits services for the problematic devices. |
| | Bulk configuration leading to bulk provisioning. | Analytical techniques like anomaly detection. |
| **MEC** | MEC deployment billing risk. | Periodic polling from UE to core network to cross check received charging records from edge. A new or similar mechanism like that of 3GPP. |
| | MEC applications run on the same platform of network function. | A new framework for either providing access to only trusted MEC devices or making MEC and network operator independent of trust. |
| | Influence on network by an allowed third party. | Network operators must limit network distortion to a certain level. |
| | Providing security service to a third party. | Expose security services to trusted applications only. |
| | MEC environment user plane attacks. | It is required to carefully study the scenario specially in case of a number of caches and new architecture. |
| | Sensitive security assets on Edge. | Proper encryption, assurance of security, protection of decryption keys. |
| | Exchange of data between Edge and Core. | Encryption of the sensitive asset. |
| | Trust establishment between the edge and the core functions. | Authentication between communication resources. |
| | MEC Orchestrator communication security. | Guarantee of the security level as per recognized scheme. |
| | Multiple new nodes, RD and many LI points will raise security risk. | Follow strong physical security and identified method of implementation and location for LI/RD functionality. |
| **Latency** | Security mechanism for latency targets. | Changes in 3GPP architecture, moving encryption operation to lower layer, dropped user plane security, use a fast stream cipher. |
| | Subscriber authentication within visited network. | Re-use of old SA (Security Association) for low latency at user plane and high latency at signalling plane and Delegating DSS (Distributed Subscriber Server) from HSS (Home Subscriber Server) to visited network by a key "Ki" for subscribers' authentication. |
| | Re-authentication request for the loss of service on a user plane. | No critical path on user plane and no strict bound between user plane and control plane. |
| **Consistent User Experience** | Credentials to IMS (Internet protocol Multimedia Subsystem) and 3GPP network access. | Prevent credentials at required level of security. |
| | Access for non-3GPP network. | Authentication, key agreement, if untrusted access then set up authentication process between UE and the core. |
| | Weak security for less trusted 3GPP network access. | Security must be provide by home network between UE and core network. |
| | Secure interfaces between UE and non-3GPP radio access points. | UEs and 3GPP servers must have the capability to derive the credential and to mannage these credentials. |

Table 7. Security threats and recommendations[24]

In addition, they have listed and took a review of threats present in the IoT field (Internet of Things) as follows.

| Technology | Challenge/Threat | Solutions |
|---|---|---|
| IoT Smart water system | •Cyber-attacks.<br>•Epidemic attack.<br>•Faults and destructive attacks.<br>• Security and Privatized Security. | •ABA-IDS algorithm |
| IoT security component | •Authentication.<br>•Authorization. | •OAuth 2.0-based oneM2M component |
| General IoT | •Eavesdropper collusion. | •PLS. |
| IoT environment | •Dolev-Yao threat. | •Signature-based AKA scheme. |
| SDN based IoT-Fog | •MitM | •Blood filter method |
| Industrial Mobile-IoT | •Malware. | •Dynamic, static, and hybrid analysis. |

Table 8. Available threats in IoT[24]

Furthermore, security issues related to key technologies(SDN/SDMN, NFV, MEC, and Network Slicing)of 5G were also reviewed. More details are discussed in previous pages.

# J

Shane Fonyi in[25] has addressed broken down the 5G vulnerabilities into three sections: Confidentiality, Integrity, and Availability (known as CIA).

| Security Principle | Threat | Impact |
|---|---|---|
| Confidentiality | • AKA Attack<br>• Unsecured DNS Paging Broadcast | • Spoofing<br>• Malware dropping MITM<br>• Location Determination |
| Integrity | • Silent Downgrade<br>• AKA Attack | • Phone/SMS snooping<br>• Subscriber Impersonation |
| Availability | • Spectrum Slicing Attack<br>• Botnet Attack Paging Attack | • Performance Degradation<br>• Denial of Service |

Table 9. 5G vulnerabilities and related threats[25].

In addition to traditional techniques to securing the 5G, which rely on cryptographic algorithms at upper layers of the protocol stack, there is another technique known as PLS(physical-layer security), which takes advantage of the characteristics of wireless channels to degrade the received signal qualities at the malicious users and realize secure keyless transmission via signal design and signal processing techniques. Three main differences of PLS approach compared to cryptographic approaches are as follows:

- The achieved security does not rely on encryption and decryption
- Can realize flexible configurations of security levels
- Only need to perform simple signal processing, with little overhead

The major physical layer security approaches are summarized in the table below.

| PLS Approach | Anti Eavesdropping Mechanism | Required CSI(channel state information) at Transmitter | Additional Overhead | Implementation Complexity |
|---|---|---|---|---|
| Artificial noise injection | Exploitation of noise | Instantaneous | CSI feedback, additional power | Moderate |
| Anti-eavesdropping signal design | Exploitation of interference Instantaneous | Instantaneous | CSI exchange | High |
| Secure beamforming/ precoding | Exploitation of fading and noise | Instantaneous | Multi-antenna structure, CSI feedback | Moderate |
| Cooperative jamming | Exploitation of noise | Not necessary | Additional power, dedicated helper | Moderate |
| Relay selection | Exploitation of fading | Not necessary | Additional power, dedicated helper | Moderate |
| Cooperative secrecy enhancement | Exploitation of interference and noise | Instantaneous/ Not necessary | Data and (or) CSI exchange | High |
| Power control and resource allocation | Exploitation of fading | Instantaneous | CSI feedback | Moderate |

Table 10. The major physical layer security approaches[25].

PLC solutions also have some drawbacks, which are detailed below:

1) Most of the existing PLS techniques try to guarantee security via exploiting noise, fading, and interference. 5G acts as a multi-level multi-user system, and its behavior depends on both properties of the individual links and interaction among users and sub-networks. Furthermore, Yet, it is still unclear how these mechanisms will act as an anti-eavesdropping resource.

2) The PLS techniques developed focusing on the optimization of the secrecy rate or secrecy outage performance of the system, but different services have different quality-of-service (QoS) needs in 5G, which implies that the PLS protocols should jointly consider various aspects of user demands such as delay, reliability, throughput, and secrecy which It seems impossible.
3) Particularly, To implement the Artificial Noise Injection method, additional power is consumed; for secure beamforming/precoding schemes, multi-antenna configuration is required at the transmitter /to send jamming signals for Cooperative jamming approach, dedicated nodes have to be deployed in the networks. Since most of IoT devices have very simple functionalities and need very limited power, storage, and processing capabilities, therefore, most of the existing PLS solutions cannot be directly applied in IoT communications.

# K

Jin Cao et al. in [26] reviewed the security vulnerability in the 5G Access Procedure as follows:

Vulnerability in the 5G Access Procedure:

1) **Disclosure of the identifiers shall enable various privacy attacks*:*** as we mentioned so far, 5G security adopts temporary identifiers 5G-Globally Unique Temporary Identity (5G-GUTI) and the Subscription Concealed Identifier (SUCI) to protect the SUPI, but it seems there are some worries bout the identifiers. Firstly, when the temporary value 5G-GUTI, which has no change for a long time, shall also cause the disclosure of IMSI. Secondly, unlike the LTE-A system, when the AMF sends an Identity Request message to the UE, the UE shall respond with the SUCI, which contains the concealed SUPI. However, in case of an emergency situation, the UE shall still send the SUPI directly in the Identifier Response message; the identifier confidentiality shall not be guaranteed.

*2)* **5G-AKA cannot avoid Denial of Service (DoS) attack**: Upon receiving the Identifier Request message, the UE shall respond with the SUCI. If the rogue base station sends multiple Identifier Request messages, the UE has to consume its overheads to respond to it and run out of UE's resources. In addition, If the SEAF receives a valid 5G-GUTI, the SEAF shall contain the corresponding SUPI in the authentication request message. Otherwise, the SEAF will forward the SUCI and makes it is easy for an adversary to launch DoS attacks to the SEAF, the AUSF, and UDM/Authentication credential Repository and Processing Function (ARPF)/Subscription Identifier De-concealing Function (SIDF).

3) **Similar to the EPS-AKA, in 5G-AKA:** since the visited network and the home network require a strong trust relationship for the 5GS, the authentication processes are required not only between the visited network and the home network but also among service parties in 5G wireless networks. With the emerging of heterogeneous networks in 3GPP 5G architecture, the complete trust relationship between them seems impossible and difficult to implement. Additionally the leakage of the long-term secret key would cause serious problems to the whole network For example, the long-term key K may have been leaked during the production phase of the USIM card. Just by having a long-term secret key, an adversary can obtain the shared key to further wiretap the communication channels or to perform man-in-the-middle attacks, impersonation attacks, and so on. That's why 3GPP has set up a project on long-term key updates to try to solve this problem, but there is no final conclusion.

4) **Traceability attack**: In case of the failure in authentication procedure two different types of error messages (MAC_FAIL, SYNC_FAIL) may be sent to the SEAF. An attacker simply by captures a legal authentication request message (RAND, AUTN) sent to the UE and binding it to the UE. If the attacker receives the SYNC_FAIL message, it can be determined that the UE to be tracked is in a specific area.

5) **AKA missing key confirmation attacks in 5G-AKA/EAP:** During 5G-AKA/EAP-AKA authentication prodecure there could be two vulnerabilities Firstly, the 3GPP committee has specified that the serving network can initiate Key-change-on-the-fly, and thus an attacker could forge as a legitimate base station observing network to modify the session key after the execution of the 5G-AKA/EAP-AKA. Secondly, in order to prevent attackers from counterfeiting the serving network, the key $K_{SEAF}$ is bound to the serving network identity. However, since the key $K_{SEAF}$ may not be used in some special scenarios, for example, subscribers use the presence of SNs for making sensible decisions, it is feasible for an attacker to impersonate as a legal serving network.

6) **Similar to 4G-AKA:** When a cellular device is not actively communicating with a base station, it enters an idle, low-energy mode to conserve battery power. Consequently, When there is a phone call or an SMS message for the device, it needs to be notified by this is achieved

by the paging protocol. The paging mechanism could be a target of an attack known as ToRPEDO (short for TRacking via Paging mEssage DistributiOn) in which attackers inject fake paging messages and mount denial-of-service (DoS) attacks.

7) **IMSI-cracking attack in 5G-AKA:** another attack enabled by ToRPEDO is the IMSI-Cracking attack which allows an adversary to fully uncover the victim's unique International Mobile Subscriber Identity (IMSI) number if the phone number is known. simply by launching a brute-force attack, it is possible to retrieve the victim's IMSI in less than 13 hours.

## Security Solutions of 5G Access Procedure:

In this section, they had a review of some existing solutions to the above issues.
A USIM compatible 5G-AKA protocol has been proposed in which the Diffie-Hellman (DH) key exchange protocol is embedded in the 5G-AKA protocol. In this procedure, the generation of the session key depends on not only the long-term secret key, but also the ephemeral DH parameters. Even if the long-term secret key is compromised, it is infeasible for an adversary to obtain the shared key. Thus, this scheme can achieve Perfect Forward Secrecy (PFS) and resist against passive attacks simultaneously. It should be noticed that it costs some computational and communication overheads for mobile devices because of resource limitations.
Similarly, another scheme can withstand the identifiers disclosure by encrypting the identifiers with the encrypted key and replay attacks using one-time random numbers and Message Authentication Code (MAC). Additionally, in this scheme, these two different authentication failure messages (MAC_FAIL, SYNC_FAIL) are sent to the SEAF in the same format and are encrypted with the encryption key $K_E$ calculated from the DH key. so, this scheme can avoid traceability attacks.
By introducing the blockchain-based distribution trust architecture in the access process, it can save a large number of signaling and connection costs. A cross-layer authentication scheme for ultra-dense 5G HetNet based on channel information and EAP-AKA protocol is proposed in which when a UE wants to access the network, the EAP-AKA authentication protocol is first adopted to perform the initial authentication. After the initial authentication is completed successfully, the proposed physical layer authentication scheme is employed. This mechanism can reduce the time delay and computation complexity and satisfy the strong security requirement. Moreover, a lightweight authentication scheme is also proposed such that by combining the traditional lightweight authentication with the cross-layer access authentication mechanism, the scheme can achieve fast authentication and minimize the packet transmission overheads without compromising the security requirements simultaneously. The access control scheme based on a Simple Public Key Infrastructure (SPKI) certificate based on a multilayer communication architecture designed for 5G networks. In this scheme, by taking advantage of the Zero Knowledge Proof (ZKP) scheme, the verifier signs the authorization certificate and sends it to the device. Then UE first collects the physical information and generates the fingerprint parameters which would be used to randomize the parameters used in the AKA protocol. Subsequently, with the aid of the fingerprint parameters, an enhanced AKA protocol is performed. Since the fingerprint parameters are used to masquerade the important parameters in the handover authentication scheme, the scheme can avoid man-in-the-middle attacks, impersonation attacks, etc. Besides, the author introduces the concept of the radio trusted zone database, and thus the computation complexity can be largely reduced. Then two simple solutions in order to withstand the missing key confirmation attacks in 5G-AKA are proposed. Firstly, a MAC with a key derived from $K_{SEAF}$ can be added at the very end of the protocol. Secondly, by binding linear to SN identity, subscribers can acknowledge that the HN has committed to a specific Serving Network(SN) identity without using $K_{SEAF}$[26].

# L.

Chafika Benzaïd et al. in their research on Trust in 5G and Beyond Networks[27] had a look at the trust concept in 5G and beyond networks and its dimensions and grouped them into six domains, including Trust in Communications, Trust in VNF, Trust in Management and Orchestration, Trust in NF V Infrastructure, Trust in AI/ML Models, Trust in Data and Trust in Services and Applications. They have Summarized trust dimensions and related security threats and Potential Security Measures as the table below. Then they advocated some emerging enablements (e.g., blockchain, trusted platforms, big data analytics) that can be used to improve the trust in a 5G and beyond ecosystem.

| **Trust Dimension** | **Potential Security Threats** | **Potential Security Measures** | **Emerging Enabler** |
|---|---|---|---|
| Communication | - Spoofing<br>- DDoS<br>- MITM<br>- Message reply<br>- Eavesdropping<br>- API abuses | - Authentication and authorization controls | Blockchain |
| | | - Encrypted transmission services (e.g., TLS) | Trusted platforms (Protect encryption keys) |
| | | - Throttling/rate limiting APIs usage | Behavioral & Big data analytics |
| VNF | - Privilege escalation<br>- Escape isolation<br>- Data exposure and exploitation<br>- Malware dissemination<br>- DDoS attacks | - VNF software validation (authenticity and integrity) | Blockchain |
| | | - VNF software certification (quality and security tests) | Behavioral & Big data analytics |
| | | - VNF instance identify assurance | Blockchain |
| | | - VNF instance's behavior and performance monitoring monitoring | Behavioral & Big data analytics |
| NFVI | - Isolation failure<br>- Introspection attacks | - Secured boot<br>- Measured boot | Trusted platforms |
| MANO | - Impersonation<br>- DDoS (resource depletion) | - Identity and integrity mechanisms | Blockchain |
| | | - Continuous assessment of MANO's activities and resiliency to attacks | Behavioral & Big data analytics |
| | | - Redundancy procedures | |
| AI/ML | - Incorrect patterns learning<br>- Wrong decision making<br>- Sensitive data leakage | - Explainable AI | |
| | | - Privacy-preserving AI | |
| | | - AI/ML models resilient to adversarial attacks | Blockchain (Prevent poisoning attacks) |
| Data | - Manipulated and inaccurate data | - Data quality (accuracy, completeness, timeliness, validity, consistency) | |
| | | - Data provenance (track its sources and derivation history)<br>- Data security (integrity checks) | Blockchain |
| Applications & Services | - Endanger user safety<br>- Impact network security (e.g., DoS)<br>- Data security and privacy violation | - Continuous monitoring and assessment of QoS and QoE | Behavioral & Big data analytics |
| | | - Application/service integrity check | Blockchain |
| | | - Authentication and authorization mechanisms | Blockchain |
| | | - Quality and security assurance tests | Behavioral & Big data analytics |
| | | - Audit trails on use of PII | Blockchain |

Table 11. Trust dimensions and related security threats and Potential Security Measures[27].

In their research, they present the blockchain as an enabler for guaranteeing the integrity of data. The main reason for choosing the blockchain instead of cryptographic algorithms their reliance on trust in a third party for public/private key generation. Because if the key generator is compromised, the whole system will be compromised.

Finally, by using ML algorithms and a data source, they analyzed the data access time with and without the use of blockchain for varied numbers of chunks and different hashing algorithms (i.e., MD5, SHA256, and SHA512). And the results show that while the access time increases with the increase in the number of chunks of data, blockchain had a significant impact on the access time. Furthermore, the

access time is also affected by the hashing algorithm used. In fact, the more robust the hashing algorithm is, the longer the hashing time will be[27].

# Chapter 3

# Risk management in Cybersecurity of 5G

The NATO Cooperative Cyber Defence Centre of Excellence in [28] written by Luiz A. DaSilva et al. outlines measures that governments, and in particular the NATO Alliance, should put in place for risk assessment and the certification of secure 5G components and systems. The introduction of 5G, besides its advancements on previous generations of cellular technology by improving the bandwidth, capacity, latency, and reliability of mobile broadband services, creates the potential threat surface for new security attacks. This article proposed some recommendations as follows:

### A. International Partnership for Risk Assessment and Product Testing

Countries must conduct a risk assessment of their security processes and adopt advanced security measures to ensure the successful deployment of 5G. NATO and the Allies must each develop a strategy to ensure security by design for 5G beyond infrastructure deployment. Develop a framework for assessment, mitigation, and management of the range of risks to 5G networks.

### B. Cyber Threat Intelligence Sharing

Organizations should be swift in responding to a cyber threat require the fast sharing of relevant information by them. Sharing of relevant information should be done through an Information Sharing and Analysis Centre (ISAC) with the help of a blockchain-based manner like Mission Partner Environment (MPE). The MPE is empowered by blockchain private channels that allow the exchange of unclassified information between unclassified and classified networks.

### C. Expansion of Standardisation to the 5G Ecosystem

Although 3GPP provides 5G infrastructure security specifications, there is a need for different standard bodies at the intersection of 5G and technologies such as blockchain, IoT, and autonomy.
These efforts have to benefit from government funding to realizing:
(i) standards-compliant network;
(ii) innovation support for start-up companies;
(iii) international collaboration and partnerships that create joint academic and research programs focused on 5G;
(iv) participation in standards bodies responsible for 5G and related technologies;
(v) exchange programs among leading research universities.

Royal United Services Institute for Defence and Security Studies, in their paper[29]which has written by James Sullivan and Rebecca Lucas, identified three principal risks to 5G networks for policymakers:

### Risk 1: Supply chain complexity.

In this category, three conditions are proposed which should be applied in the supply chain of the primary vendor and all companies to ensure a high degree of confidence in the equipment produced by them.
The vendors should have an effective quality control process to find accidental or deliberate security vulnerabilities.
The vendor regularly screens all employees to identify anyone who could tamper with the equipment.
The vendor has physical and information security measures in place that protect unauthorized access to its intellectual property and processes.

### Risk 2: An increased attack surface and attack opportunities.

Even if a vendor could provide more trustworthiness in its equipment, 5G brought more risks than previous generations. Larger physical and virtual attack surfaces, the physical disaggregation of network components, the number of devices connected to the network, and the frequency of software patching and vulnerabilities in legacy networks are potential risks of using 5G networks. Just as an example, although the 5G would be the best cornerstone of the Internet of Things(IoT), we have to consider that usually, these systems are coming to the market with weak security and authentication measures. So it shows that these systems rely on software updates and patches and will increase the number of attacks like distributed denial of service (DDoS) attacks.

### Risk 3: Lack of vendor diversity.

The small number of vendors and lack of diversity in the 5G market is another topic that should be pointed out. Huawei, Ericsson, Nokia, and ZTE are the only providers of RAN equipment in mainland Europe. Consequently, these vendors may have too much leverage to offer their products. There is also a risk that vendor-specific vulnerabilities could easily spread across the whole network. Therefore, a blanket ban on one could increase the cyber risk to 5G networks and reduce vendor competition.

To control and mitigate the above-mentioned risks, they have proposed various measures which have to take place.

### Measure 1: Resilient network architecture.

5G networks should be designed with defense-in-depth and an emphasis on resilience. To fulfill this requirement, regulators and operators sould take o account two important considerations: network segmentation and redundancy. Network segmentation refers to measures that prevent attackers from moving between different layers; they can make it much more difficult, time-consuming, and resource-intensive. On the other hand, redundancy ensures the network's consistent availability. it means network equipment mustn't rely on a single vendor's products because it makes it easier to spot unusual behavior from one particular vendor. In the longer term, governments should think about increasing network diversity. Initiatives promoting interoperability, such as OpenRAN, may also help lower barriers to market entry. OpenRAN is a group of companies trying to make it technically possible for different vendors' equipment to interoperate in the RAN, but it has its own challenges, such as it may not yet be economically viable and it will take a long time to achieve.

### Measure 2: Access management.

Access controls could include supervising vendors while they are in the network and have remote access or providing maintenance or while they are performing patching support of original product and etc. In this case, limiting the amount of time that vendors access the network could be beneficial. In summary, the operator's inability to monitor any vendors' access to the network would be a significant problem for the network's security. So defining some level of access management and monitoring seems to be a critical component of 5G network security.

### Measure 3: Testing and monitoring.

Random and continuous testing of every piece of equipment and following that monitoring the network is another measure that is important to protect the network. Monitoring makes it easier to detect any unusual behavior that may indicate malicious activity.

### Measure 4: Strong cybersecurity standards.

It is important to clearly state that although a strong approach to cybersecurity policy and practice is a must for the protection of 5G networks. But in addition, some cybersecurity rules– like effective IT asset management, keeping patching up to date, deploying effective firewalls and other protection and

detection measures, and employing staff with the right skills to implement cybersecurity – need to be implemented as fundamentals of security protection.

### Measure 5: Banning of certain components in certain parts of the infrastructure.

Refers to banning of using some technologies and equipment from specific vendors like Huawei in sensitive areas of the network like core network. But my opinion, the biggest concern of Western countries is their monopoly in global markets rather than security concerns because providing one hundred percent security is unattainable; if Huawei products and services are found to be vulnerable, what guarantee is there for American and European products?
As a result, in addition to the strong will to overcome the concerns of operators and governments about data leakage in telecommunications equipment, Security by design would be a better solution for vendors.

Network and Information Systems Cooperation Group(NIS Cooperation Group), in their report[30] published in 2019, identified five categories of risks of strategic importance from an EU perspective.

1- **Risks scenarios related to inadequate security measures**

**Misconfiguration of networks:** refers to penetrating into 5G networks with poorly configured systems and architecture in order to violation of information confidentiality and disrupt different services.

**Lack of access controls:** someone with high-level access privileges tries to adverse action, leading to confidentiality/integrity and/or availability breach. (these actions could be done legally or just because of rogue behavior of the contractor's staff)

2- **Risk scenarios related to the 5G supply chain**

**Low-quality products:** refers to espionage that has been done by state or state-backed actors to attack vulnerable network components.

**Dependency**: A mobile network operator sources a large number of its sensitive network components or services from a single supplier, increasing the risks to the network. Consequently, the quality of a supplier's equipment decreases due to a lack of competition between different vendors.

3- **Risk scenarios related to modus operandi of main threat actors**

**5G supply chain**: exercising pressure over a supplier to provide access to sensitive network assets through (either purposefully or unintentionally) pre-embedded vulnerabilities.

**The exploitation of 5G networks by organized crime:** disrupting various services to ransom businesses relying on those services, By taking control of a critical part of the 5G network architecture.

Alternatively, **targeting the end-users**, e.g., by injecting false messages to the users of the network as part of a large-scale "phishing" attack or online scam, or gaining access to confidential data about users by using the compromised network.

4- **risks on 5G networks and its interdependencies with other critical systems**

Disruption of critical infrastructures or services by malicious hackers gaining control of their dedicated network slice to compromise the whole or part of the network. Threats targeting interruption of electricity supply or attacks to the energy grid by a state, a state-backed actor, or an organized crime group.

5- **Risk scenarios related to end-user devices**

Targeting IoT devices due to weaknesses and security vulnerabilities in them.

## Analysis of Potential Regulatory Approaches

With respect to the research of Jukka Salo et al. in[31], There are at least three levels at which Security and Privacy could be regulated, each with benefits and drawbacks:

- Regulation of government;
- Self-regulation of Industry; and
- Regulation of consumer or market.

The governments are the most powerful and responsible organizations to define the laws and regulations in society. On the other hand, industries can develop principles and practices that reflect consensus on the best approach to privacy. For example, in "industry self-regulation," a network of outstanding companies may require their business partners to meet industry standards on privacy. Although the service providers offer security and privacy at the consumer or market regulation level to satisfy consumers and corporate users, but most of the issues would remain unresolved.

## Existing mitigating measures

- Follwoing of Security requirements which are set out notably in EU telecoms legislation and in the NIS Directive in EU level and also coordination between Member States in case of cross-border risks and incidents.

- Deploying frameworks at EU and national level, including General Data Protection Regulation(GDPR) and e-Privacy Directive as well as requirements applicable to critical infrastructures.

- Specifying Binding rules to apply to mobile network operators in the national level of Member States. (trying to avoid diverse approaches to the implementation of them)

- Applying different security measures (both technical and process-related)by mobile network operators.

- 3GPP SA3 as a standardization perspective has addressed several 5G security-related concerns and supports end-to-end encryption. It should be noted these bodies do not deal with security concerns related to the deployment and configuration of the technology.

# Chapter 4

# 5G in Italy

According to the report published on [32] by European Commission, the Italian 5G strategy started late in 2016 by announcing the development of 5G infrastructure and the utilization of the spectrum above 6 GHz.

Then in March 2017, five cities were selected as trial cities of 5G, including Milan, Prato, L'Aquila, Bari Matera by the cooperation of different mobile operators (Telecom Italia, Vodafone, WindTre, Open Fiber Fastweb). They were allowed to use 100 MHz of 3.6-3.8 GHz spectrum under provisional licenses from September 2017 to 2020.

Later in August 2020, Agcom extended-spectrum licenses also in the 900 and 1800 MHz bands. Therefore Iliad Italia was licensed to use 900 MHz, and TIM, Vodafone, and WindTre were licensed to use 2100 MHz frequency band. The expiry of provided licenses would be 2029.

In 2018, the NRA(National Regulatory Authority) announced 5G multi-band spectrum auctions (in the 700 MHz, 3.6-3.8 GHz, and 26 GHz bands). Furthermore Ministry of Economic Development, according to the national regulatory authority (AGCOM) rules, has established coverage obligations for the 700 MHz FDD band and 3600-3800 MHz band to ensure widespread improvements in mobile coverage across Italy.

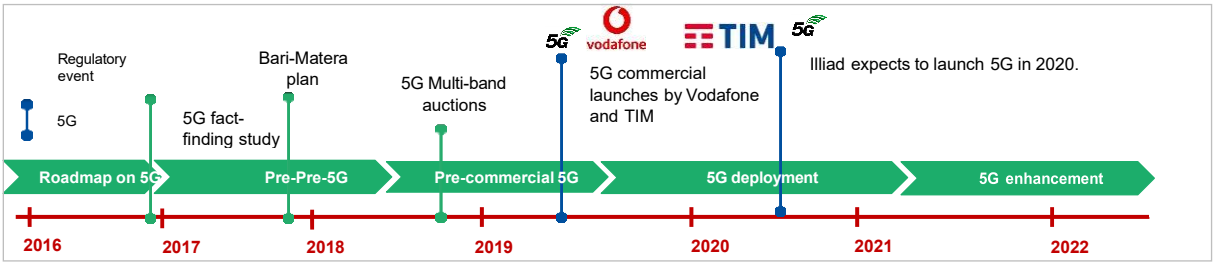


Figure 10. 5G timeline in Italy[32].

## 4.1 Status of 5G in Italian mobile operators

**Vodafone**

5G services launched by Vodafone Italy in five cities in June 2019 (Milan, Rome, Turin, Bologna, and Naples). Vodafone network covered 80% of the city in Turin, with 120 cell sites. Later the number of cities covered by this company increased up to 100 by the end of 2021. Vodafone and Telecom Italia signed a 5G network-sharing deal with Telecom Italia in 2019.

**Telecom Italia**

In 2019 Rome, Turin, and Naples were the first cities where TIM launched its 5G service. As of late March 2020, Bologna, Brescia, Florence, Genoa, Milan were added to the list of covered cities under the TIM network. The company is planning to reach the coverage of 120 cities by the end of 2021.

**WindTre**

WindTre launched its 5G network in around ten regional capitals in 2020. This operator claimed around 73.7% of the population is covered up to January 2021.

**Iliad Italia**

In December 2020, Iliad Italia launched its 5G services in 27 Italian cities with highly competitive promotions compared to other Italian competitors.

## 4.2 Security of 5G in Italy

European House–Ambrosetti, in their white paper [33], had some recommendations for the security of 5G in Italy as follows:
Italy and other Member states of the European Union need an inherently reliable 5G. This implies considering the potential drivers of all vendors, economic and geopolitical, and auditing their supply chain even before designing cybersecurity countermeasures.
Three measures are recommended to Italian Policy Makers (PM) and Industry Players (IP) with the key objective to create a more secure Italian 5G system:
1. An assessment of its critical infrastructures (1, 2, 3 priority level) – PM, IP
2. A process to audit the whole supply chain of the vendors – PM, IP
3. The establishment of a COE - Centre of Expertise for threat intelligence where processes and experiences are continuously shared with like-minded countries and bring to augmented capability – PM, IP

# Chapter 5
# Cyber Security in 6G

Regarding research[34] done by A. Dogra et al., 5G(the fifth generation technology standard for broadband cellular networks), with all its related services and use cases, is still in the initial stage of its development and commercialization. It is expected that in the next decade(2030-2035), 6G networks will be available in most parts of the world with the slogan of "everything connected". In parallel to various countries like Finland, which have already started their research on 6G networks, ITU has established the "Network 2030" group focusing on exploring new technologies for the systems beyond 2030. It is predicted that 6G will operate with high bandwidths, Terahertz frequencies (up to 3THz), and high data rates (up to 1Tb/s), which would be the cornerstone of the Internet of Everything. In 6G, the transmission networks will be based on AI and ML-based automatic information collection and decision making. Applications of 6G will cover space, air, and ground communication and underwater as well. Another advancement in communications would be mobile satellite communication, In which would have global coverage at a very low cost and will support the high-speed mobility of users. In addition to current use cases(eMBB, mMTC, and uRLLC), which developed in 5G, there are some use cases proposed for 6G, including Computation Oriented Communication (COC), Event Defined uRLLC (EDuRLLC), Contextually Agile eMBB Communications (CAeC), ultra-High Speed with Low Latency communication (uHSLLC), ultra-High Data Density (uHDD), ubiquitous Mobile Ultra-Broadband (uMUB). It is expected that next-generation networks will take advantage of Optical Wireless Communications (OWC) and Visible Light Communication (VLC) to achieving high data rates.
Data security and privacy are crucial aspects issues of wireless networks. So in order to ensure security and privacy in 6G, several PHY security techniques and encryption algorithms are required to be developed in the future because the economy and society will become more dependent on this technology. Thus, a trusted architecture with required secrecy and privacy is mandatory.

P. Porambage et al. in[35] have studied the 6G from the security point of view. Their findings of possible attacks and their impact on 6G architecture are summarized in the table below.

| | | 6G architectural blocks | | | | | Key 6G applications | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Security attacks** | **Possible defense mechanisms** | Int. Radio/RAN-Core Convergence | Edge Intelligence and Cloudification | Specialized 6G Networks | Int. Net. Management/ Orchestration | Consumer end (terminals and users) | UAV | Holographic Telepresence | Extended Reality | Connected autonomous vehicles | Smart Grid 2.0 | Industry 5.0 | Hyper-intelligence health | Digital Twin |
| **AI/ML** | | | | | | | | | | | | | | |
| Poisonous attacks | Moving target defense/ Input validation | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | | ✓ | ✓ | |
| Evasion attacks | Defensive distillation/ Adversarial training | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | |
| Infrastructure physical attacks & communication tampering | Use tamper-proof hardware | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Compromise of AI frameworks | Security solutions for software, firmware and hardware. | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| ML API-based Attacks | Control information provided by ML APIs | | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | |
| Model inversion attacks | Noise injection | | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | |
| Model extraction attacks | Control information provided by ML APIs/ Noise injection | | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Adversarial attacks | Defensive distillation/ Adversarial training/ Input validation | | ✓ | | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | |
| Privacy attacks | Differential privacy/ Homomorphic encryption. | | ✓ | | | ✓ | | ✓ | | | | | ✓ | ✓ |
| **Blockchain** | | | | | | | | | | | | | | |
| Majority/ 51% attack | Select proper DLT architecture | | ✓ | ✓ | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Double-spending attacks | Protect transactions. | | | ✓ | | | ✓ | | ✓ | ✓ | ✓ | | ✓ | |
| Re-entrency attack | Use security check tools. | | | ✓ | ✓ | | ✓ | | | ✓ | | ✓ | ✓ | |
| Sybil attacks | Use strong authentication and access control mechanisms. | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Authentication access control attacks | Use robust authentication and access control mechanisms. | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Security misconfigurations | Identify semantic flaws. | ✓ | | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Privacy attacks | Privacy by design approach | | ✓ | | | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| **Quantum computing** | | | | | | | | | | | | | | |
| Quantum cloning attack | Uncloneable encryption mechanisms | | | | | ✓ | | ✓ | | | | | | ✓ |
| Quantum collision attack | Quantum resistant encryption solutions | | | | | ✓ | | ✓ | | | | | | ✓ |
| **VLC** Visible Light Communication | | | | | | | | | | | | | | |
| Authentication/ access control attacks | Location-based authentication | ✓ | | ✓ | | ✓ | | | | ✓ | | ✓ | | |
| Eavesdropping | Artificial noise-assisted visible light MIMO beamforming | ✓ | | | | | | | | ✓ | | ✓ | | |
| Jamming and data modification attacks | ML techniques to learn the environment in real time | ✓ | | ✓ | | | | | | ✓ | | ✓ | | |
| **THz** | | | | | | | | | | | | | | |
| Authentication access control attacks | Electromagnetic signatures for physical layer authentication | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | | ✓ | | |
| Eavesdropping | Characterization of the backscatter channel / Exploting multipath. | ✓ | | | | | ✓ | | | ✓ | | ✓ | | |
| **Molecular communication** | | | | | | | | | | | | | | |
| Authentication access control attacks | Biochemical cryptography | | | ✓ | | ✓ | | | | | | | ✓ | |
| Privacy attacks | Information-theoretic privacy /Camouflage of DNA-based messages | | | | | ✓ | | | | | | | ✓ | |
| **RIS** Reconfigurable Intelligent Surface | | | | | | | | | | | | | | |
| Authentication access control attacks | RIS-assisted secret key generation | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | | ✓ | | |
| Eavesdropping | Controlling of phase shifts of RIS to improve secrecy performance. | ✓ | | | | | ✓ | | | ✓ | | ✓ | | |

Table 12. Summary of security attacks and their impact on 6G architecture, key technologies, and applications[35].

# Chapter 6
# Conclusion

This dissertation started with a brief review of the history of mobile broadband networks. The main technical features of mobile generations from 1G to 4G are discussed. Then we had a deep dive into the Cybersecurity of 5G. Different meanings were provided and the difference between Cybersecurity and Information security. Furthermore, different security mechanisms hired by previous mobile technologies were summarized. Later, studies and research, together with their findings focused on Cybersecurity of 5G, were presented. Chapter 3 and chapter 4 focused on Risk management in Cybersecurity of 5G and the status of 5G in Italy, respectively. Finally, this thesis is finished by a fast study on the Cybersecurity of 6G.

5G could be considered as a revolution in telecommunication networks. It supports massive bandwidth, massive interconnectivity of machines, and reliable, low-latency communication; Besides all its advantages, the threat landscape has also become broader. So it is evident that how important it is to ensure security remains in place throughout a product or service lifetime and is a continuum rather than a point-in-time effort for vendors and operators. Securing 5G must be implemented by design and not be an afterthought, and network security needs to evolve continuously. Since 5G is a newborn technology and it is not commercially launched in many countries, and yet its unique features were not implemented in IoT enabled equipment so there would be many vulnerabilities that are still undiscovered.

In summary, in order to provide network resilience on top of the OAM(Operations, Administration, and Maintenance) system, new technologies such as Artificial Intelligence (AI) / Machine Learning (ML) great potential to detect and analyze the security threats to the network operation. NIST CSF is also could be used as An to build end-to-end network resilience management. Controlling 5G security risks is achieved through joint efforts of all industries. Additionally, taking a Zero-Trust approach, combined with the advanced techniques of cyber threat intelligence and Network Slicing that 5G offers, will further enhance 5G’s security.

Government regulators should work closely with all relevant industries and partners. It is also important to obtain the support of network equipment suppliers and relevant verticals. risk awareness and security capabilities and generates a positive impact on the healthy and sustainable development of various applications in the 5G era.

# Bibliography


[1] Mohammad Meraj ud in Mir and Dr. Sumit Kumar. Evolution of mobile wireless technology from 0g to 5g. 6(3):2545–2551, 2015.

[2] Segan, Sascha. “What Is 5G?” *PCMAG*, PCMag, 25 Feb. 2021, www.pcmag.com/news/what-is-5g.

[3] Dahlman, E., Parkvall, S., & Sköld, J. (2018). Chapter 1 - What Is 5G? In E. Dahlman, S. Parkvall, & J. Sköld (Eds.), 5G NR: the Next Generation Wireless Access Technology (pp. 1–6). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-814323-0.00001-6

[4] Chapman, T., Dahlman, E., Larsson, E., Parkvall, S., Skold, J. and Von Wryca, P., 2015. *HSPA evolution*. London: Academic Press.

[5] Madhusanka Liyanage; Ijaz Ahmad; Ahmed Bux Abro; Andrei Gurtov; Mika Ylianttila, "Evolution of Cellular Systems," in *A Comprehensive Guide to 5G Security* , Wiley, 2017, pp.1-29, doi: 10.1002/9781119293071.ch1.

[6] Jonathan Rodriguez, "Drivers for 5G," in *Fundamentals of 5G Mobile Networks* , Wiley, 2014, pp.1-27, doi: 10.1002/9781118867464.ch1

[7] 3GPP SA1 (2016) Feasibility study on new services and markets technology enablers; stage 1, Technical report, TR 22.891 (Release 14), September 2016.

[8] ITU-R (2015) IMT vision – framework and overall objectives of the future development of IMT for 2020 and beyond, Recommendation, REC M. 2083-0, September 2015.

[9] Dahlman, E., Parkvall, S., & Sköld, J. (2018). Chapter 2 - 5G Standardization. In E. Dahlman, S. Parkvall, & J. Sköld (Eds.), 5G NR: the Next Generation Wireless Access Technology (pp. 7–25). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-814323-0.00002-8

[10] Services, P. and Core, P., 2021. Control Plane and User Plane Separation (CUPS) Data Sheet. [online] Cisco. Available at: https://www.cisco.com/c/en/us/products/collateral/wireless/packet-core/data-sheet-c78741416.html.

[11] Dahlman, E., Parkvall, S., & Sköld, J. (2018). Chapter 6 - Radio-Interface Architecture. In E. Dahlman, S. Parkvall, & J. Sköld (Eds.), 5G NR: the Next Generation Wireless Access Technology (pp. 73–102). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-814323-0.00006-5

[12] “Glossary Archive.” *Mpirical*, www.mpirical.com/glossary.

[13] “Computer Security Resource Center.” *CSRC*, csrc.nist.gov/glossary.

[14] Njoroge, Fredrick & Kamau, Lincoln. (2018). A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G.

[15] Madhusanka Liyanage; Ijaz Ahmad; Ahmed Bux Abro; Andrei Gurtov; Mika Ylianttila, "Mobile Networks Security Landscape," in *A Comprehensive Guide to 5G Security* , Wiley, 2017, pp.59-74, doi: 10.1002/9781119293071.ch3.

[16] “5G Security Issues.” *Positive Technologies: SS7, Diameter Signalling Firewall, 5G, IoT Security Solutions.*, positive-tech.com/expert-lab/research/5g-security-issues/.

[17] Bartock, M., Cichonski, J. and Souppaya, M., 2020. *5G Cybersecurity: Preparing a Secure Evolution to 5G*. [ebook] National Institute of Standards and Technology(NIST). Available at: <https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-final.pdf>

[18] GSMA. (2021). *Mobile Telecommunications Security Landscape*. GSMA. Retrieved from https://www.gsma.com/security/wpcontent/uploads/2021/03/id_security_landscape_02_21.pdf

[19] Cisco. (2021). *5G Cybersecurity Guidance*. Retrieved from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf1.pdf

[20] 5G Americas. (2020). *Security Considerations for the 5G Era*. 5G Americas. Retrieved from https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf

[21] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. 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 (WiSec '19). Association for Computing Machinery, New York, NY, USA, 221–231. DOI:https://doi.org/10.1145/3317549.331972

[22] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov and M. Ylianttila, "Security for 5G and Beyond," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3682-3722, Fourth quarter 2019, doi: 10.1109/COMST.2019.2916180.

[23] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, Firstquarter 2020, doi: 10.1109/COMST.2019.2933899.

[24] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, Firstquarter 2020, doi: 10.1109/COMST.2019.2933899.

[25] Fonyi, S. (2020). Overview of 5G Security and Vulnerabilities [Ebook]. The Cyber Defense Review. Retrieved 11 July 2021, from https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20%2008_%20Fonyi_WEB.pdf.

[26] J. Cao et al., "A Survey on Security Aspects for 3GPP 5G Networks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170-195, Firstquarter 2020, doi: 10.1109/COMST.2019.2951818.

[27] C. Benzaïd, T. Taleb and M. Z. Farooqi, "Trust in 5G and Beyond Networks," in *IEEE Network*, vol. 35, no. 3, pp. 212-222, May/June 2021, doi: 10.1109/MNET.011.2000508.

[28] DaSilva, L., H. Reed, J., Shetty, S., Park, J., Wijesekera, D., & Wang, H. (2019). *Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation* [Ebook]. The NATO Cooperative Cyber Defense Centre of Excellence., from https://ccdcoe.org/uploads/2020/12/4-Securing-5G_ebook.pdf.

[29] Sullivan, J., & Lucas, R. (2020). *5G Cyber Security: A Risk-Management Approach* [Ebook]. Royal United Services Institute for Defence and Security Studies.

[30] Network and Information Systems Cooperation Group. (2019). EU coordinated risk assessment of the cybersecurity of 5G networks [Ebook]. https://ec.europa.eu/newsroom/dae/redirection/document/62132.

[31] Madhusanka Liyanage; Ijaz Ahmad; Ahmed Bux Abro; Andrei Gurtov; Mika Ylianttila, "Regulatory Impact on 5G Security and Privacy," in A Comprehensive Guide to 5G Security , Wiley, 2017, pp.399-419, doi: 10.1002/9781119293071.ch17.

[32] PUJOL, F., MANERO, C., CARLE, B., & REMIS, S. (2021). *5G Observatory Quarterly Report 11* [Ebook]. European Commission DG Communications Networks. http://5gobservatory.eu/wp-content/uploads/2021/04/90013-5G-Observatory-Quarterly-report-11-2.pdf.

[33] The European House - Ambrosetti S.p.A. (2019). *5G and security in Italy An overview of problems and possible remedies* [Ebook]. https://www.sipotra.it/wp-content/uploads/2019/11/5G-and-security-in-Italy.-An-overview-of-problems-and-possible-remedies.pdf.

[34] A. Dogra, R. K. Jha and S. Jain, "A Survey on Beyond 5G Network With the Advent of 6G: Architecture and Emerging Technologies," in IEEE Access, vol. 9, pp. 67512-67547, 2021, doi: 10.1109/ACCESS.2020.3031234.

[35] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.