

Security Analysis of 6G Networks



By

Masooma Zahra

(Registration No: 00000330270)

Department of Information Security

Military College of Signals

National University of Sciences and Technology (NUST)

Rawalpindi, Pakistan

(2024)

Security Analysis of 6G Networks



By

Masooma Zahra

(Registration No: 00000330270)

A thesis submitted to the National University of Sciences and Technology, Islamabad, in
partial fulfillment of the requirements for the degree of

Masters in

Information Security

Supervisor: Dr.Imran Rashid

Military College of Signals

National University of Sciences and Technology (NUST)

Rawalpindi, Pakistan (2024)

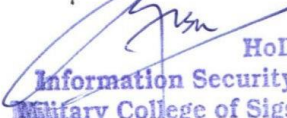
THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis Security Analysis of 6G Network written by Mr/MS **NS Masooma Zahra** Registration No. **00000401600** of **MSIS-19 Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis. <http://10.250.8.41:8080xmului/handle/123456789/>.

Signature: _____


Name of Supervisor Dr. Imarn Rashid

Date: _____
24/10/24

Signature (HoD): _____

HoD
Information Security
Military College of Sigs

Date: _____
24/10/24

Signature (Dean/Principal): _____

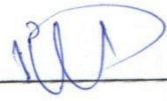


Dean, MCS (NUST)
Adil Masood Siddiqui, PhD


Date: _____
24/10/24

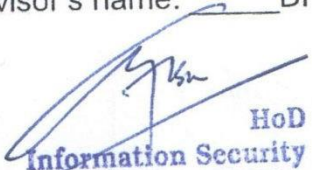
National University of Sciences & Technology
MASTER THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Regn No.) Masooma Zahra 00000330270
Titled: Security Analysis of 6G Networks be accepted as partial fulfillment of the requirements for the award of Master of Science in Information Security (MS-IS) degree.

Examination Committee Members

1. Name: Maj Bilal Ahmed Signature: 
2. Name: Maj Sarmad Idrees Signature: 
3. Name: Dr Shahzaib Tahir Signature: 

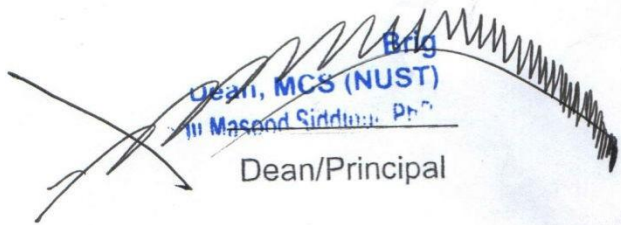
Supervisor's name: Dr Imran Rashid Signature: 
Date: 24/10/2024


HoD
Information Security
Military College of Sigs
Head of Department

24/10/2024
Date

COUNTERSIGNED

Date: 24/10/24


Dean, MCS (NUST)
Maseed Siddique, PhD
Dean/Principal

CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled "Security Analysis of 6G Network." was conducted by NS Masooma Zahra under the supervision of Dr Imran Rshid. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Military College of Signals, National University of Science & Technology Information Security Department in partial fulfillment of the requirements for the degree of Master of Science in Field of Information Security Department of information security National University of Sciences and Technology, Islamabad.

Student Name: NS Masooma Zahra

Signature: Ali

Examination Committee:

- a) External Examiner 1: Name Maj Sarmad Idrees (MCS) Signature: [Signature]
- b) External Examiner 2: Name Maj Bilal Ahmed (MCS) Signature: [Signature]
- c)
- d) External Examiner 2: Name Dr Shahzaib Tahir (MCS) Signature: [Signature]

Name of Supervisor: Dr Imran Rashid.

Signature: [Signature]

Name of Dean/HOD: Dr Muhammad Faisal Amjad

Signature: [Signature]
HoD
Information Security
Military College of Sigs

PLAGIARISM UNDERTAKING

I solemnly declare that research work presented in the thesis titled Security Analysis of 6G Network is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagi

arized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/ revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagi arized thesis.

Student Signature: _____



Name: NS Masooma Zahra

Date: 24 october2024

arized thesis.

AUTHOR'S DECLARATION

I NS Masooma Zahra hereby state that my MS thesis titled Security Analysis of 6G Network is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world. At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Student Signature: _____

Name: NS Masooma Zahra _____

Date: 24 october 2024 _____

ACKNOWLEDGEMENTS

I would like to thank my mother, Dr Naheed Fatima, and my brother, Muhammad Momin Abbas, for their constant support and guidance. I wouldn't have been able to complete my thesis if it wasn't for them.

Contents

<u>ACKNOWLEDGEMENTS</u>	<u>VI</u>
<u>LIST OF TABLES</u>	<u>X</u>
<u>LIST OF FIGURES</u>	<u>XI</u>
<u>LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS</u>	<u>XII</u>
<u>ABSTRACT</u>	<u>XIII</u>
1 <u>INTRODUCTION</u>	<u>1</u>
1.1 <u>DEFINE THE PROBLEM</u>	
1.2	
1.3 <u>PURPOSE OF THE STUDY</u>	
1.4	
1.5 <u>RESEARCH QUESTION</u>	
1.6	
1.7 <u>SIGNIFICANCE OF STUDY</u>	
1.8	
1.9 <u>DELIMITATION OF STUDY</u>	
1.10	
1.11 <u>OUTLINE/ORGANISATION OF STUDY</u>	
2 <u>LITERATURE REVIEW</u>	<u>5</u>
2.1 <u>BACKGROUND</u>	
2.1.1 <u>First Generation of Cellular Network (1G)</u>	
2.1.2 <u>Second Generation of Cellular Network (2G)</u>	
2.1.3 <u>Third Generation of Cellular Network (3G)</u>	
2.1.3.1 <u>Security in 3G</u>	

- 2.1.3.2 [Security in CDMA 2000](#)
- 2.1.3.3 [Security in UMTS](#)
- 2.1.3.4 [Security Threat of 3G](#)

- 2.1.4** [Fourth Generation of Cellular Network \(4G\)](#)
 - 2.1.4.1 [Key Technologies \(4G\)](#)
 - 2.1.4.2 [Security of 4G](#)
 - 2.1.4.3 [LTE Security Model](#)
 - 2.1.4.4 [Security in WiMAX](#)
 - 2.1.4.5 [Security Threat Analysis for 4G](#)

- 2.1.5** [Fifth Generation of Cellular Network \(5G\)](#)
 - 2.1.5.1 [Security Requirements](#)
 - 2.1.5.2 [Security Landscape](#)
 - 2.1.5.3 [Threat Analysis of 5G Security](#)
 - 2.1.5.4 [Latest Trends in 5G technologies](#)
 - 2.1.5.5 [Network Function Virtualization \(NFV\)](#)
 - 2.1.5.6 [Software Defined Network \(SDN\)](#)
 - 2.1.5.7 [Security in SDN-based Networks](#)
 - 2.1.5.8 [Business Models for Cyber Security of 5G](#)
 - 2.1.5.9 [Physical Layer Security](#)
 - 2.1.5.10 [5G WLAN Security](#)

- 2.1.6** [Sixth Generation of Cellular Network](#)
- 2.1.7** [Identifying potential threats and challenges](#)
 - 2.1.7.1 [Threat Analysis and Prioritization](#)
- 2.1.8** [Framework development, review of best practices existing solutions](#)
 - 2.1.8.1 [Development Models](#)
 - 2.1.8.2 [Subscriber and Device Protection](#)
 - 2.1.8.3 [Network Protection](#)
 - 2.1.8.4 [New IP Protocol Stack](#)
 - 2.1.8.5 [Technologies Utilized by 5G](#)
 - 2.1.8.6 [Cryptographic Counter Measures](#)
 - 2.1.8.7 [Entity Attribute Counter-measures](#)
 - 2.1.8.8 [Intrusion Detection System \(IDS\)-based Counter-measures](#)
 - 2.1.8.9 [Authentication Techniques](#)
 - 2.1.8.10 [Threat Landscape and Possible Solutions Related to 6G Technologies](#)
- 2.1.9** [Formulation of Framework](#)

2.2 [Summary](#)

3 [METHODOLOGY](#) 60

3.1 [Phase I: Security Analysis of 4G and 5G networks](#)

3.2 [Phase II: Data Collection along with Categorization and Prioritization of threats](#)

3.3 [Phase III: Review of Best practices and existing solutions](#)

3.4 [Phase IV: Formulation of Framework](#)

3.5 [Summary](#)

4 [CONCLUSION AND FUTURE RECOMMENDATIONS](#) 74

4.1 [Summary](#)

4.2 [Discussion/Conclusion](#)

4.3 [Recommendation/Way forward](#)

5 [FINDINGS, ANALYSIS AND DISCUSSION](#) 76

5.1 [Analysis of security threats](#)

5.1.1 [Categorization according to aspect of security they affect](#)

5.1.2 [Categorization according to mechanism of action](#)

5.2 [Analysis of best practices](#)

[BIBLIOGRAPHY](#) 79

List of Tables

1. Table 1: Types of SDN threats, their impact likelihood of occurrence	Pg 12
2. Table 2: Security issues pertaining to Packet Switched Network	Pg 22
3. Table 3: Risk assessment of different attacks on Availability, Integrity, and Confidentiality	Pg 24
4. Table 4: Security and privacy issues on Physical, Connection, and Service Layers	Pg 25
5. Table 5: Security principle, threat and impact	Pg 25
6. Table 6: Threats based on Nefarious Activity/Abuse of Assets (NAA) and areas of impact	Pg 26
7. Table 7: Threats based on Eavesdropping/Interception/ Hijacking (EIH) and areas of impact	Pg 28
8. Table 8: Threats based on Physical Attacks and areas of impact	Pg 29
9. Table 9: Threats based on unintentional damages (accidental) (UD) and areas of impact	Pg 30
10. Table 10: Threats based on failures or malfunctions (FM) or outages (OUT) and areas of impact	Pg 30
11. Table 11: Threats based on disasters and legal issues, and areas of impact	Pg 31
12. Table 12: Comparative analysis between security aspects of 4G and 5G	Pg 53

List of Figures

1. **Figure 1:** Security Issues of Different Security Attacks **Pg 15**
2. **Figure 2:** Security Issues due to Causes and Methods of Security Attacks **Pg 15**
3. **Figure 3:** Security Issues due to Physical Access **Pg 16**
4. **Figure 4:** Security Issues due to Unauthorized Access to Sensitive Data **Pg 17**
5. **Figure 5:** Security Issues due to Manipulation of Sensitive Data **Pg 18**
6. **Figure 6:** Security Issues due to Unauthorized Service Access **Pg 18**
7. **Figure 7:** Security Issues pertaining to Physical Layer **Pg 19**
8. **Figure 8:** Security Issues pertaining to Medium Access Control (MAC) **Pg 20**
9. **Figure 9:** Important steps for Formulation of Framework for Secure 6G **Pg 47**

LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

1G 1st Generation
2G 2nd Generation
3G 3rd Generation
4G 4th Generation
5G 5th Generation
6G 6th Generation
RIS re-configurable intelligent surfaces
FDMA Frequency-Division Multiple Access
ITU International Telecommunication Union
UMT Universal Mobile Telecommunication
SDN Software Defined Network
RAN Radio Access Network
NFV Network Function Virtualization
VoLTE Voice-over-Long-Term Evolution
VLC Visible Light Communications
MAC Medium Access Control
LTE Long Term Evolution
DTLS Datagram Transport Layer Security
eMBB Enhanced Mobile Broadband

ABSTRACT

Tremendous influx of novel technologies to enhance the global connectivity leads to vulnerability to security breaches by organized malicious actors. Hence, the need of a secure future communication system is becoming mandatory.

This study is carved out into four phases. In **Phase I**, literature review was done to identify threats and challenges in emerging technologies and how they can pose challenges to 6G's security. In **Phase II**, data was collected by publicly available resources. Then, threats were classified based on their severity, impact, and likelihood of occurrence. Taxonomy was developed based on specific network layers, protocols, and applications. In Phase III, by reviewing the best practices and existing solutions. A robust and adaptable security framework for 6G network was formulated, which should satisfy all security measures regarding confidentiality, integrity, and availability.

In this paper, all possible areas of 6G security were discussed, but still it is in these initial stages and a lot of research is required in future is required. Potential future research areas of 6G communication are also highlighted.

Today's communication system having enhanced global connectivity is more and more vulnerable to security breaches by organized and complicated malicious actors. Hence a secure communication system is becoming need of the hour. In this research, work was carried out in four phases. In phase I & II, different types of security threats were identified by literature review and categorized according to their impact on confidentiality, integrity and availability of data. Security threats were prioritized according to their likelihood of occurrence and severity of impact in phase III. In phase IV, best practices were reviewed and latest security trends introduced in 5G technologies were analyzed. In the last phase, a framework was formulated, highlighting important steps to be taken for a secure upcoming 6G network. Finally, few recommendations were suggested.

Keywords: novel technologies, security threats, challenges, best practices.

CHAPTER 1

INTRODUCTION

1.1 Define the Problem

The world is being digitalized, day by day. Every walk of life is dependent on connectivity to flourish and grow. Healthcare, education, agriculture, business, industries, transport, and et cetera are few to name. Speed, efficiency, and security of communication are being met by new technologies to fulfil the requirements of enhanced connectivity. As we stand at the precipice of the sixth generation (6G) of mobile networks, the promises of hyperconnectivity, ultra-low latency, and unprecedented network intelligence are dazzling. However, amidst this excitement lies a critical shadow: the daunting challenge of security. Unlike its predecessors, 6G is envisioned not just as a communication platform, but as an entire ecosystem, interwoven with the fabric of our lives – powering critical infrastructure, shaping healthcare, and driving industrial automation. In this intertwined landscape, a security breach transcends mere data loss; it becomes a potential threat to societal well-being.

5G wireless technologies were deployed in 2020 by the wireless carriers. Software-based technologies will be explored in the future through analysis towards 2025. Clouding and microservice-based architecture being the two major parts of 5G network are the two important features of 5G network. It becomes a change from use of physical resources into virtual and mental environment. 5G networks will require smart networks as management in the future will be data-driven. The smart networks will be the outcome of RIS (reconfigurable intelligent surfaces), VLC (visible light communication), MC (molecular communication), and QC (quantum computing). The topology of 6G will be based on the vRAN architecture and the cloudified core network. 6G architecture is going to improve in terms of platform, functionality, specialization and orchestration. These problems in 5G will be addressed in the upcoming 6G.

Platform: Heterogenous cloud infrastructure comprising of multiple clouds will be the platform.

Functional Architecture: New functionalities like no limit to, RAN core convergence, self-free radio, and information collection for AI will be the future functional architecture.

Specialization: Personal networks, extreme slicing, and flexible workload offloading will be the specializations of 6G networks.

Orchestration: Cognitive closed loop and automation will be part of future orchestration of 6G.

Hence, security considerations of upcoming 6G network need to be addressed in above-mentioned aspects. In light of all these technical advancements catering for expansion of network traffic, the probability of malicious actors ready to exploit has been surging. Novel methods of attacking the telecommunication networks are the signs of organized cybercrime. Secure telecommunication system is becoming the need of the hour.

1.2 Purpose of the Study

The thesis will review all the literature related to different security threats being faced by cellular networks. The detailed review of security infrastructure of networks will be done to understand its impact on mitigating such attacks. The knowledge of potential vulnerabilities, possible solutions, and best practices to address them will enable us to propose a secure 6G network's framework.

This thesis will delve into the uncharted territory of 6G security, embarking on a comprehensive analysis of its vulnerabilities and potential solutions. We begin by exploring the unique security landscape of 6G, characterized by increased network complexity, dynamic deployments, and the integration of novel technologies like Artificial Intelligence (AI) and quantum computing. This analysis will identify key attack vectors that adversaries may exploit, ranging from traditional eavesdropping and man-in-the-middle attacks to AI-powered manipulation and disruption of network functions.

1.3 Research Question

Keeping in view the evolution of cellular networks right from the first generation to the sixth

generation, the important security features were introduced in accordance with emerging needs. Therefore, what new security features were implemented in 4G in comparison to 3G cellular networks? As novel technologies are being introduced in 5G, what type of security threats are being anticipated? Current trends in security technologies for upcoming 6G systems based on best practices enable network developers to adopt a suitable framework for a more secure 6G network.

1.4 Significance of the Study

In this modern world, which is the era of global village has transformed our lifestyles with new methods of learning, working, entertaining, shopping, and travelling. In this age of digitalisation in addition to the connecting humans by internet, mobile devices and machines are also being connected similarly. Huge amount of data is being transferred every moment. Today's telecommunication systems is carrying various valuable things e.g., revenue streams and brand reputation. Risks of hack visits and cybercrimes are estimated to be even higher. Not only businesses or reputation, even public safety is at risk. Therefore, security is the mandatory requirement of cellular networks. This thesis will be one of possible step towards the said aim. This thesis aims to contribute significantly to the ongoing dialogue on 6G security. By providing a thorough analysis of potential threats, evaluating existing solutions, and exploring cutting-edge approaches, we hope to illuminate the path towards a secure and resilient 6G future. As we navigate this critical juncture, ensuring robust security is not just an option, but an imperative.

1.5 Demilination of Study

New technologies that affect security and privacy legislation include cloud, SDN, and NFV. New type of market structures are evolving with the use of such novel technologies. Thus, new type of players of such market will have different type of security requirements. Laws pertaining to data security vary throughout nations. Regulators must implement a uniform security and privacy framework. Necessary actions are required to foster inter-operability and data portability.

1.6 Outline/Organization of the Study

This thesis will be comprised of background on cellular network, discussing its evolution on how with the passage of time, new technologies were introduced to fulfil the emerging needs. Security architecture of cellular networks will be explained in detail. The methodology is on how to identify different threats by collecting data from authenticated sources i.e., organisations engaged in developing cellular networks and published literature on this subject.

Comprehensive analysis of 3G and 4G cellular networks. Identification of potential threats and security challenges to be faced in future. Gathering knowledge about the new technologies and security for improvement of efficiency and security of future 6G network, possible solutions and best practices.

In this thesis, these are main aspects of this study:

- (1). Gathering and reviewing the related literature on the topics of security challenges faced by 5G, emerging technologies being embedded in the development of 6G, the impacts and potential risks of the new technologies, and providing the best practices to handle such security risks. A background of the evolution of cellular network and how new technologies were introduced to fulfil the emerging demands are provided, too. It includes a comprehensive analysis 3G and 4G networks. Further on, we will provide a detailed meta-analysis based on the gathered and reviewed literature.
- (2). In the methodology, we will detail our process adopted for the study. Elaborating the purpose and the research questions of this study will be given to aptly describe our intended objectives and work done for that. Here, we will present our gathered data from the authenticated sources, who are engaged in the research and development of cellular networks. We will identify the potential threats based on the collected data.
- (3). Furthermore, we will meticulously examine the current state of security solutions and protocols, assessing their suitability for this new paradigm. We will delve into the strengths and limitations of existing cryptographic methods, authentication mechanisms, and intrusion detection systems in the context of 6G's unique challenges. Building upon this foundation, we will explore promising new security approaches designed for the 6G landscape. This includes

investigating the potential of AI-driven security solutions, blockchain-based trust models, and quantum-resistant cryptography.

CHAPTER 2

LITERATURE REVIEW

2.1 Background

2.1.1 First Generation of Cellular Network (1G)

The background of security analysis for 6G can be understood by looking back in history at the first-generation cellular network. By 1980s, the so-called first generation of mobile phones appeared and it was an analog system. Analog radio signals were the mean of communication on the 1G wireless networks. The stronger is the pressure, the more complex the modulation gets that can be as high as almost 150MHz and higher in order to be transmitted from one radio tower to another. That phenomenon will be assigned with an acronym Frequency-Division Multiple Access (FDMA). [1]

Drawback of 1G:

- Short capacity
- Untrustworthy handoff
- Poor voice links
- Lack of call privacy due to third party eavesdropping
- Signal interference issues
- Limited protection against hackers [1]

2.1.2 Second Generation of Cellular Network (2G)

2G network is the older one among 3G network and 4g network since it was first introduced in 1991 that is based on digital signaling technology that is GSM. This pressed the security and the amount of capacity and bandwidth that ranged from 30KHz to 200KHz, thus helping the participants in sending SMS and MMS. However, the speed remained low at 64 kbps. As time went by, gradual improvement in GSM led to the introduction of 2.5 G, which comprised of packet switching in the shape of GPRS as well as EDGE technology. User can send and receive email messages as well as browse the web by using high data rates of 2.5 G that were up to 144 kbps. [2]

2.1.3 Third Generation of Cellular Network (3G)

With the arrival of technology 2G was quickly followed by 3G after the introduction of which the basic technology was set up for portable devices and mobile communications. These arguments

relied on the same requirements stipulated by the International Telecommunication Union (ITU) on the International Mobile Telecommunications-2000 (IMT-2000) claim.

Applications of 3G

- Wireless voice telephony
- Video calls
- Fixed wireless internet access
- Mobile internet access
- Mobile TV

The effective data transfer rate of 3G mobile network was at least 200 kbit/s. Besides, another fixed point is the establishment of 3.5G. And 3.75G are the next move. The advancement of mobile communication standards is visible after every 10 years starting from the 1G. On the surface, all new generations have a set of new frequency bands, higher data rates, and front compatible multimedia technology. [1]

2.1.3.1 Security in 3G

Introduction of services like video, audio and graphic application in 3G cellular network makes it different from 1G. 3G, also known as IMT 2000 or Universal Mobile Telecommunication (UMTS), offers a single cellular network standard that is interoperable with all devices and may be utilized for mobile applications anywhere in the world. It facilitates data transfer over circuit switched and packet switched networks. The 3G standard for IS-95 was known as CDMA 2000, and it included both UMTS CDMA and CDMA 2000. Improved speech quality and interactive gaming were made possible by the 3G technology, which also improved internet surfing, emailing, and streaming of multimedia apps. Although the 3G air interface, known as wide-band CDMA (WCDMA), multiplies user data with pseudo-random codes for synchronization, channelization, and scrambling, the architectural architecture of UMTS was comparable to that of the GSM/GPRS network.

2.1.3.2 Security in CDMA 2000

CDMA 2000 security comprises of the following entities:

- The home network,
- the mobile station controller/packet data serving node (VLR & MSC/PDSN),
- the mobile subscriber (MS),

- the visitor location register,
- the home location register,
- the authentication center (HLR/AC),
- the serving network,
- the user identity module (UIM)

UMTS AKA mechanism in CDMA 2000 is used for authentication and key management protocol. There are two parts to the AKA procedure. Transferring security credentials (authentication vector, or AV) from the home environment (HE) to the serving network (SN) is the initial step in the process. The HLR and AC are mostly found in the HE, while the fundamental network components that are directly involved in connection establishment make up the SN.

The packet switched network element (PDSN) and the circuit switched nodes (VLR/MSC) are the elements of relevance in the SN network when it comes to access security. A typical operator will have both HE and SN nodes if they have a physical access infrastructure.

2.1.3.3 Security in UMTS

As illustrated in figure, the UMTS security architecture is divided into five distinct feature sets. These characteristics are described as follows:

1. Network access security: shields the radio interface from assaults and offers the subscriber safe access to 3G services.
2. Network domain security: Guards against assaults on the wire-line network and enables all customers to safely exchange signaling data.
3. User domain security: Addresses safe mobile station access.
4. Application domain security: Ensures that apps in the provider and user domains can safely exchange information with one another.
5. Security features' visibility and configurability: Informs users about the security measures in place, including which ones need to be activated and when.

The features mentioned above for network access security can be further divided into the next two groups. The following lists the categories along with an explanation of each:

1. User authentication: the network function that guarantees the validity of an identity and
2. Network Authentication: this is the feature that the user confirms; it is connected to a serving

network that has been authenticated by the user's home network. [3]

2.1.3.4 Security Threats of 3G

3G introduced new risks and challenges in order to offer mobile users the next generation of data services and internet connectivity.

When mobile networks shifted to a packet switching paradigm, IP-based RAN (Radio Access Network), and IP core network, the IP-based threat vector—which had not existed in previous generations of mobile networks—was unleashed.

Small computers known as smartphones took the role of mobile devices and became a target for operating system flaws. Modern smartphones need to have their systems patched and updated on a regular basis to prevent vulnerabilities. If these upgrades aren't done, the phone could be vulnerable to attacks by malicious parties who could use the phone to obtain personal information or infect it with malware.

Unauthorized or harmful program installations led to phone hacking, and these devices were occasionally used to attack the network and reduce the quality of service provided by mobile service providers. A tight application security policy for a centralized app store was successfully implemented by some phone manufacturers, but others struggled to keep up with the increasing amount of harmful software housed on their app store platform. [3]

As GTP's architecture ignores security and lacks inbuilt security mechanisms, it has glaring security flaws that are simple for attackers to take advantage of. Attacks that are common include those that target infrastructure or over-billing. In general, GTP security problems fall into the following categories:

1. Abnormal attack on protocol. Attacks of this type frequently result in PDU packets that are broken or irregular, or that do not follow the protocol. One common attack of this type is GTPoverGTP. This type of attack may result in DoS or other effects.

2. An attack on the infrastructure. This type of attack frequently results in unauthorized access to infrastructure equipment, including mobile terminals, GGSN, OAM systems, and SGSNs. An

attacker can connect to the core network by changing his own address. He can then encapsulate attack packets within GTP and attack targets that are mobile or on different networks.

3. Attack on resource utilization. Attacks of this nature can originate from other networks as well as terminals. A common assault in this category is the SYN attack. Denial of service is a common consequence of such an attack.

We believe that a GTP traffic analysis and filter could be a potential solution for safeguarding GTP against the aforementioned security vulnerabilities. We will also explain the answer in the following part. [4]

2.1.4 The Fourth Generation of Cellular Network (4G)

The fourth generation, or 4G, replaced 3G and included ITU-defined IMT enhanced capabilities.

Applications of 4G:

- Amended mobile web access IP technology
- Gaming services
- High-definition mobile TV
- Video conferencing
- 3D television

Two versions of 4G deployed are the Mobile WiMAX standard (since 2007) and the other is the Long-Term Evolution (LTE) (since 2009). However, it has been debated whether these two first-release versions should be considered 4G or not. [1]

4G stands the fourth generation of mobile technology. The 4G system standards are defined by the ITU in IMT advanced. These requirements are:

- A global feature sharing policy that will enable a large number of services and applications at a reasonable cost.
- Interoperability of the internet with other radio access networks as well as the IMT.
- Interoperability of services on both fixed and IMT networks.
- Excellent mobile devices.
- Global roaming capacity.
- Equipment, services, and programs that are easy to use.

- To provide sophisticated services, devices with relatively modest mobility should use 1 Gbps, while those with significant mobility should use 100 Mbps. [3]

2.1.4.1 4G's Key Technologies

1. Enhanced MIMO
2. Cooperative Multi-point LTE Advanced Transmission and Reception
3. Spectrum and bandwidth management
4. Carrier Aggregation
5. Relays [3]

2.1.4.2 Security of 4G

More user data rates, less latency, and an IP-based network architecture are all promised by fourth generation cellular networks. 4G networks solely use the IP protocol and architecture, which is the main distinction between them and 3G networks. WiMAX is therefore regarded as a component of 4G networks. When discussing technologies beyond 3G, LTE is the primary underlying technology that is mentioned. Although there are some similarities between LTE and WiMAX, their network architecture and security are different due to the IP-based protocol and architecture.

2.1.4.3 LTE security model

When the authentication server delivers the UE an Enhanced Authentication Protocol request/identity message (EAP), the UE initiates the LTE authentication procedure. The identification message and its Network Access Identifier (NAI) are included in the EAP-response/identity message that the UE sends in response. The authentication server attempted to retrieve the UE's certificate from its record after receiving the EAP-response/identity message. The authentication server uses the standard AKA method to generate the EAP-Request/Authentication and Key Agreement (AKA)-challenge message.

2.1.4.4 Security in WiMAX

The WiMAX group integrated the IEEE 802.11 security vulnerabilities into the IEEE 802.16 specifications. This was carried out because the requirements for line-of-sight WiMAX changed as the standard did, from 802.16 to 802.16a to 802.16e. As a result, to meet the shifting needs, security requirements and related standards also have to change. In order for the security features of the original IEEE 802.16 standard to work with the IEEE 802.16e standard, the following additional features are added:

1. Privacy Key Management Version 2's protocol (PKMv2)
2. For user authentication, The Extensible Authentication Protocol (EAP) technique is used
3. For message authentication, The Hash-based Message Authentication Code (HMAC) or Cipher-based Message Authentication Code (CMAC) scheme is used
4. Confidentiality is achieved by Advanced Encryption Standards (AES)

2.1.4.5 Security threat analysis of 4G:

Ensuring end-to-end network security in WiMAX is mostly dependent on over-the-air security. Even with the development of security architecture to counteract threats over the air, certain obstacles still exist. Finding a balance between security requirements and implementation costs, performance, and compatibility appears to be the primary problem. WiMAX relies on IP transport methods for managing and controlling traffic, therefore network operators need to protect against wider IP security risks.

2.1.5 Fifth Generation of Cellular Network (5G)

Speed, bandwidth, and the number of connected devices have all significantly increased as a result of the switch from analog or circuit-based to packet-based mobile cellular systems. The number of internet of things (IoT) connected devices is expected to expand by 16 billion by 2021, making up a total of 28 billion more devices.

The demand placed on industrial sectors including transportation, agriculture, heavy industries, and automobiles presents a significant challenge to the current generation of mobile cellular systems, or 4G. It necessitates the creation of 5G, which is anticipated to be an ecosystem for any devices with internet access. The 5G standardization process is still in its early stages.

In order to stay competitive in a global market, nations are investing more in 5G-based smart city initiatives. According to some analysts, this will pose serious security issues and call for cybersecurity specialists' attention.

5G will integrate many access technologies, such as LTE, New Radio (NR) for 5G, and Wireless Local Area Network (WLAN). Additionally, 5G will combine network function virtualization (NFV), software-defined networking (SDN), and cloud computing into a unified, programmable, software-centric system and infrastructure.

In order to support millions of connected devices, densely packed networks, and a variety of use cases for which the older frequency bands—typically less than 6 GHz—might not be able to

provide enough bandwidth, large quantities of new spectrum will be allotted for 5G. The global rollout of 5G technology coincides with corporations' and organizations' global push for remote and hybrid work arrangements. Increased network speed is necessary for flexible work patterns in order to facilitate seamless communication among a dispersed workforce.

Security and privacy are a crucial factor that must be considered in the development of 5G, among many other considerations.

2.1.5.1 Security Requirements

5G security will require assurances at the infrastructure, service, and access levels, among other levels.

Infrastructure level

- SDN
- NFV
- Network Slicing

As SDN is implemented, a more secure channel of communication will exist between the data and control planes. Once network slicing is activated, securely isolate and manage slices.

Service level

Service delivery models are necessary for certain essential services, such e-Health and public safety. New business models must be introduced with carefully considered new trust structures.

2.1.5.2 Security Landscape

The information and communication technology (ICT) sector has an important role in a nation's GDP since, by the time 5G is formally introduced in 2020, there will be 5.5 billion mobile users worldwide.

This sector may turn into a top target for criminal and anti-state activities.

Considering the wide range of 5G services and applications and their vital role in advancing social progress, economic development, and public safety in society. With 5G, there could be a broad threat vector.

5G is more likely to become a focal point for illicit behavior driven by a range of reasons, such as enemies, state-sponsored political goals, cartels involved in organized crime, espionage, and

cyberwarfare.

It will be considerably easier for crooks to avoid detection and keep making money when digital payment systems and technologies like Bitcoin become more widely used.

With a wider range of potential risks, 5G will cover end user devices, mobile core networks, RANs (Radio Access Networks), and the internet.

The network contains a variety of threat kinds, including ransomware, spyware, and bots for smartphones. A MitM attack might be conducted at the cloud RAN domain, whilst a DDoS attack could target the IP core network.

In order to safeguard 5G against sophisticated and intricate attack environments, an advanced security model can provide comprehensive defense against both current and emerging threat types.

2.1.5.3 Threat Analysis for 5G Security

The majority of the threats present in 4G will be carried over into 5G. The following list of sophisticated attacks, which are depicted in the table, may target 5G networks.

Mobile network security monitoring must provide various cutting-edge security services, like:

- Tests for vulnerability
- Flow-based network visibility
- Regular security health assessments for the entire network
- Security alert management system
- Traffic monitoring and inspection

The accelerated rate of development presents opportunities for the creation of novel hacking and cracking techniques for mobile devices and wireless networks.

Three guiding concepts form the foundation of the secure 5G system vision.

- Adaptable security measures
- Extreme internal security
- Distinctiveness

Security protocols need to be adaptable enough to include new technologies, such identity and authentication. The flexibility should allow for the application of encryption for user plane and per-network slice security parameter modifications. Additionally, the security system needs to be automated so that it can intelligently change and adapt to the environment, threats, and security regulations.

Virtualization is used to isolate a system's service model from its physical implementation and to establish virtual linkages in networking, for example.

Beyond only putting security measures in place, cybersecurity professionals in the telecom industry face challenges. It's about determining wisely where to focus our efforts in a dynamic environment. Complex systems have replaced the old, closed, and simple networks, creating new vulnerabilities. Making a cybersecurity start might be difficult to navigate. The need for Telecom Threat Intelligence (TI) is more important than ever as we deal with more complex cyberattacks. Threat intelligence (TI) includes information on possible threats, attack strategies, and projections of future dangers. This information is essential for comprehending the particular difficulties that the telecom industry, which is at the center of international communication, encounters.

5G and the metaverse will merge this year, according to US-based data center equipment vendor Vertiv, to deliver speeds that can keep up with the needs of an extremely advanced technology. According to Vertiv, these two initiatives will come together in 2023, with 5G networks being used by metaverse implementations to provide the extremely low latency features that the application requires.

2.1.5.4 Latest Trends in 5G technologies:

Switching to 5G and beyond makes way for various security gaps and new risks which demands up to date strategies and resources for secure networks. According to GSMA intelligence in operators focus survey 2021 several security concerns arise when 5G based services are provided to operators and businesses. Inadequate knowledge, tools and resources to diminish security vulnerabilities pose as the main obstacle for 48% of the operators.

For 47% of the operators they presume having confidentiality and privacy related liabilities.

41% of operators foresee considerable challenges related to virtualization while 39% acknowledge having inadequate pool of expertise to cope with latest security issues. 63% of the enterprises that utilized IoT services assume having more security issues as most of them did not upgrade their securities policies to encounter the requirements of the latest growing technologies. A number of security challenges and issues demand a more up to date inspection and solutions after being offered 5G based services, which justifies the necessity of dealing with these security concerns.[87]

2.1.5.5 Network Function Virtualization (NFV)

Sharing physical network resources between several tenants or network users is made possible by virtualization, which may lead to security flaws. Virtualization increases availability, but there are significant security implications for confidentiality, integrity, authenticity, and non-repudiation,

according to studies. Since virtual machines are quickly produced, erased, and moved within a network, identifying a hostile virtual computer would be considerably more difficult.

Conversely, virtualization can enhance user and network security. For instance, secure network slicing can isolate communications between various parties, thereby excluding harmful traffic from the network.

2.1.5.6 Software Defined Network (SDN)

SDN centralizes network control onto software-based controller platforms, severing it from the forwarding hardware. The creation, improvement, and quick deployment of novel network features will be accelerated by this, making SDN-based wireless networks a popular area of study. However, softwarizing and centralizing network functions creates additional security risks, like denial-of-service assaults. Thus, new security designs are required for SDN-based networks from the start.

Table 1: Impacts and likelihood of occurrence of different threats.[3]

Threat	Impact	Occurrence
Ransomware	Severe	3
Advanced malware	Extreme	3
IoT botnet	Severe	2
Critical infrastructure threats	Extreme	3
Zero-day attacks	extreme	1

Critical data access is only possible upon payment of the ransom. It has a highly serious effect and a high probability of happening.

Advanced malware has extreme impact as it targets billions of mobiles and IoT devices. It occurs quite often.

IoT botnets have severe impacts due to exploitation of command and control systems. However, it occurs occasionally.

SCADA attacks, such as Stuxnet and Shamoon, have a significant impact since they frequently

target vital infrastructure.

Attacks using a combination of several attack types (malware, rootkits, and botnets) can be used to target unidentified system vulnerabilities. Though rare, it has a profound effect.

2.1.5.7 Security in SDN-based Networks

Open Flow, the current iteration of SDN, is based on traffic flows. Three primary entities comprise Open Flow.

1. SDN application plane: Open Flow apps
2. SDN control plane with Open Flow controllers
3. SDN data plane open flow switches

Strong security for mobile networks is made possible by the SDN paradigm. To guarantee that data moves between approved endpoints and is neither intercepted or redirected during transit, data link security is required. Both Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are supported by the Open Flow protocol.

A 5G network is expected to include multiple control points, which means that control communications between them must be secure.

Traffic monitoring can be used to detect and prevent incursions. Traffic monitoring is made easier by SDN, which enables network programmability and global visibility of network traffic behavior. Control of access SDN provides global awareness of network traffic behavior by centralizing network control and enabling automation through programmability. This makes it possible to easily monitor both traffic entering the network and traffic leaving it, something that was not possible with earlier, more conventional access control methods.

Interaction When faced with difficulties such as equipment breakdowns, operational overload, incorrect settings, or cyberattacks, resilience mechanisms aid a network's ability to function. SDN-based resilience frameworks that provide policy-controlled administration and policy-based network design are developed using resilience approaches.

Accurately assessing current and potential security risks in order to provide cutting-edge security solutions for 5G is need of the hour[3]

2.1.5.8 Business Models for Cyber Security in 5G

Cybersecurity has grown to be a major worry for sectors like online social media, financial services, healthcare, and journalism. Cybersecurity aids in the protection of digital assets for both individuals and enterprises. There are two categories of organizations whose operations depend

on security. First, those who provide security solutions; and second, those who face the possibility of cyberattacks and have notable digital footprints.

Cybersecurity in 5G should address issues with security and privacy in addition to standard data security.[3]

2.1.5.9 Physical Layer Security

Many applications in today's world, such as bank services, machine-to-machine communications, e-commerce, broadband internet, radio terminal payments, remote health and hospital services, etc., rely on the security of radio interfaces on wireless networks.

Cryptographic procedures in wireless network they are placed on the top layer and are either symmetric (based on a shared secret that is unknown to others) or asymmetric (based on public and private keys), provide the foundation for most commonly used security measures. The processing capacity of the attacker influences how quickly a code word can be cracked. Physical layer security doesn't assume anything about the attackers' level of computing power. The first layer, or the physical layer, is crucial since data security is vital at all levels.

There are now two accepted methods for securing communications. The first method enhances current protocols with encryption and authentication. In the second, physical layer security technologies are embedded.

Blind physical layer security (WBPL Sec), which uses watermarks, is a dependable defense against eavesdropping and other information leak assaults. WBPL Sec system model, where secrecy is provided by both the water marking and the jamming receiver. The required information is provided by the chosen watermarking technology, which is destroyed during jamming. Those mobile devices that have several air interfaces can effectively use the WBPL Sec. Software-Defined Radio (SDR) is expected to be prominent when those air interfaces are used to new designs in the 5G network. Thus, to provide physical layer security solutions in 5G devices, WBPL Sec with SDR is used. [3]

2.1.5.10 5G-WLAN Security

WiFi (Wireless-Local Area Network)

The IEEE 802.11 standards-based radio technology known as WiFi (Wireless Fidelity) operates in licensed spectrum bands (2.4 GHz or 5 GHz ISM bands) for short-range communication.

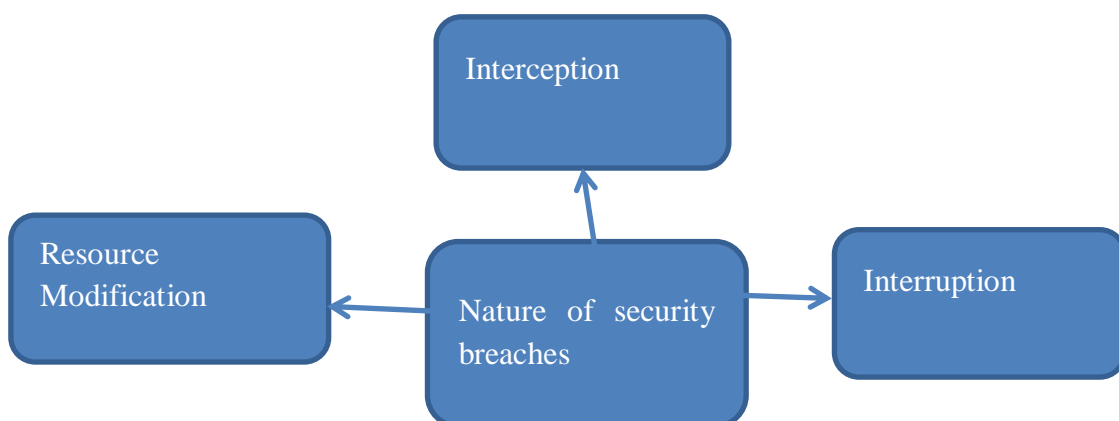
WiFi Security

5G radio access technology will offer extremely high data rates, low latency, ultra-high dependability, energy efficiency, and device density. 5G networks could be implemented with the help of current radio access technologies and LTE advancements. Furthermore, for machine-to-

machine (M2M) and internet-of-things (IoT) connectivity, LTE's compatibility with state-of-the-art radio access technologies and fast wired backbone networks is essential. 5G's wireless connectivity opens up a world of new applications, including time-sensitive industrial processes, smart homes, traffic safety and control, and essential infrastructure. This exemplifies the kinds of uses for 5G networks and the viability of attaining universal connectivity for all devices.

With small cells densely arranged in current circuit switched cellular networks, 5G networks are incredibly diverse. In addition to offering incredibly high data rates with strict latency requirements, 5G heterogeneous networks are making security provisioning increasingly difficult. All people, everywhere (IoT) and smooth communication between people and machines as well as between machines and other machines wherever they are, anytime they need to, and via any electronic devices, services, or networks they choose (anyway) are the objectives of 5G networks. Because of this, it's critical to plan, create, and implement security protocols (authentication, secrecy, and integrity) that safeguard data when packets are switched between network technologies via interoperability.

There are several security concerns according to the nature of security breaches, as shown in figure 1 below. The first is interception which is carried out through control/data signaling. The hacker obtains the information but does not alter or remove it. This type of attack compromises both the subscriber's and the network operator's privacy. Another concern is resource modification whereby the hacker causes harm to the system by altering system resources. In interruption, the hacker attempts to halt the process by crashing system resources, such as subscriber data, signaling messages, delivery stops, etc. Reply attacks is another security issue where the hacker may bring fraudulent objects into the system (such as false messages, phoney service logic, or counterfeit subscriber data) depending on the target and type of physical access[4].



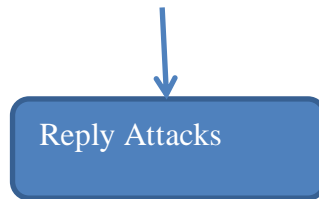


Figure 1: Security concerns according to the nature of security breaches.[3]

Security flaws depending on the attack’s methodology are shown in figure 2. Attacks based on data occur by changing, adding or removing data from the system, the hacker attacks the data kept in the 5G communication network and creates harm. Attacks based on messages, where the hacker targets the 5G system by adding, deleting, replaying and discarding control/data signaling to and from the network. Service logic attacks also works similarly to the attacks based on messages. [4]

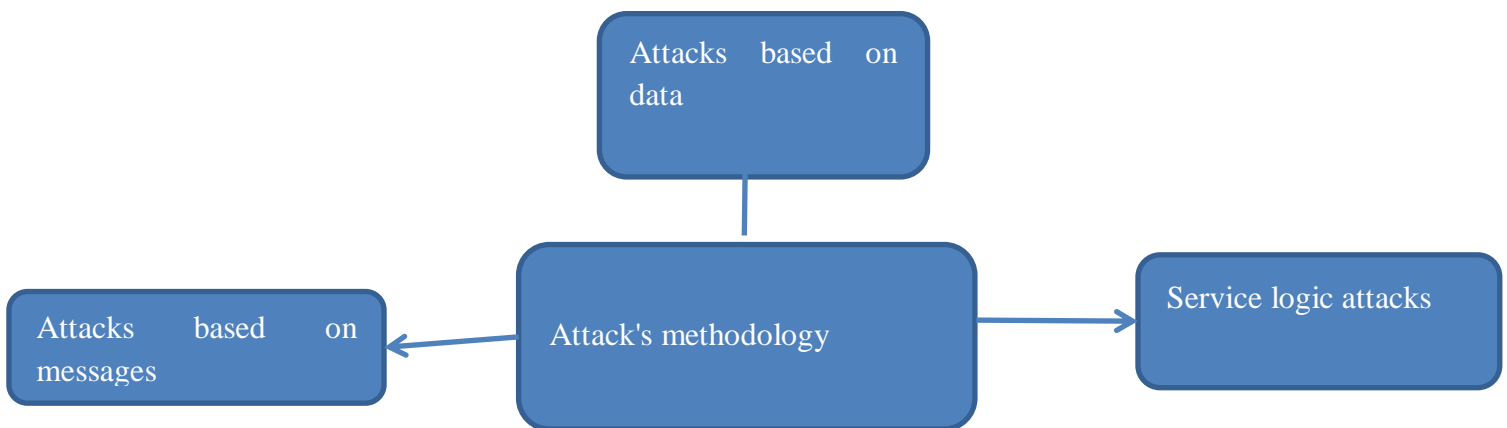


Figure 2: Security flaws depending on the attack’s methodology.[3]

Concerns of security based on the degree of physical access are divided into classes, as shown in figure 3 below. In class I, after employing a physical device to get access to the radio interface, the hacker broadcasts the radio signal at a higher frequency, eavesdrops and launches “man in the middle attacks” using the modified mobile stations (eNodeBs). In class II, the physical cables that connect the 5G network switches are compromised, allowing the intruder to potentially cause significant harm by interfering with the regular transfer of control and data signaling messages. In class III, the hacker will be able to access some of the most sensitive parts of the network and cause significant harm to service by changing the logic used to provide the service or the subscriber data stored in the 5G network entity. In class IV, the intruder can cause disruptions through communication channels connecting the internet to the 5G network by transmitting control/data signaling messages into the link between the two heterogeneous networks. In class V,

by modifying the subscriber data (security services and profile) saved in the cross-network servers or by manipulating the service logic, a hacker can harm mobile users connected to the 5G network. The internet servers or cross-network servers that offer these subscribers' services are accessible to the hacker [4].

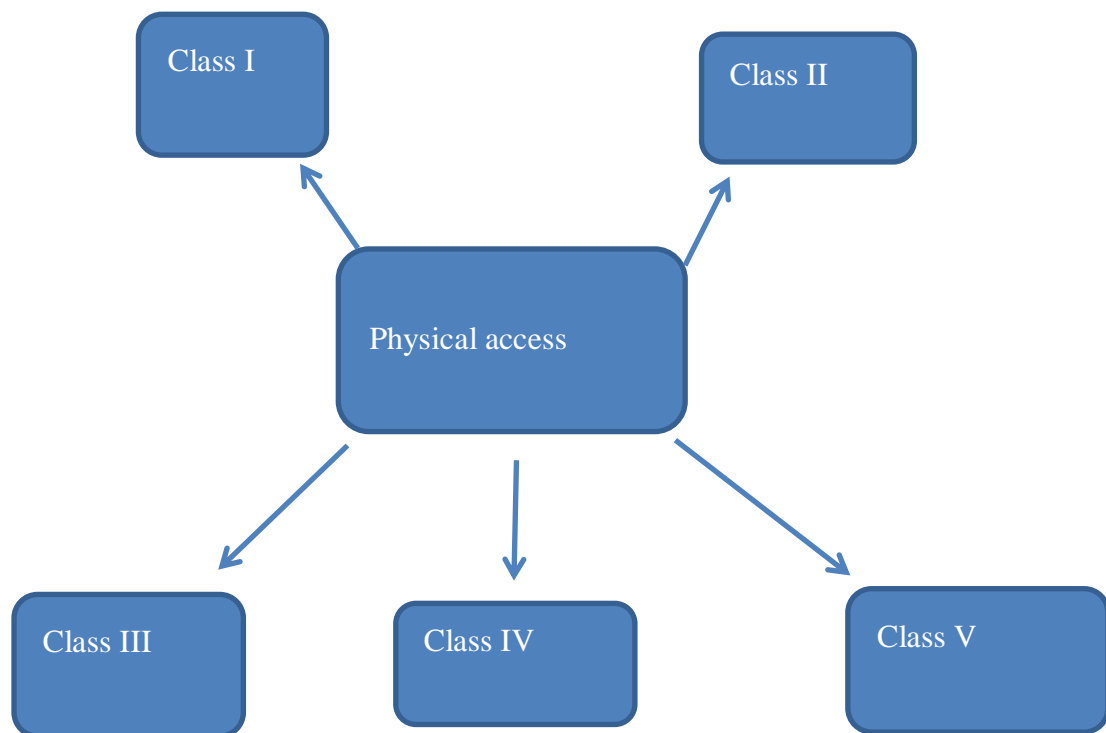


Figure 3: Concerns of security depending on the degree of physical access[3]

Security issues based on access of unauthorized sensitive data are highlighted in figure 4 below. Eavesdropping, is where the hacker keeps an eyes on how the communication network is operating in order to intercept messages. Masquerading, where the hacker impersonates a genuine user and tricks an authorized user into revealing crucial information in order to get access to the communication network or the end user. Analysis of the traffic flow; in order to determine the user's location, the hacker listens in on the communication flow and records its duration, rate, time, source, and destination. Next is browsing, where the hacker looks for data storage in order to find the sensitive information. Data leakage, which occurs by taking advantage of the methods for gaining access to the genuine user data, the hacker obtains sensitive information. Inference,

where an intrusive party sends a query or control/data signal to a system to see how it responds.
[4]

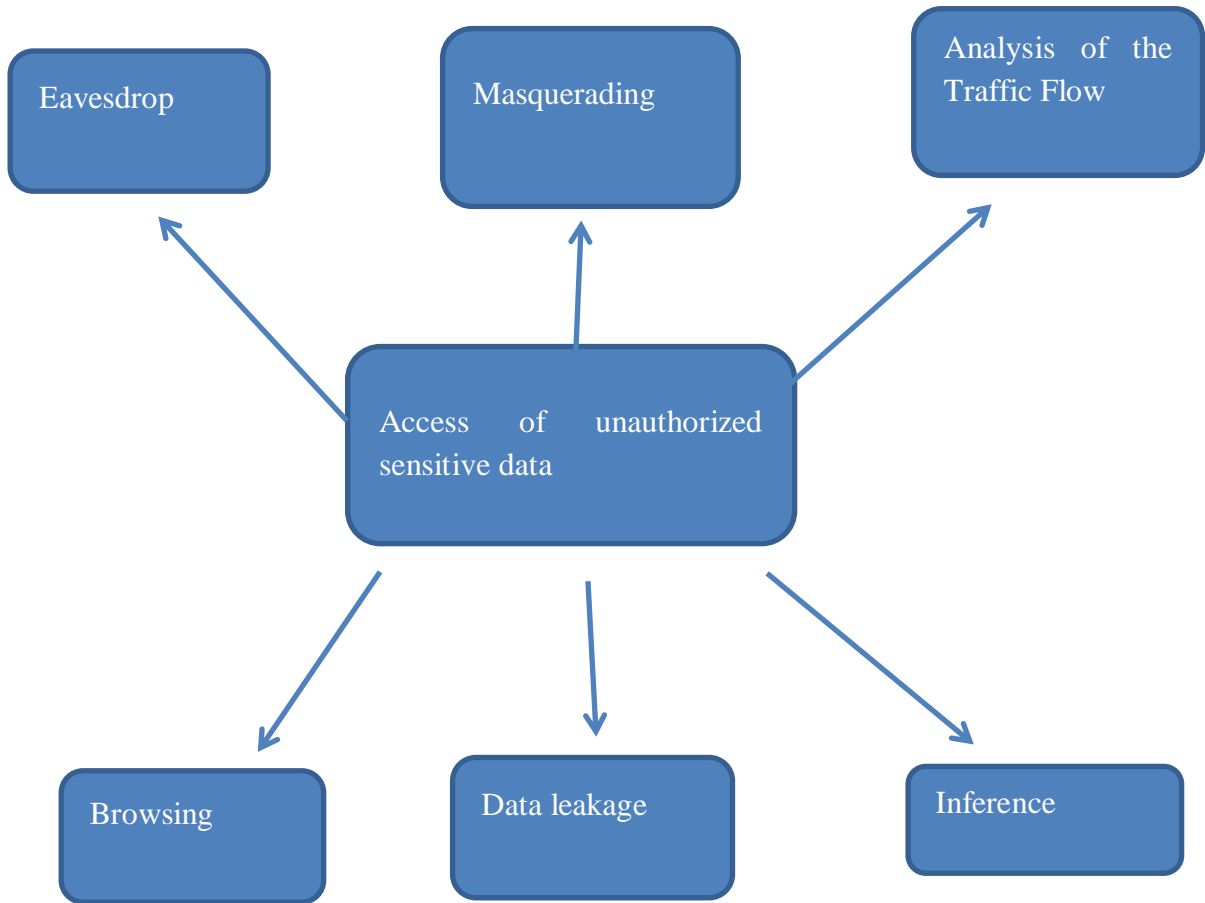


Figure 4: Security issues: Access of unauthorized sensitive data.[3]

Security issue caused by manipulation of sensitive data is shown in figure 5. The Modification of user information, where an intentional hacker may purposefully alter, add, replay, or remove user data. [4]

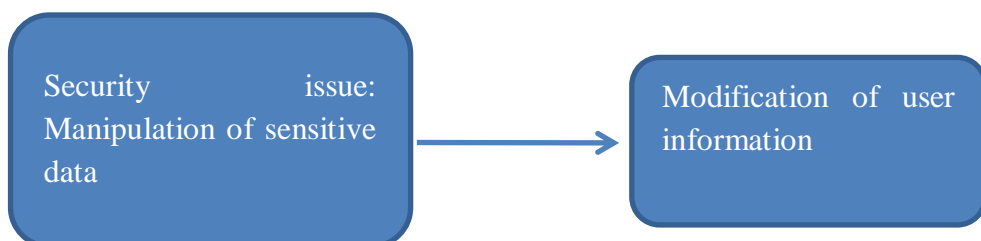


Figure 5: Security issue due to manipulation of sensitive data.[3]

Figure 6 shows the security issue caused by unauthorized access to services. Access Rights are compromised and the hacker will gain access to the services by impersonating end users or network organizations. [4]

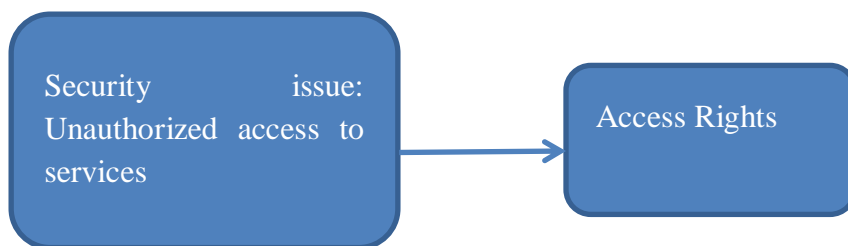
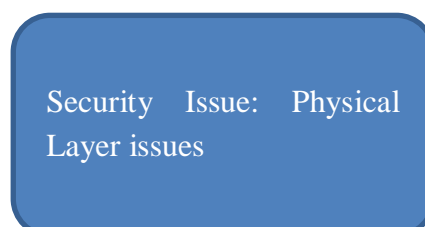


Figure 6: Security issue: Unauthorized access to services.[3]

Security issues caused at the physical layer are shown in figure 7. Inference, when someone purposefully introduces artificial interference onto a communication channel, the high signal to noise ratio. Scrambling- This kind of interference is set up by brief intervals of time.

A service is intended to be disrupted by a specified frame. Implementing this kind of security attack in a communication network is quite difficult.[4]



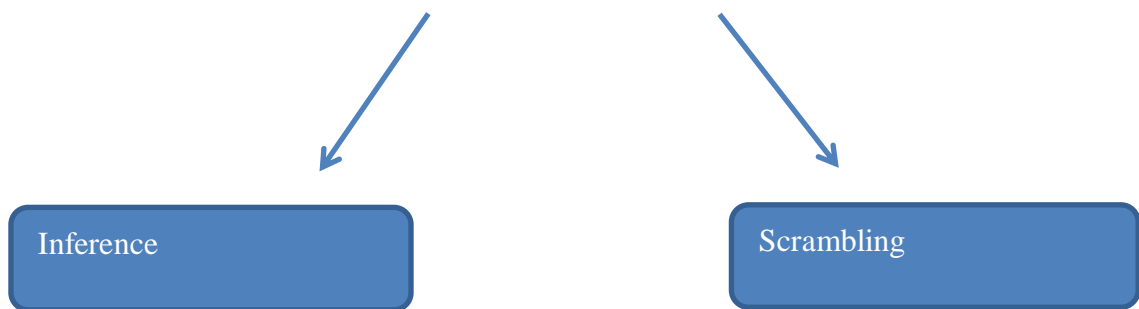


Figure 7: Security Issue: Physical Layer issues.[3]

Security issues caused at the Medium Access Control (MAC) level are highlighted in figure 8. Location Tracking- The hacker searches for user equipment inside the coverage area of one cell or across many cell coverage regions. Bandwidth stealing- The hacker uses fake buffer status reports or messages injected during the Discontinuous Reception (DRX) period to create this kind of attack. Open architecture security issues- An open design of an IP-based 5G network raises more security risks because these networks are I-enabled and have a large density of dynamic, highly mobile devices. Security issues at higher layers- The transition from proprietary to open and standardized operating systems for portable devices, coupled with the open architecture and protocols of the LTE wireless network, presents an increasing number of possible security risks. These attacks can come in a variety of shapes and sizes, including viruses, Trojan horses, and malware[4].

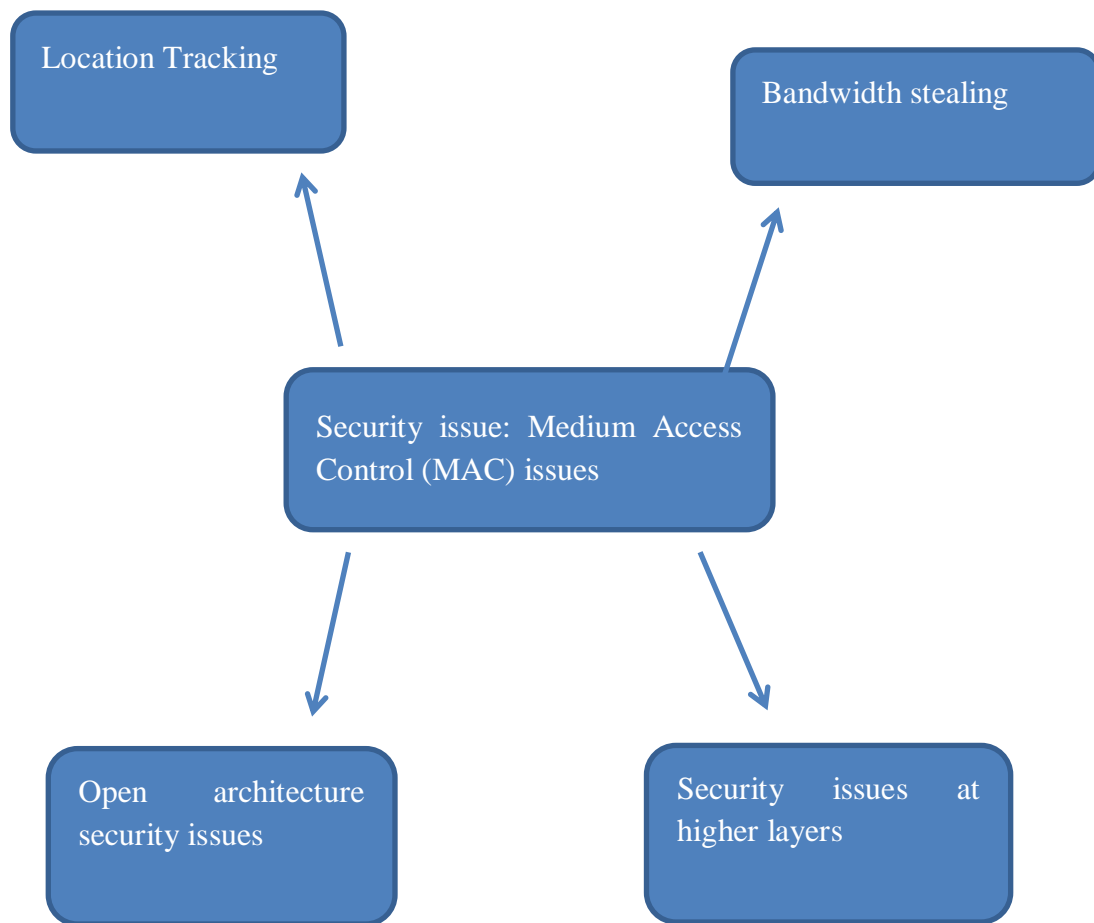


Figure 8: Security issue: Medium Access Control (MAC) issues.[3]

Security issues in packet switched network

Table 2: Security Issues in packet switched networks[3]

Security issue type	Security issue description- based on attack type
De-authentication	<p>The hacker aims to interfere with Wireless LANs' authentication system. By doing this, the hacker obtains the identity of the authorized wireless users.</p> <p>In addition, without first finishing the security procedure and evaluation, the hacker tries to take over the deployment powers of authorized wireless access points in order to establish rogue access points.</p> <p>Some possible security threats that fall under this category are as follows:</p> <p>i) IP spoofing: using the end-user's source IP address to impersonate a valid user, the hacker can evade IP address-based verification; ii) MAC spoofing: the hacker can get around MAC filtering regulations by altering the MAC address of a wireless client; iii) Rogue access points: By setting up an illegal wireless access point, an intruder can have unrestricted access to the WLAN.</p>
Eavesdropping and interception in wireless domain	<p>The intruder can listen in on or intercept the genuine wireless traffic flows by breaking into the radio access channel used by the legitimate users. He may now access all of the data that the end user transmits thanks to this.</p> <p>The following categories of security attacks are included in this category:</p> <p>i) Man-in-the-middle attacks: by observing in the center of the two-way communications, the attacker tries to gain, intercept, alter, and mimic the end-to-end communication between the source and destination, thinking they have a secure channel; ii) Network traffic eavesdropping: the hacker listens in on all network traffic over the Wireless LAN using a network sniffer; iii) Network injection: the hacker spies on actual user traffic by injecting fictitious network traffic into it in an effort to carry out destructive tasks;</p> <p>iv) Session hijacking: the hacker will take control of the entire session of a particular traffic flow between the source and the destination by stealing a valid, authorized conversation session ID.</p>

Traffic jamming	The hacker uses strong radio frequency signals, a lot of WLAN bandwidth, or floods the network with fake messages in an attempt to drown out legitimate activity. This group of attacks includes the following ones: Hackers can use two methods to interrupt genuine user traffic and reach their target: (i) Denial of Service (DoS) attacks, in which they send bogus messages or high-frequency radio signals; (ii) Spam assaults, in which they exploit wireless communication channels to send out a large number of spam messages to the recipient.
Brute force attack to take control of passwords for Access Points (APs)	The hacker leverages brute force dictionary attacks to compromise the access point's single shared password (in point-to-point (P2P) connection) by attempting every possible password.
Attack against security protocols	By changing, adding, or removing data from the system, the hacker attacks the data kept in the 5G communication network and creates harm.
Attacks based on messages	The hacker exploits holes in the current WiFi Protected Access (WPA) and Wired Equivalent Privacy (WEP) security mechanisms.
Misconfiguration	To take over the access point, the hacker takes advantage of the WLAN administrator's inadequate security expertise, user error, or incorrect operation.

2.1.6 Sixth Generation Cellular System

In next-generation networks, the functions of trust, security, and privacy are distinct yet partly related. The development of a reliable 6G faces diverse issues in the fields of politics, techno-economics, technology, legislation, and ethics.

Decentralized systems, in which users can join and exit at will to form a dispersed system, have been emerging on the open Internet without the need for controllers. This means that the end systems will handle the trust issue. A typical method relies on a third party to validate the accuracy of the services in order to verify participants' trust in the services. The inability of the parties to agree on a single third party that can be trusted frequently results in the employment of multiple third parties concurrently, which lowers overall security.

When conclusive information about dynamic trust relations is generated in 6G, it may be kept in a DL and the linked parties' potential conclusive answers may be appropriately handled.

Consequently, a long-term history that reflects the various parties' long-term reliability or quality may be generated. This could be used to promote longer-term enhancements in the 6G operations.

Mobile networks have relied on the physical storage of symmetric keys on a Subscriber Identity Module, or SIM card, since the advent of digital mobile communication in 2G. International standards replaced traditional encryption algorithms, and new cryptographic techniques were introduced to enable mutual authentication. But at its core, 5G's security approach still depends on SIM cards. Even though SIM cards have shrunk to "nano" size, they still require a plug to function, which restricts their use in applications like Internet of Things. This obstacle is partially addressed by the introduction of eSIMs, although physical size issues remain. Future devices may use the iSIM, which is now under development, as part of their System-on-Chip, despite operators' objections regarding potential control loss.

The paradigms of quantum and conventional computing are essentially distinct from one another. Certain computational problems remain unsolvable on modern computers, but there exist quantum computing methods that can tackle them effectively. Among these is the discrete logarithm issue, upon which contemporary asymmetric cryptography is built.

Automated security using the ideas of security function softwarization and virtualization, as well as machine learning, will become inevitable as 6G moves toward THz spectrum with much higher bandwidth, more densification and cloudification for a hyperconnected world by connecting billions of devices and nodes with global reach for terrestrial, ocean, and space. Security systems utilizing the current principles of SDN and NFV need to be further upgraded with embedded intelligence for dynamicity to match the needs of 6G security in order to alleviate limits in the security of both current and evolving 5G networks.

In order to guarantee end-to-end network security and deliver the required services, 6G networks will merge the ideas of SDN, NFV, and AI into a cohesive whole. AI will be able to proactively detect threats and start the transfer of security functions from one point to another across the network by utilizing programmable interfaces on programmable forwarding planes, allowing the deployment of softwarized security functions similar to VNFs in any network perimeter or instance in a virtual environment.

In the smartphone era, cloud computing has emerged as the primary paradigm for service provisioning with the introduction of virtualization and softwarization.

The number of connected devices, their density, and their service requirements will increase significantly with the inclusion and anticipated further fusion of the IoT and mobile telecommunications domains. This will necessitate a significant increase in the number of network access points, network capacity, and service capabilities that are available. Given the performance limitations of ordinary IoT devices, it is therefore reasonable to assume that the offloading of computing, storage, and networking capabilities to other nodes will expand with the success of 5G, generalize, and eventually become a standard feature in 6G.

The research community has focused much of its emphasis on two physical layer technologies: (1) Cell-free massive MIMO and (2) Intelligent reflective surface (IRS). Right now, these two are the most promising options for the physical layer of 6G communication networks.

Physical layer security (PLS) can be a key component in cutting down on the complexity and latency of new security standards. In order to fulfill the demands of 6G networks, it is anticipated that the sharp rise in high data rate services would continue. Visible Light Communications (VLC), a variation of optical wireless communications, and other variants provide appealing qualities such as unlicensed spectrum, high capacity, intrinsic security, high degree of spatial confinement, and resilience to electromagnetic interference[5].

2.1.7 Identifying Potential Threats and Challenges

Based on anticipated 6G technologies at the physical, connection, and service layers as well as lessons gained from the shortcomings of current security designs and cutting-edge countermeasures, Security and privacy for 6G: A survey on prospective technologies and challenge offers a methodical summary of security and privacy concerns[6].

Preventive security measures and cooperation between network providers, device manufacturers, and users are crucial to ensure a secure future alongside the transformative power of 6G. Although 6G promises a future of lightning-fast connectivity, its complex web of devices and reliance on AI create new security challenges. Network vulnerabilities, sophisticated cyberattacks, and the vast amount of data flowing through the system raise concerns about data privacy and potential manipulation of AI.

Table 3: Attack name and associated risk[3]

Target	Attack name	Risk
Availability	Signaling DoS attacks	High
	Paging DoS attacks	High
	DDoS Authentication server	High
	SMS Saturation attacks	High
	Energy Depletion attacks	High
Integrity	Cloning attacks	High
	SIM card rooting	High
	Partitioning attacks	High
	Impersonation attacks	High
	Voice IP attacks	High
Confidentiality	SMS interception	Medium
	IMSI-catcher	High
	Traceability attack	High

Table 4: Security and Privacy issues at each layer[3]

Layer	Security and Privacy Issues
Physical Layer	Eavesdropping, jamming
	Location jamming
	Compromised IoT devices
Connection Layer	Man in the Middle
	DoS, DDoS attacks
	IP spoofing
	SDN controller attacks
	Traffic trace
Service Layer	Malware/Virus/spam
	NFV and VNF attacks
	Malicious micro-services
	Data breach

Some noteworthy vulnerabilities have been discovered as a result of research done in the 5G community and existing published standards. Future iterations of the standards can address these vulnerabilities, and once 5G standards are established, mitigation for some of them should be in place. This article addresses three categories of vulnerabilities: Availability, Integrity, and Confidentiality (CIA). The cornerstone of security policy and the one that determines the most important aspects of security is the so-called "CIA triad." [7].

Table 5: Security principle, threat and impact[3]

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

Table6:Threats based on Nefarious Activity/Abuse of Assets (NAA) and areas of impact[3]

Threat type	Threats	Areas of Impact
Nefarious Activity/Abuse of Assets (NAA)	Data forgery and network configuration manipulation - Manipulation of routing tables - Tampering with CORE configuration data - DNS manipulation - Data manipulation pertaining to radio technology settings and access networks - Taking advantage of improperly or incorrectly constructed networks or systems - Malicious network functions registering; - Tampering with security data (cryptography keys, security policies, access rules, etc.). - Tampering with operating system (OS) services - Network implementation data	Integrity and Availability
	Taking advantage of hardware and software flaws - Zero-day vulnerabilities Utilizing edge open application programming interfaces (APIs) inappropriately; - Exploiting APIs - Modification of software - Abuse of system execution	Integrity and Availability
	Distributed denial of service (DDoS) is a type of denial of service (DoS). - Flooding base stations; - Flooding critical network components - Attacks by amplification - Attacks at the MAC layer - Overloading the edge node; - Authentication traffic spikes; - Jamming the network radio; - Jamming device radio interface; - Jamming base station radio interface	Availability and Outage
	Exploitation of remote access -hijacking of the intra-RAT mobility mechanism -hijacking of the RAT session	Integrity and Confidentiality
	malicious software or code - Rootkits - Injection attacks (SQL, XSS) - Ransomware - Botnet - Worms/trojan - Rogueware - Malicious functionalities on networks; - Attacks by malware on network goods; - Attacks by malware on business applications	Integrity and Availability

	<p>Abuse of external remote services for network products (such as VPNs)</p> <ul style="list-style-type: none"> - Abuse of remote access to the network 	<p>Integrity and Confidentiality</p>
	<p>Misuse of disclosed information</p> <ul style="list-style-type: none"> - Data theft and/or leakage from cloud computing - Theft and/or leakage from network traffic - Theft or loss of security keys - misuse of security data obtained from audit tools - uncertified access to user plane data - uncertified access to signaling data 	<p>Integrity and Confidentiality</p>
	<p>Abuse of authentication: An increase in authentication requests</p> <ul style="list-style-type: none"> - Employees of third parties abusing user login and authorization data - Abuse of the key agreement process and application management function (AMF) authentication • Abuse the login information for current accounts 	<p>Integrity and Availability</p>
	<p>Hardware and software manipulation</p> <ul style="list-style-type: none"> - Modification of hardware apparatus - The orchestrator of network resources being manipulated - Memory scraping - Attacks via side channels <p>A phony network node for access</p> <ul style="list-style-type: none"> - Rogue or false MEC gateways; - Exploitation of the UICC format; - Compromised UEs; - Inadequate UE security capabilities - Software backdoor 	<p>Integrity and Availability</p>
	<p>Data leaks, thefts, manipulations of information</p> <ul style="list-style-type: none"> - tampering with network product logs - abuse of file write permissions - mishandling ownership files - customer data breaches - thefts of personal information 	<p>Integrity and Confidentiality</p>
	<p>Unauthorized actions or incursions into networks</p> <ul style="list-style-type: none"> - IMSI detecting assaults - Brute force - Lateral movement - Port knocking 	<p>Integrity</p>

	Account or service fraud including identity - IP spoofing - MAC spoofing - Identity theft - Identity spoofing	Integrity and Availability
	Spectrum Sensing	Availability
	Supply chain, vendors, and service providers compromised - Abuse of personnel from third parties that have access to MNO facilities - Tools for network product development tampering - Tools for configuring network products - tampering with the source code of network products - manipulating updates for network products	Integrity and Availability
	Abuse of virtualization methods - circumvention of network virtualization - abuse of virtualized hosts - manipulation of virtual machines - dangers to data centers - Abuse of cloud computing resources - Cloud container image implant - Cloud container image backdoor	Availability and Integrity
	Signalling threats - signalling storms - signalling frauds	Integrity and Availability

Nefarious activity/Abuse of Asset (NAA) includes Data forgery, DDoS, exploitation of remote access, malware software or code. Abuse of external remote services and misuse of disclosed information. It also includes abuse of authentication, hardware and software manipulation, data thefts, leaks and manipulation of information. Unauthorized incursion into network, account or service fraud and abuse of virtualization methods. All types of NAA cause integrity, availability and confidentiality issues.

Table 7: Threats based on Eavesdropping/Interception/ Hijacking (EIH) and areas of impact[3]

Threat type	Threats	Areas of Impact
-------------	---------	-----------------

Eavesdropping/ Interception/ Hijacking (EIH)	Nation state espionage	Integrity and Confidentiality
	Corporate espionage	Integrity and Confidentiality
	Traffic sniffing	Integrity and Confidentiality
	Network traffic manipulation, information collection, and reconnaissance - radio network traffic manipulation - malicious traffic diversion - traffic redirection - misuse of roaming connectivity	Integrity and Confidentiality
	Man in the middle/Session hijacking - Rogue base station hijacking via hijacking sessions - Rogue base station downgrade attacks	Integrity and Confidentiality
	Information interception - Data eavesdropping through hacked small cell - Eavesdropping on unencrypted message content - Device and identity tracking through rogue base station - Eavesdropping on air interface	Integrity and Confidentiality

Eavesdropping/Interception/Hijacking(EIH) include nation state espionage, corporate espionage, traffic sniffing, network traffic manipulation, man in the middle/session hijacking and information interception. These threats effect integrity and confidentiality of data.

Table 8: Threats based on Physical Attacks and areas of impact[3]

Threat type	Threats	Areas of Impact
Physical attacks (PA)	Sabotage of network infrastructure (radio access, edge servers, etc.) - Hardware additions	Integrity and Availability
	Vandalism of network infrastructure (radio access, edge servers, etc.)	Integrity and Availability
	Physical asset theft	Integrity and Availability
	Terrorist attack against network infrastructure	Integrity and Availability
	Fraud by MNO employees	Integrity and Availability

	Unauthorized entry into shared locations' based stations	Integrity and Availability
--	--	----------------------------

Physical attacks include sabotage of network infrastructure, vandalism of network infrastructure, physical asset theft, terrorist attack against network infrastructure, fraud by MNO employees and unauthorized entry into shared locations' base stations. These threats impact integrity and availability of data.

Table 9: Threats based on unintentional damages (accidental) (UD) and areas of impact[3]

Threat type	Threats	Areas of Impact
Unintentional damages (accidental) (UD)	improperly configured or misconfigured networks and/or systems	Integrity and Availability
	Poor planning and design, or a failure to adapt - Outdated systems or networks due to inadequate update or patch management - Configuration change management errors - Network and system architecture with poor design	Integrity and Availability
	misuse or mishandling of the network, systems, and equipment	Availability and Integrity
	Information sharing and leakage brought on by human mistake	Integrity and Confidentiality
	Loss of data due to inadvertent deletion	Integrity and Confidentiality

Unintentional damages (accidental) (UD) threats include improperly configured or misconfigured networks, poor planning and design, misuse or mishandling of the network, Information sharing and leakage brought on by human mistake and Loss of data due to inadvertent deletion. These threats impact integrity, confidentiality and availability of data.

Table 10: Threats based on failures or malfunctions (FM) or outages (OUT) and areas of impact[3]

Threat type	Threats	Areas of Impact
Failures or Malfunctions (FM)	malfunction of the systems, devices, or network	Availability and Integrity
	Communication link failure or disruption	Integrity and Availability

	Main power supply failure or disruption	Integrity and Availability
	Service providers' failure or disruption (supply chain)	Integrity and Availability
	Equipment malfunction (devices or systems)	Integrity and Availability
Outages (OUT)	Depletion of resources: People and physical resources	Integrity and Availability
	assistance services	Integrity and Availability
	Data network (access)	Integrity and Availability
	Interfering radiation	Integrity and Availability

Failures or malfunctions (FM) threats include malfunction of the systems, devices, or network, Communication link failure or disruption, Main power supply failure or disruption, Service providers' failure or disruption (supply chain) and Equipment malfunction (devices or systems. These threats impact integrity and availability of data.

Outages (OUT) threats include depletion of resources, assistance services, Data network (access) and Interfering radiation. These threats impact integrity and availability of data.

Table 11: Threats based on disasters and legal issues, and areas of impact[3]

Threat type	Threats	Areas of Impact
Disasters (DIS)	Landslides, earthquakes, and other natural calamities	Integrity and Availability
	Natural disasters: storms, floods, pollution, dust, and corrosion - Flames, strong winds Unfavorable weather circumstances	Integrity and Availability
	Legal (LEG)	Breach of service level agreement (SLA)
	Breach of legislation	Integrity and Availability
	Failure to meet contractual requirements and/or legislation	Integrity and Availability

Disasters (DIS) threats include landslides, earthquakes and natural disasters like storms, floods, pollution, dust, and corrosion. These threats impact integrity and availability of data.

Legal (LEG) threats include breach of service level agreement, breach of legislation and failure of meet contractual requirements. These threats impact integrity and availability of data.

2.1.7.1 Threat Analysis and Prioritization

Categorization/Prioritization of Threats

Confidentiality Threats

- Snooping
- Collaborative
- Man-in-the-Middle (MitM)
- Chosen Plaintext
- Impersonation
- Disclosure
- Stalking
- Eavesdropping

Most prone area is related to MitM threats. Here, attack occurs in the middle of two communicating parties. False base station play important role in such attacks [8]. Public key cryptographic solutions are required to counter such attacks. [9]. Artificial intelligence (AI)-based machine learning is also being used for enhancing security in smart cities which can also encounter many threats including man-in-the-middle [11].

Blockchain-based authentication mechanisms are also used as in eavesdropping, there is compromised confidentiality, through data transmission via unsecure channels. Therefore, it is recommended to use blockchain-based confidentiality probability indicators to determine the extent of data secrecy [12].

Data aggregation through multiple statistical functions provide security regarding text chosen attacks [13]. Blockchain-based transparent data management can address attacks related to disclosure of confidential data [14].

Availability Threats

- Redirection
- Free-riding
- Physical
- Environment

- FIFO
- DDoS
- SYNC Flood

An energy-efficient topology for preventing DoS assaults in 6G networks is the DoS attack identification approach which can be utilised for such attacks [15]. Embedment of concept of virtual shadow network in security architecture of virtual networks can successfully address traffic redirection attacks [16]. To prevent RF-saturated environments, which can pose availability risks, intelligent interference reduction is necessary [17].

When entry/exit time interval of data or communication is gathered or predicted by adversary, FIFO attacks occur. For this, ML-enabled IDS system is required [18]. Currently, federated learning is being employed in 6G. Much emphasis is required to keep this in mind while developing secure communication network as free riding attacks can occur in federated learning-based models [19].

In order to encounter conventional flooding attacks due to possible vulnerabilities of following protocols, intelligent mechanisms are required. The aforementioned protocols include internet control message protocol (ICMP), hypertext transfer protocol (HTTP), and transport control protocol (TCP) [20].

Integrity Threats

- Message append
- Alteration
- Data diddling
- Session hijack
- Tampering

Blockchain methods are being explored for 6G-enabled IoT integrity measures. Blockchain methods based on machine learning can handle data integrity [21]. There are difficulties for 6G-enabled IoT since different cryptographic approaches to handle message addition, change, and manipulation result in enormous processing overheads in dense communication [22]. Attacks like time-specific session hijacking jeopardize the integrity of data exchange. In a fog computing environment offered by 6G, this may lead to further security incidents [23]. Similarly, data diddling causes some integrity problems while communicating messages. According to recent

studies, 6G-enabled IoTs can prevent data diddling by using QR-code-based secret sharing [24].

Authentication Threats

- Forgery
- Brute force
- Reuse threat
- Password
- Partial collision recovery

In communication environment, all those entities which portray themselves as legitimate entities, easily attack password-based authentication schemes. An attacker use various cryptographic methods to obtain secret keys, hash et cetera in partial collision. Radio access network (RAN) is more prone to collision based attacks [25]. Lightweight authentication scheme can be used to encounter forgery attacks in 6G-enabled maritime transport system [26]. Key establishment protocols and anonymous mutual authentication can enhance protection against message recovery attacks in 6G-enable IoT. Conventional protocol like Voice-over-Long-Term Evolution (VoLTE) protocol is risky regarding key stream reuse. Hence, critical analysis of such protocols is required to address such reuse attacks [27]. AI-based security schemes having proven strength against brute force attacks are being designed [28]. Public key cryptography in combination electronic subscriber identity module (eSIM) enhances protection against replay attacks [29].

Access Control Threats

- Social engineering
- Access aggregation
- Birthday
- Cloning
- Phishing

Organisations pertaining to proprietary or other sensitive information related things are more prone to access control threats. Hence, protection of vital information form unauthorised access by implementation of computer-based control is required. As such attacks are very sophisticated and advance in nature, Thus, a variety of blockchain-based applications can be used to create access control and other security measures. Social engineering poses a significant risk to 6G-enabled IoT smart infrastructure. It is necessary to create key management protocols based on blockchain.

Data mining attacks are result of illegitimate accumulation of data that seems to be insensitive or unidentified from 6G-enabled networks. Unconventional birthday attack resistant algorithm are required in post-quantum era of 6G communications.

Similarly, for cloning attacks, cloning theorem-based quantum computing is not a likely solution. To diminish 6g mm wave beam prediction aattacks adversial learning algorithms are suggested. Here, data can be destroyed by phishing attacks leading to hindrance in performance of artificial intelligence-based models in 6G spectrum management.

2.1.8 Framework Development and Review of Best Practices and Existing Solutions

As compared to the previous generations of network, 5G has designed its security controls to counteract current threats. These control mechanisms include new mutual authentication capabilities, improved subscriber identity protection etc. New technologies adopted by 5G offer new threats of their own kind. In the light of this, 5G is being developed on the principle of “secure by design”.

Five-generation (5G) networks must be secured using multiple strategies. Strong segmentation in network slicing allows for the isolation of sensitive data, and end-to-end encryption safeguards data while it's in transit. Strong identity and access management with multi-factor authentication guarantees that only authorized users can access the network, and proactive monitoring with advanced threat detection systems aids in identifying and addressing security threats. Ultimately, it's critical to maintain network software updated with the most recent updates in order to remove any vulnerabilities that an attacker could exploit.

For the aforementioned principle, trust between sender and receiver can be established via mutual authentication. Users of 5G should presume it as an open network and employ safety methods at their own ends, too. Keeping in view, the frequent interceptions of network traffic encryption is mandatory. As business is being conducted more and more on this network, 5G has to be more secure than its predecessors.

Following are the best practices for upcoming 5G security:

2.1.8.1 Development models

Among multiple implementation models for 5G standards, non-standalone (NSA) mode is the only option currently being employed. In this, 5G uses a combination of existing 4G LTE architecture with a 5G RAN.

In next phase of 5G, standalone (SA) mode will be deployed where 5G RAN and a cloud native 5G core is used. Survey showed that operators are planning to deploy SA 5G within next 3 years. (Source: GSMAi, 2019)

2.1.8.2 Subscriber and device protection

User data and device data confidentiality and integrity is being planned to improve in future by following measures:

- Enhancing the confidentiality of initial non-access stratum (NAS) messages (protocol to facilitate communication between users) between device and network resulting in protection against attacks like man in the middle (MiTM) and fake base station attacks
- ‘Home control’ protection mechanism will be used to prevent various roaming fraud types thus enabling operators to authenticate devices correctly to the services
- 5G networks would be able to manage all unmanaged and unsecured connections by performing reauthentication of user equipment
- User plane integrity checking will ensure safe transit meaning that user traffic cannot be modified during transit
- Public/private key pairs will increase privacy by concealing the subscriber identity

2.1.8.3 Network Protection

Ensuring data’s integrity is vital for network protection. Hence, for this purpose, 5G is introducing/proposing a new architecture called “the security edge protection proxy” (SEPP). Under the arrangement SEPP acts as a security gateway between home and visited networks. Therefore, SEPP is able to provide security for application layer, end to end CIA via signatures and encryption, key management for required cryptographic keys and procedures, message filtering and topology hiding and validation of JSON objects.

This architecture is designed to mitigate the existing security risks posed to SS7 and diameter usage. Adding a dedicated security mode within the standards for 5G development is a remarkable achievement.

JSON I.e. JavaScript object notation, is a data format for storage and transmission between server and web application.

2.1.8.4 New IP Protocol Stack

Traditionally, each operator had used a propriety protocol for network management. 5GC changes this as it is opting an IP protocol stack for the task. The protocols adopted for the 5GC are:

- Transport Layer Security (TLS) provides encryption between network functions inside a public land mobile network (PLMN)
- TCP is replacing SCTP in the transport layer
- HTTP/2 over N32

Such protocols, which are already widely used, will benefit the attacker. These protocols will lead to higher impact of vulnerabilities located within itself, prolonging the exploits. Further on, the attackers will be at more ease since they faced tough time cracking the proprietary standards.

2.1.8.5 Technologies Utilized by 5G

Virtualization

5G will operate differently than traditional network architecture. For this, it will use a cloud network rather than the operators. As the new technology brings in new threats, there are new solutions being considered. Virtualization controls like “Tenant and resource isolation” is on the list. The spectre and meltdown microprocessor-level vulnerabilities highlighted the need to segregate tenants based upon their security. This is to make sure that tenants fulfil the security requirements and each one of them has a high-level security.

A new virtualization is gaining popularity, containerization. It is an OS-level technology. Here, the host blocks the container’s access to physical resources for consumption. Hence, all virtualizations run network segmentation and resource isolation. The impact and availability of attacks are significantly reduced.

Cloud Services

Since cloud is a key 5G enabler, the architecture is designed in such a way to bring in elasticity and scalability. Securing the coding practices is obligatory as we can not risk the existence of any exploits of cloud or operator data and code are ensured to be leak proof.

Network Slicing

In this, we specify the network for different use cases while using the same hardware. Thus, the security model has to be adopted for slice of network and applied to that use case. For instance, for a remote surgery, the network slice will be required to do a constant mutual identification and authorization. This is to mitigate man in the middle (MiTM) attack. However, the slice for VR/AR does not need such requirements.

Mobile IoT

The IoT connections are inevitably going to increase in a 5G network. The security controls are only required to be scalable in this regard. IoT has to be securely coded, implemented and vigilantly administered in its life-cycle. It faces three common attack scenerios:

- Attack on devices I.e end points
- Attack on service platforms I.e Clouds

- Attack on communication I.e Links

eSIM

An eSIM is embedded into a system which does not require a separate SIM card. The eSIM profile is downloaded via HTTPs into eUICC, identified by its unique EID, globally.

Artificial Intelligence and ML/DL

ML and DL are beneficial for automating the threat and fraud detection. Considering the enormous data generated by 5G, it is feasible and somewhat reliable to mitigate known and unknown attacks in real-time. However, we have to anticipate the attacker's leverage as he can launch an AI driven attack. This raises the complexity and severity of the risks. Unprecedented damage could be possible in such circumstances. [30]

Telecommunication industry is hosting machine to machine communications along with human to human via IoT. Following are the key considerations to keep in mind to ensure 5G security.

- Constant monitoring of 5G infrastructure is required especially of GTP protocol which will be partially active as 5G is on non-standalone mode.
- New protocols convergence onto the 5G has made it an open system, making API access more and more easy. Keeping this in view an embedded security in its design is must.
- Salient actions to enhance security and address upcoming threats are:
 - Trained operators for tackling vulnerabilities associated with IoTs
 - Real time monitoring of signaling traffic to detect illegal activities blocking it and taking security measures to prevent them
 - Regular security assessments of newly added network equipment

Signaling firewall protection against multiprotocol attacks e.g., DoS attacks, fraud and configuration errors[31].

2.1.8.6 Cryptographic countermeasures

For the impending 6G communications, these countermeasures are discussed along with their benefits and drawbacks. Most of the main traditional and non-traditional methods for achieving a dependable degree of security architecture in new mobile communication situations are included in cryptographic techniques. Both the traditional ideas of symmetry and asymmetry are present in cryptography.

Confidentiality

The countermeasures to enhance confidentiality are as follows:

- 1. Paillier Cryptosystem:** Equipped with three algorithms i.e., key generation, decryption and encryption. It uses a conventional approach of using two sizeable, independent and arbitrary prime numbers. However, it has huge processing power requirement, man-in-the-middle attack vulnerability, and quantum computing-based factorization [32].
- 2. Lightweight Cryptography:** It does a color image-based scheme cryptography, has multiple secret sharing, and a Cuckoo search optimization algorithm. However, it does not cover network exploits and has a specific application of multimedia data [33].
- 3. Random Number Generator:** Utilizes a PRNG algorithm with XOR-shift operation and 23.8 Tbps through-put. However, it is sensitive to stream cipher; does not cover network exploits and explain memory and key sharing [34].
- 4. Stream Cipher:** FPGA-based with reconfigurable logic and lower hardware utilization, but uses a complex design riddled with limited memory and prone to Cryptanalysis attacks. [35]
- 5. Distributed Encryption:** A physical layer security tool with low intercept probability and D-OMA. However, it has compatibility issues with upper-layer in network and non-OMA adaptable devices [36].
- 6. Asymmetric Encryption:** Equipped with VLC-based indoor applications; has ideal error rates alongside RSA encryption keys and data lengths. However, it requires to be in line of sight, faces integration issues and has RSA in quantum computing [37].
- 7. AES Encryption:** Offers AES encryption and AI-based QoS for cooperative network optimization. forecasts future key-length switching and harvesting power using Kalman filtering. Despite these advantages, small keys are vulnerable and there are restrictions on key distribution in heterogeneous IoT [38].
- 8. Post-Quantum KEM:** A remedy to quantum breaches, but a huge processing requirement in IoTs and hinder requirements of 6G [39].

Authentication

The countermeasures to enhance authentication are as follows:

- 1. Rivest–Shamir–Adleman (RSA) Cryptosystem:** A group-based signature public-key cryptosystem that is resistant to quantum computing and needs processing in the IoT [40].
- 2. Quantum Secure Ring Signature:** Uses Chameleon hash function with accumulator

and ZK arguments, but has minimal expandability with backward compatibility issues and has a linear growth of signature size [41].

3. Proxy-Ring Signature: Uses handover authentication and ECC algorithm, but has unsafe data and a processing price at edge server alongside a historical data transfer issue [42].

4. Key Exchange: It is a digital signature-based key exchange that uses AES encryption. However, it has a processing issue at IoT device level with authentication delay above 1 ms and is prone to MEC exploitation with quantum computing [43].

5. Lightweight Cryptography: It is used for device-to-device (D2D) communications with MEC integration, but the role of CA is not explained and faces limitations in key-generation and management [44].

2.1.8.7 Entity Attribute Countermeasures

For 6G communications, such countermeasures are discussed along with their characteristics and drawbacks. Several conventional and non-traditional entity qualities based on theoretical and technical advancements over time are included in this category. Context-aware and adaptive data traffic control techniques are thought to be the best for both network administration and security because wireless networks are symmetric.

Confidentiality

The countermeasures to enhance confidentiality are as follows:

1. Conditional Attributes: It is a bloom filter-based private set intersection and has a dependable privacy conservation. However, it has scalability problems added with large communication overhead and high computational cost as well [45].

2. Antenna Selection: It provides joint utilisation of optical and RF links with random secrecy evaluation. It runs Monte Carlo simulations i.e. the computational algorithm using random sampling, too. However, it is limited to eavesdropping attacks using MIMO technology. Moreover, it has shown limitations in regards to its compatibility with heterogeneous networks [46].

Integrity

The countermeasures to enhance integrity are as follows:

1. Context aware Security: It uses adaptive protocols to provide physical layer security for wireless edge awareness. However, it suffers from physical layer processing issues, backward

compatibility issues, and interference/jamming degradation [47].

Authentication

The countermeasures to enhance authentication are as follows:

- 1. QR Code:** It has a private sharing strategy with confidential image shadow based on polynomial and RS encoding for secret recuperation. However, it is riddled with QR security issues e.g., Q-phishing replacing QR code [48].
- 2. Quantum Key Distribution:** It runs a imitation strategy for the quantum key distribution and provides the last length key for symmetrical encryption. Nonetheless, it is only a simulation solution which is MitM-specific and has integration problems with higher layers in a network [49].
- 3. 3D Location:** Utilises a spectrum matching game and mixed integer nonlinear programming which strengthens UAV-based communications. Still, it is subjected to GPS spoofing and regulatory issues [50].

Availability

The countermeasures to enhance availability are as follows:

- 1. Physical Layer Attributes:** It comprises of numerous methods to implement authentication and privacy preservation i.e., multiantenna which have reconfigurable surfaces and beamforming. Such methods are jamming/interference-resistant for a dense 6G environment. Yet, it is complex, not scalable, and is beneficial in combating DoS attack only [51].

2.1.8.8 Intrusion Detection System (IDS)-Based Countermeasures

The intrusion detection-based countermeasures for 6G networks are discussed.

ALL FIVE SECURITY PARAMETERS (CIA3)

The countermeasures to enhance confidentiality, integrity, authentication, availability, and access-control are as follows:

- 1. Simplified Threat Matrix** Although there are compatibility problems and a consensus to maintain the threat library across heterogeneous networks, it serves as a threat library for effective detection and classification [52].
- 2. Machine Learning:** A ML-based model which mitigates and contains seven various kinds of advanced and present day attacks e.g., jamming, malware, and DoS/DDoS. Nonetheless, it is mired with the similar issues like compatibility issues in a heterogeneous networks [53].

Confidentiality

The countermeasures to enhance confidentiality are as follows:

- 1. Moving Target Defense:** It provides a proactive defense and standardization perspective, but it is limited only to wireless domain and compatible with the network's upper layer only [54].
- 2. Neural Network-based Prediction:** The attacks prediction-making will be equipped with Secrecy Outage Prediction (SOP) and transmit antenna selection to contain malicious intrusions. However, it has issues with physical layer processing and heterogenous devices' compatibility [55].

Integrity

The countermeasures to enhance integrity are as follows:

- 1. Blockchain:** The blockchain-based data accumulation to enable dispensed data-controlled applications. It is also utilized to provide security by service delegation and secure columniation environment. Yet, it still faces scalability issues and resources and constraint [56].

Availability

- 1. Routing Scheme:** Detection and identification of malicious maneuvers by using an unconventional routing scheme. It improves the LEACH protocol with minimum resource consumption. But, this is specific to flooding attacks only [57].
- 2. SDN-enabled Fog Computing:** This computing technique provides an intelligent intrusion detection and lightweight security infrastructure. It is a collaborative trust model, too. Yet, it has the SDN-based vulnerabilities and scalability issues [58].

Authentication

- 1. Sparse Signatures Matrix:** A Non-Orthogonal Multiple Access (NOMA) can act as a threat detection system providing channel state information with linear minimum square error. However, its coverage is only for wireless domain and is incompatible with non-NOMA IoTs [59].
- 2. Channel State Information (CSI):** An authentication method based on channel characteristics that employs the Hilbert Schmidt independence criterion and secret key distillation for physical layer security. Yet, it is limited to wireless domain, has backward compatibility issues and degradation in interference/jamming [60].
- 3. Digital Twin:** Utilizes public key update process alongside optimal synchronization and cryptogram authorization. Nonetheless, it requires thorough processing power and uses quantum

computing-based factorization [61].

2.1.8.9 Authentication Techniques in 6G Wireless Network Handover Authentication

It is such a technique where access to multiple access points controlled in a mobile wireless network. With an exponential expansion in mobile devices, cellular data traffic has been enlarged tremendously. Safe transfer of devices in extremely challenging environment hugely depends on authentication during handover process. Handover authentication is very important in unconventional networks e.g., terrestrial satellites.

In order to reduce handover delays, signaling overheads, and fast convergence, lightweight clustering and game-base handover decision framework are suggested [62]. In this certified ground mobility handling, configuration in 6G infused mega-satellite constellation is required. Handover in higher layer constellation, interlayer management and management are some of its limitations.

- In 6G Cybertwin, between mobile devices and edge nodes, proxy-based ring signature approach for handover authentication can be proposed [42].
- For fog-computing environment, lightweight cryptography-based handover authentication scheme is suggested [63].
- Due to mobility pattern traceable schemes, handover authentication latency is reduced by mobile edge computing. Categorization on basis of mobility patterns can be done for reauthentication delays and handover latencies [64].
- Numerous mobile entities like vehicles, drones/UAV et cetera are making 6G networking more and more heterogeneous. Drones and UAVs are untethered in 3D space, making authentication more and more challenging [65].
- Increased coverage and improved handover procedural efficiency can be achieved in fading signals by implementing multi-connectivity architecture [66].

Mutual Authentication

One of the authentication schemes which is being proposed in resource constrained IoT devices is random HMAC and ECC-based D2D interchangeable authentication plan. It is better because of efficient processing, robust against free-riding attacks, less complex, and promises message

authorship with 7.7-times lower delay [67].

In mobile node communication, security can be achieved by MAC address-based mutual authentication scheme with fingerprints. It provides strong bit-level integrity and high trust level on password security. Fingerprint hacking vulnerability is a threat.

Mutual authentication schemes use Maritime Transport System (MTS) to prevent unauthorized vessel location data access. As it gives better performance and less latencies. However, his strategy is prone to extreme force and attacks due to SHA-I [68].

Batch authentication in 6G vehicular networks uses bilinear passing approach for decreasing computational overload and message modification, but at the same time, it is vulnerable to data privacy issues [69].

Client-server key management scheme using both bilinear parsing and ECC can be prevent almost all of network the attacks and gives less overhead and computational costs. Fixed curve issues in ECC and weaknesses of SHA-I can cause brute force attacks.

Physical Layer Authentication

Physical layer authentication is achieved by critically designed secret modulation on waveform and has resilience to interference and negligible bandwidth dependence [70]. Since spread spectrum-enabled hardware is a component of spread spectrum-based secret modulation for interference-resistant authentication. Hence, it is less compatible with traditional modulation schemes.

There are certain pre-requisites for better performance of authentication schemes like channel estimation and protocol compatibility with communication link variations [71].

For better authentication mechanism in time-varying scenarios, adaptive ML-based intelligent physical layer authentication is recommended [72]. MIMO technology can control physical wireless links in 6G. All management of elevated layers in 6G-enabled network planning became secure because of physical layer authentication mechanism.

In order to cover attacks like small integer attacks, spoofing, and replay attacks, channel state information (CSI)-based lightweight symmetric cipher-based authentication is recommended [73].

Self-taught mechanisms to decrease transfer amount and transmission inaccuracy solution like physical layer security (PLS)-based on mailbox theory with dispensed learning is proposed [74].

Joint implementation of MIMO with orbital angular momentum (OAM) modes increases throughput in point-to-point transmission [75]. OAM-based physical layer authentication is suggested for the improvement of bit error rate (BER).

Deniable Authentication

In security verification of communication, pre-sharing of system parameters is necessary part of authentication process. There are Deniable Authentication (DA) protocols which make the sender capable of rejecting the authentication process to any third party. By rejecting third-party links, a source-hiding strategy with projective hash functions secures Wi-Fi authentication.

[76].

To maintain heterogeneity of communication environment in wireless network, there is a need of developing Deniable Authentication (DA) protocols. Identity-based DA protocol for mobile ad-hoc network (MANET) with formal security authorization by random oracle design is suggested [77].

Random oracle design for authentication is suggested in social media networks. It decreases cipher text length and computational cost [78].

Token-Based Authentication

The low energy consumption of token-based authentication makes it ideal for Internet of Things applications [79].

Token-based authentication in combination with lightweight security module is suggested in 6G-enabled smart city infrastructure. Here, mal-intended interference is reduced because tokens are bound with timespan limits [80].

Prediction and stealing attacks can affect token-based authentication mechanisms; hence, verification and security of token generation and distribution is required. Therefore, token are blended with time- and session-based attributes.

Certificate-Based Authentication

The foundation of a certificate-based authentication system is laid by the application of both cryptographic techniques and handshaking protocols. These days, smart infrastructures like smart houses and other global applications employ this. Lightweight cryptography-based certificate authentication is recommended as a defense against MitM, DoS, impersonation, and replay threats. Better anonymity and untraceability are offered by this type [81].

Key Agreement with Privacy

For the majority of authentication techniques, key agreement is essential. Possible problems include identity manipulation, protocol replay, deniability, signature tempering, server trust

difficulties, and key reuse, among others. Exploitation of privacy can result in irreversible harm. Privacy-protected key agreements are therefore necessary [82].

For safe communication between smart meters and the grid management server, a novel one-way hash-based key agreement mechanism that is both authenticated and unclonable is suggested[83].

Multi-Factor Authentication

Multi-factor authentication (MFA) is a multi-step account login process that requires user to enter more information than just a password e.g., along with password user has to enter code sent to their email, a secret question or scan a fingerprint. It reduces the risk of security breach and sensitive data stays protected.

For communication enabled by 6G, MFA is advised. It can thwart cryptographic assaults based on quantum computing [84]. For combination of authentication and access control, blockchain-based authentication is recommended [85].

2.1.8.10 Threat Landscape and Possible Security Solutions Related to 6G Technologies

Distributed Ledger Technology (DLT): Blockchain of DLT is the most attractive technology for today's telecommunication industry. As AI/ML is among one of the most important data analytic technologies, is also prone to several attacks. So it is of utmost importance to secure data, which is fuel for AI algorithms. DLT can provide trust by immutable records and distributed trust among stakeholders.

Some of the security issue of blockchain and smart contract systems are:

- **Majority Attack/51% Attack:** Where more than 51% nodes are captured by malicious user.
- **Double Spending Attack:** Where user spends cryptographic token multiple times due to lack of physical nodes.
- **Sybil Attacks:** Where attacker or group of attackers hijack the blockchain peer network by fake identities.
- **Privacy Leakage:** In order to achieve too much transparency some times sinister information is revealed e.g business logic information to other competitors etc.
- **Other Attacks:** Like destroy-able contracts, exception disorder, call stack vulnerability, broken authentication, security misconfiguration, call stack vulnerability, bad randomness and unbombed computational power intensive operations.

Possible Solutions: Suitable security mechanisms should be deployed in public blockchain, for example:

- Debugging of smart contracts
- Validation of smart contracts
- Identification of semantic flaws
- Proper use of security check tools
- Formal verification
- Proper access control
- Authentication mechanism to detect malicious bots & AI agent based BC nodes
- Privacy by design
- Smart use of different architecture types blockchain/DLT (e.g, public, private, consortium and hybrid) according to 6G application and service

Quantum Computing: Quantum computing which will be commercially available soon has a huge threat impact on cryptographic schemes so quantum-safe cryptography should be introduced. Quantum-safe cryptography along with physical layer security schemes may consume a secure 6G communication links. Quantum ML algorithm may also enhance security and privacy.

Many 6G applications such as:

- Ocean communication
- Satellite
- Terrestrial wireless networks
- TeraHertz communication

All these can use quantum key distribution (QKD)

Threat Landscape

Quantum computing threats on IoT devices need considerable attention, they may require light weight cryptographic solution.

In two party communication, sender being unaware as which piece of information among many has been shared with a receiver so any leakage leads to huge damage.

In quantum cloning attacks (no rewinding is possible), attacker can make exact copy without altering the original state of the information by using optimal cloning schemes. Moreover, when two different inputs of hash function give the same output, a quantum collision attack can occur in quantum setting.

Possible Solution

Investigations of scientists has been started on solutions e.g., quantum-resistant hardware and solutions like latest-, code-, hash-, and multivariate-based encryptions.

Protection of post-quantum cryptography with classical random oracle model is no longer possible, so its security verification is needed.

Distributed and Scalable AI/ML: Discussion on 6G security comprises of both AI for security and security for AI.

AI for Security:

- Autonomous system (capable of self-monitoring, self-optimisation, self-configuration, and self-healing) without human involvement.
- Federated learning.
- Deep learning
- Privacy preserving machine learning

Security for AI:

- Trustworthiness.
- Liability and ethics.
- Resilient model and resistant data.

Threat Landscape

AI/ML related attacks e.g., poisoning attacks of training phase and evasion attacks of testing phase. Here, an attacker alter data by injecting malicious sample needing to miss prediction of resource requirements and misclarification of services. Introduction of disorders to test data leads to invasion attacks.

Possible Solutions

In order to address poisoning attacks, data integrity and authentication by blockchain, moving target defence and input validation is needed.

Invasion attacks and adversarial attacks can be addressed by injection of perturbed examples similar to attacks and defensive distillation via soft labels.

Information provided by ML APIs to the algorithm should be controlled and add noise to ML predictors. This step will lead to address model inversion attacks.

Noise injection to the execution time of ML model will decrease model extraction attacks.

Physical Layer Security (PLS): PLS mechanisms are required to enhance confidentiality. There are four key technologies for physical layer security mechanisms: terahertz (THz), visible light communication (VLC), reconfigurable intelligent surface (RIS), and molecular communication (MC).

In the following paragraphs, we will discuss threat landscape and possible solutions of each.

Terahertz THz: Frequencies ranging from 1 GHz to 10 THz are required to improve spectral efficiency and to provide high speed internet access. Such frequencies make the signals highly directional making their interception more limited to illegitimate users.

Threat Landscape

Sometimes, illegitimate receiver can intercept signals in light of sight (LoS) transmission, so data transmission exposure, eavesdropping, and access-control attacks can occur

Possible Solution

Some of the counter-measures are:

- Characterisation of backscatter of channel to detect eavesdropper.
- Sharing data transmission over multiple paths to decrease probability of eavesdropping.
- Electromagnetic signature of THz frequencies for authentication at physical layer.

Visible Layer Communication (VLC): VLC is another key technology having more advantages compared to radio frequency (RF) systems. So, it can be used to complement RF systems.

Threat Landscape

Due to broadcast nature of VLC, it is more prone to eavesdropping attacks. VLC systems are more vulnerable at locations that present strong reflections.

Possible Solutions

Following are the some of the solutions:

- Linear precoding of MIMO (multiple input, multiple output) VLC system to enhance secrecy.
- Discreet input signalling schemes for peak power constraints.
- Jamming receiver joints with spread spectrum water marking techniques to enhance secrecy of VLC systems.

Reconfigurable Intelligent Surface (RIS): RIS is an option to handle all challenges of intelligent environments' security, energy, and spectral efficiency. It is a meta-surface to enhance wireless propagation performance.

Threat Landscape

Traditional PLS techniques having friendly jammers and artificial noise (AN) using more costly hardware and high energy can not guarantee desirable secrecy propagation properties of wireless channels need to be controlled by suitable methods.

Possible Solutions

RIS-assisted PLS is a promising technology for secure and low cost 6G networks.

Molecular Communication (MC): Bio-nanomachines communication using chemical signals or molecules in an aqueous environment is called molecular communication, which will be significant in healthcare.

Threat Landscape

Along with communication of highly sensitive information, there are number of security and privacy challenges.

Possible Solutions

As issues in MC need to be handled in very early stages; hence, PLS mechanism would definitely have an impact on providing security for MC. More research on chemical cryptography and diffusion-based channel can be beneficial. [31]

2.1.9 Formulation of Framework

The important steps to be taken for the development of framework of a secure 6G network are as follows:

Carry out critical analysis of all domains of upcoming 6G communication environment.

Comprehensive study of all emerging concepts of each domain.

Recommendation of suitable/potential solutions to address these security challenges, keeping in view of all best practices.

Complete understanding of potential security challenges associated with emerging concepts.

2.2 Summary

In this chapter, related literature of mobile network evolution was reviewed. Right from the beginning i.e. in the 1980s, first generation of mobile phones appeared. At that time means of

communication was analogue radio signals having range of almost 150 MHz and what were its main drawbacks. Then in 1991, second generation was introduced having signalling technology of GSM, having range from 30 kHz to 200 kHz. Users can send and receive email messages. Then, third generation mobile network came. It is different application were reviewed. Security mechanisms in 3G were also reviewed. Various security threats of 3G were identified. How 4G had replaced 3G and included ITU-defined IMT enhanced capabilities. Different applications and key technologies of 4G were reviewed. Security mechanism in 4G like LTE security model and security in WiMAX was reviewed. Increasing pressure of improved speed, bandwidth, and number of connected devices necessitated the creation of 5G. 5G with several access technologies including Wireless Local Area Network (WLAN), New Radio (NR), LTE were the need of hour. Along with advancements in technology, security and privacy remained the crucial factor to be kept in considerations. Security requirements of 5G were also discussed. Along with this security landscape of 5G with different security threats were also analysed. Two important technologies of 5G like Network Function Virtualization (NFV) and Software Defined Network (SDN) with security risks attached to them were also analysed. Business model for cyber security in 5G were also briefly discussed. Security of Physical Layer, WLAN, and security issues in 5G were discussed in detail. Then at the end, sixth generation of mobile networks and its security requirements were reviewed. How much trust security and privacy. How literature review revealed that 6G will emerge the ideas of SDN, NFV, and AI.

CHAPTER 3

METHODOLOGY

The objectives of my study were:

1. To carry out comprehensive security analysis of 3G, 4G
- 2. Analysis of latest security trends introduced in latest 5G Technologies
- 3. Analysis of Research trends for implementation of Security in 6G technology
- 4. Propose a framework based on best practices and current trends in Wireless Security technologies for 6G systems

In the light of these objectives, I have shaped my study.

The imminent arrival of 6G technology promises revolutionary advancements in wireless communication, offering unprecedented levels of speed, connectivity, and intelligence. However, these advancements also introduce new security challenges that need to be addressed promptly and effectively. This thesis aims to develop a robust framework for securing 6G networks through a comprehensive analysis of potential threats and challenges, drawing upon best practices and existing solutions.

This research will be conducted in several phases, employing a combination of qualitative and quantitative methods:

3.1 Phase I: Security Analysis of 4G and 5G networks:

4G network primarily relies on EPS-AKA (Enhanced packet system Authentication and key agreement) for user authentication while 5G introduces enhanced authentication mechanisms to identify protection. It aims to provide a more secure environment for user authentication. 4G employs strong encryption algorithms to protect data in transit. 5G builds upon 4G's encryption capabilities with stronger algorithms and protocols. However, the increased complexity of 5G networks introduces new encryption challenges. While 5G offers improved security compared to 4G, its not immune to threats. New attack vectors, such as those targeting network slicing and IoT devices, require continuous monitoring and mitigation. As technology evolves so must security practices to protect user data and network integrity.

Table 12: Comparative analysis between security aspects of 4G and 5G.[88]

Standard	4G	5G
Start Form	2010	2016
Data Rate	2 Mbps – 1Gbps	1Gbps and higher
Frequency Domain	2 – 8 GHz	3 – 300 GHz
Handover	Horizontal and Vertical	Horizontal and Vertical
Core network	All IP network	Flatter IP network, 5G network interfacing (5G-NI)
Multiple Access	CDMA	CDMA, BDMA

3.2 Phase II: Data collection along with Categorization and prioritization of threats:

Data collection:

Data of different security threats was collected by reviewing related research papers and publicly available data sets.

By reviewing literature, we have identified a number of threats. These threats can be categorized according to like confidentiality, integrity, availability and authentication. As CIA is a useful triad used to satisfy all stakeholder following threats can be classified according to:

Confidentiality threats:

- Snooping
- Collaborative
- Man-in-the-Middle (MitM)

- Chosen Plaintext
- Impersonation
- Disclosure
- Stalking
- Eavesdropping

Availability Threats

- Redirection
- Free-riding
- Physical
- Environment
- FIFO
- DDoS
- SYNC Flood

Integrity Threats

- Message append
- Alteration
- Data diddling
- Session hijack
- Tampering

Authentication Threats

- Forgery
- Brute force
- Reuse threat
- Password
- Partial collision recovery

Prioritization of threats:

Threats can be prioritized on the basis of their severity of impact and likelihood of occurrence.

3.3 Phase III: Review Best Practices and Existing Solutions:

In this research paper different practices for robust security were studied like selection of development model e.g. Non standalone (NSA) mode is the only option currently being employed. In this 5G uses a combination of existing 4G LTE architecture with 5G RAN.

In next phase of 5G standalone (SA) mode will be deployed where 5G RAN and cloud native 5G core is used. Survey showed that operators are planning to deploy SA 5G within the next 3 years. (Source GSMAi, 2019)

In subscriber device protection user data and device data confidentiality and integrity is being planned to enhance the confidentiality of initial non access stratum. In network protection ensuring data integrity is vital, SEPP acts as a security gateway between home and visited networks. In new IP protocol stack transport layer security provides encryption between network functions inside a public land mobile network (PLMN).

Technologies such as virtualization, Mobile IoT and eSIM were also reviewed. In virtualization operating system (OS) level technology the host blocks the container's access to physical resources for consumption. While in mobile IoT common attack scenarios include attacks on devices end points, attacks on services platform and attack on communication. Meanwhile an eSIM is embedded into a system which does not require a separate SIM card.

Cryptographic measures:

These countermeasures are mentioned with their attributes and limitations for the upcoming 6G communications

Confidentiality countermeasures:

- Pallier cryptosystem
- Lightweight cryptography
- Random number generator
- Steam cipher
- Distributed encryption
- Asymmetric encryption
- AES encryption
- Post quantum KEM

Authentication:

- Rivest-Shamir-Adleman (RSA) cryptosystem
- Quantum secure ring signature
- Proxy ring signature
- Key exchange
- Lightweight cryptography

Entity attribute countermeasures:

Such countermeasures with their attributes and limitations are mentioned for 6G communications.

Confidentiality countermeasures:

- Conditional attributes
- Antenna selection

Integrity countermeasure:

- Counter-aware security

Authentication countermeasures:

- QR code
- Quantum key distribution
- 3D location

Availability countermeasure:

- Physical layer attributes

Intrusion detection system (IDS) based countermeasures:

Confidentiality countermeasures:

- Moving target defense
- Neural network-based prediction

Integrity countermeasure:

- Blockchain

Availability countermeasures:

- Routing scheme
- SDN based fog computing

Authentication countermeasures:

- Sparse signatures matrix
- Channel state information (CSI)
- Digital twin

There are several types of authentication techniques which can be used to upgrade security system.

Such as:

1. Mutual authentication
2. Handover authentication
3. Deniable authentication
4. Physical layer authentication
5. Certified based authentication
6. Token based authentication
7. Multi-factor Authentication
8. Key agreement with privacy

6G technologies threat landscapes and their possible solutions were also reviewed such as Distributed Ledger Technology (DLT). In DLT most common attacks include majority, sybil, double spend attacks etc. and their possible security solutions are debugging and validation of smart contracts, identification of semantic flaws, authentication mechanism to detect malicious bots and AI agent-based BC nodes etc.

Quantum computing threat on IoT devices need considerable attention, they may require lightweight encrypted countermeasures. Data leakages, cloning attacks and quantum collision attack are among the main threats which can be countered by quantum resistant hardware and late-code-hash and multivariate based encryptions.

In Artificial intelligence poisoning and evasion attacks are seen which can be overcome by data integrity and authentication by blockchain along with moving target defense and input validation Physical layer security(PLS) consists of 4 different mechanisms which have different threat levels

and subsequently require different solutions. In Terahertz (THz) due to faulty signal interception data transmission exposure, eavesdropping and access control attacks can occur, these all can be avoided by characterization of signal and sharing data over multiple channels etc. Visible layer communication (VLC) is more prone to eavesdropping attacks which can be solved by linear precoding of multiple input and discrete input signaling schemes. Reconfigurable intelligent surface (RIS) is very costly hence RIS assisted PLS is a promising technology for secure and low cost 6G networks. In Molecular communication (MC) relaying highly sensitive information can be a challenge which can be avoided by applying PLS mechanism to ensure maximum security.

3.4 Phase IV: Formulation of Framework

The important steps to be taken for the development of framework of a secure 6G network are as follows:

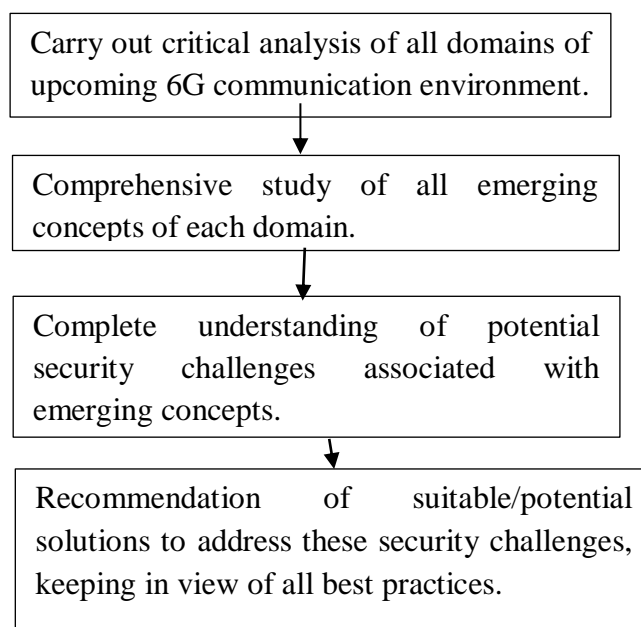


Figure 9: Important steps for Formulation of Framework for Secure 6G[3]

In order to formulate a framework of upcoming 6g network, all aspects and domains of its environment should be kept in mind. Important domains which need due considerations are enhanced mobile broadband, unconventional direct communication, safe trustworthy low latency communication, 3D and big communication. All these domains are required for the provision of wide-ranging services. Comprehensive analysis of these domains, in-depth study of emerging concepts within each domain, understanding of all possible security challenges associated with these emerging concepts and at the end, recommendations of best possible and suitable solutions for all these challenges in the light of all available best practices.

3.4.1 Domains of environment:

6G will have number of domains to provide its projected wide-ranging services. The domains are as follows:

- Enhanced Mobile Broadband (eMBB)
- Three-dimensional Communication (3Dcom)
- Unconventional Direct Communication (UCDC)
- Secure Ultra-Reliable Low Latency Communication (SURLLC)
- Big Communication (BigCom)

3.4.1.1 eMBB: Enhanced mobile broadband (eMBB) this domain of 6G communication environment comprises of following novel and emerging technological concepts:

- **IEEE 802.11 PHY:** It is a set of medium access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN). Initially, it was the Wi-Fi standard with 2.4 GHz. Now, all Wi-Fi wireless network operate on this standard.
- **Fiber Optics:** The fiber optic a set of medium access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN). Initially, it was the Wi-Fi standard with 2.4 GHz. Now, all Wi-Fi wireless network operate on this standard.
- **Broadband:** It is a high-speed internet access network. It encompasses various methods of provisions i.e., Wi-Fi, satellites, and et-cetera
- **Super IoT:** It is an IoT network embedded with cloud, big data, analytics, machine learning (ML), and deep ML can create numerous possibilities and new opportunities.
- Extra-Reality
- **Holographic technology:** It is the process of projecting a 3D image or video which can be viewed from any angle and is realistic.
- **Video LAN Client (VLC):** VLC is a portable multimedia, able to stream over networks and transcode multimedia files and save them into various formats.
- **Intelligent Network:** It allows functionality to be distributed flexibility at a variety of nodes on and off the network and allows the architecture to be modified to control the services. It provides additional information to call processing and routing requests.
- **Sensors Arrays Network:** It is a group of sensors usually deployed in a certain geometry pattern, used for collecting and processing electromagnetic or acoustic signals.

Challenges:

Enhanced mobile broadband (eMBB) is primarily comprised of smart phones with multiple

features, very dynamic real-world gaming, multimedia applications having high resolution [10]. There is tremendous variation in data rate prerequisites starting from few Mbps to 1 or more Gbps [11]. This huge data and broad bandwidth need security arrangements like up to mark intrusion data transmission network. Authentication mechanism and cryptographic requirements should be very robust especially in low processing devices such as IoTs.

So, following countermeasures are at risk and further research for suitable amendments are required:

- Intrusion Detection
- Cryptographic Processing
- Authentication
- Integrity

Possible solutions:

Keeping in view the challenges faced by Enhanced mobile broadband (eMBB), it is advised that authentic mechanism and cryptographic requirements should be robust. The intrusion faced during transmission should be avoided by deploying intrusion detection systems. There is a large amount of data transfer involved, therefore, strict integrity checks need to be put in place.

3.4.1.2 3 Dcomm:

Three-dimensional communication (3Dcomm) is a computer-generated graphic that provides the perception depth similar to real-world object. This technology is commonly used in movies, video games, graphics and virtual reality (VR) projects like the *Metaverse*. This domain of 6G communication environment comprises of following novel and emerging technological concepts:

- **Power Line Network:** It is a data network that uses a building electrical system as the transmission medium and regular wall outlet as connecting points.
- Undersea Network
- **Microwave Comm:** It is the transmission of information by electromagnetic wavelengths in the microwave frequency range (300 MHz to 300 GHz) of electromagnetic spectrum.
- **Delay Tolerant Network (DNT):** DNT is designed to operate effectively in extreme conditions and over very large distances such as space communications.
- **Dew Computing:** An information technology (IT) that combines the core concept of cloud computing with the capabilities of end devices.
- **6G Backhaul:** A network consisting of links from the core network to subnetworks having

capability of up to 20 Gbps.

- **Precision Mapping:** It is done in order to enhance localisation accuracy to below one centimetre required for mobile robots.
- Wireless Power Transfer
- 3D Networking

Challenges:

Spatiotemporal characteristic of 3D communication refers to space and time e.g., tracking of moving objects. 3Dcomm can produce security issues in authentication and cryptographic processing. Vulnerability to security can occur mostly in area of confidentiality and availability. So, following countermeasures are at risk and further research for suitable amendments are required:

- Authentication
- Confidentiality
- Availability
- Cryptographic processing

Possible solutions:

The security issues faced by 3Dcomm can be avoided by deploying strong authentication methods like biometric and context-based authentication. Asymmetric and optimized encryption methods like Elliptic Curve Cryptography (ECC) can be used to preserve confidentiality of the 3Dcomm system. Furthermore, the compromised availability can be safeguarded by maintaining a properly functioning operating system environment free of software conflicts. All these methods can ensure that the risks involved in this domain can be avoided and minimized.

3.4.1.3 UCDC:

Unconventional Data Communications (UCDC) is a flexible technological edge which envelops upcoming human-machine interface applications. This domain of 6G communication environment comprises of following novel and emerging technological concepts:

- Federated Learning
- **Quantum Machine Learning:** It is a type of reinforcement learning. Its algorithms are being effectively utilised in online web systems, auto-configuration, news recommendation, and network traffic signal control.
- Reinforcement Learning

- Deep Learning
- Augmented Reality
- Cognitive Decision
- **Brain-to-Brain Networking:** It is directly communicating via brain-to-brain interfaces (BBIs). It is the technology mediated communication between two brains without involving the peripheral nervous system.

Challenges:

Due to its openness, it is vulnerable to security issues like difficulty in attribute selection and compromised integrity and weak cryptographic processing. So, following countermeasures are at risk and further research for suitable amendments are required:

- Attributes Selection
- Cryptographic Processing
- Integrity

Possible solutions:

Future applications involving human-machine interfaces are covered by Unconventional Data Communications (UCDC), an open-ended technical edge. This technical edge faces risks to attributes selection, cryptographic processing and integrity. These risks can be mitigated by using digital signature-based authentication key exchange protocol. This protocol has been proved reliable against several attacks to the integrity of the network. [86]

3.4.1.4 SURLLC:

Secure Ultra-Reliable Low Latency Communication (SURLLC) is used in industrial automation applications. It provides reliable, low latency communication between machines and enables real-time control of processes. This allows for greater efficiency and accuracy in industrial operations. This domain of 6G communication environment comprises of following novel and emerging technological concepts:

- Extended Reality
- Automation
- **Virtual Healthcare:** It is the ability to remotely see and engage patient who is outside of the office e.g., in distant rural areas.
- Robotics
- Intelligent Gaming

- High Speed Communication
- Virtual Reality
- Sustainability
- **Molecular Communication (MC):** MC uses the presence or absence of a selected type of molecule to digitally encode messages. The molecules are delivered into communication media such as air and water for transmission. This MC uses molecules (chemical signals instead of electromagnetic waves as in information carrier).

Challenges:

SURLLC is used in fields like smart industry, smart healthcare etc., otherwise it can produce security lapse in authentication, cryptographic processing, attribute selection, and access control. Hence, innovative mechanisms that can solve these challenges in 6G communication are required in the following:

- Access Control
- Attribute Selection
- Cryptographic processing
- Authentication

Possible solutions:

Secure Ultra-Reliable Low Latency Communication (SURLLC) is a domain which faces risks to its access control, attribute selection, cryptographic processing and authentication. These challenges can be overcome by using Advanced Encryption Standard (AES)-based schemes that will preserve the authentication of the protocol. AES provides joint network optimization which can prove helpful in mitigating the risks. [86]

3.4.1.5 BigCom:

This domain of 6G communication environment comprises of following novel and emerging technological concepts:

- **Free Space Optics:** It uses propagating free space to wirelessly transmit data for telecommunication.
- Large intelligent Surfaces
- Hybrid Cell free
- 3D core Network
- Satellite Com

- Airborne Networks
- Inter-Terrestrial Coverage
- Integrated Ecosystem

Challenges:

BigCom can result in security problems especially in area of authentication and cryptographic processing. So, following countermeasures are at risk and further research for suitable amendments are required:

- Integrity
- Confidentiality
- Cryptographic processing
- Authentication

Possible solutions:

Big Communication (BigCom) comprises of free space optics, large intelligent surfaces and satellite communication, among others. The main risks it faces are to its integrity, confidentiality, cryptographic processing and authentication. These can be overcome by using strong integrity checks and encrypted protocols so that confidentiality is not compromised. The development of a QoS-ensured global level security architecture is crucial to the methodical growth of 6G communication and overcoming these risks. [86]

3.5 Summary

In this chapter, methodology of research work done is explained in three phases. Phase I is about identification of potential threats and challenges of cellular network was done and data from publicly available datasets and reports were collected and analyzed. In Phase II, different threat categorization and prioritization was done keeping in view the different aspects of security like confidentiality, availability, and integrity of data and prioritize their likelihood of occurrence was done. In Phase III, framework was developed for a secure 6G in future keeping in mind all of the best practices and solutions. Best practices like different development models e.g., NSA and combination of 4G LTE with 5G RAN were reviewed. New IP protocol stack was studied. Utilization of virtualization, cloud services, network slicing, mobile IoT, eSIM, artificial

intelligence (AI) and machine learning/deep learning (ML/DL) by 5G network was reviewed. Different cryptographic entity attribute and intrusion detection system-based countermeasures were reviewed. All types of authentication techniques in 6G wireless network were also studied.

Regarding suggested framework, four important steps in formation were discussed in detail, keeping in mind the environment of future 6G, each domain of 6G lie, enhanced mobile broadband (eMBB), three-dimensional communication (3Dcomm), Unconventional Direct Communication (UCDC), Secure Ultra-Reliable Low Latency Communication (SURLLC), and big communication (BigCom.) Emerging concepts among each domain, its challenges and possible solutions were discussed.

CHAPTER 4

CONCLUSIONS AND FUTURE RECOMMENDATION

4.1 SUMMARY

In this study, introduction of cellular networks and literature review was given initially, where evolution of cellular network starting from first generation to upcoming sixth generation of cellular network was discussed. Related research work of security mechanisms in cellular networks their threat landscape, different types of threats and all potential security challenges were reviewed. In methodology, the work was carried out in three phases. In first phase, identification of potential threats was done and data collection from various publicly available resources was carried out. In second phase, security threats were classified on basis of confidentiality, integrity, and availability (CIA). Analysis of security threats on the basis of their severity, impact, and likelihood of occurrence was also carried out. In third phase, in the light of best practices and existing solutions, a robust and adaptable security framework for 6G network was formulated which should satisfy all security requirements of CIA.

A brief summary of thesis, discussion of findings, and concluding remarks were given. Few research directions for future were also highlighted.

4.2 DISCUSSION/CONCLUSION

Tremendous influx of novel technologies to enhance global connectivity leads to more and more vulnerability for security breaches by well-organized malicious actors. Hence, a need for a secure upcoming communication system is becoming mandatory.

By reviewing the available literature, it is very much clear that every new engineering concept or emerging technology which on one side is beneficial for enhanced connectivity either by improving quality or by increasing quantity, unfortunately on other side, it is providing wider area of attack to various malicious actors.

Important considerations to be kept in mind are both technical advancement and security arrangements should go side by side, if new and more beneficial technologies are being introduced in communication system with every passing day, simultaneously advancement and more and more complication among criminal attacks and ways of hijacking the system are emerging and

posing real challenges to operators and developers of communication networks. Malicious actors are busy in innovating and implementing new ways to intercept and detect vital information. Whole communication system ranging from end-user mobile phone to mobile network is at stake. Every single domain of network is under threat. For example, as digital payment system is getting into mainstream, such actors are playing underhand and getting financial benefits. In future, all fields of life e.g., business, industry, transportation, agriculture, education, economy, health, and etc. is becoming dependent on communication network. Immense pressure from all stake-holders like billions of users, service providers, need guarantees for fully secure information transmission system. Technologies are required to mitigate these emerging potential threats and give foolproof security mechanisms for communication systems. CIA-based threat models are required to deal with such threats. Hence, all possible countermeasures should be taken to get full confidence of all stake-holders. Unfortunately, research work regarding secure upcoming 6G cellular networks is still in its initial stage. A lot of research in this direction is required.

4.3 RECOMMENDATIONS/WAY FORWARD

Potential research areas in 6G communication are as follows:

1. In order to counter 3D spatio-temporal behaviour of malicious entities, secure 6G network-dependent three dimensional computing is required.
2. 6G-enabled safe and smart design and Augmented Reality (AR) needed in the sectors of education, health, and industry.
3. SDN-based secure architecture in 6G network for massively heterogeneous network environment.
4. Routing optimisation in 6G network.
5. Molecular communication, atomic communication for secure 6G-enabled infrastructure at the physical layer.
6. Quantum computing like post-quantum cryptography, quantum-resistant network hardware, quantum fog computing, and quantum cloud computing.
7. Blockchain-based distributed security in 6G.

CHAPTER 5

FINDINGS, ANALYSIS AND DISCUSSION

5.1 Analysis of security threats

In this thesis we identified a number of security threats and how they occur. According to this study, the mechanisms of action were closely studied. The type of impact these threats had on various security domains like confidentiality, integrity, availability, authenticity, were deduced. Their likelihood of occurrence was also studied. Taking into consideration all these aspects, the threats can be categorized into different categories:

5.1.1 Categorization according to aspect of security they affect

E. g confidentiality threats

Integrity threats

Availability threats

Authentication threats

5.1.2 Categorization according to their mechanism of action

- Nefarious Activity/Abuse of Assets (NAA)
- Eavesdropping/ Interception/ Hijacking (EIH)
- Physical attacks (PA)
- Unintentional damages (accidental) (UD)

Categorization was done on the basis of likelihood of occurrence and can also to classify these attacks on basis of their likelihood of occurrence. These attacks were categorized based on which are more common and expected to occur more often.

The network developers took help from these findings in many ways. They discovered how to handle the threats and which threats need more attention than others. The categorization was done to make levels of threat more understandable.

5.2 Analysis of best practices

By reviewing likelihood, we came across so many practices which are being implemented to strengthen the security systems of mobile communication network

1. Development model:

Among multiple implementation models for 5G standards, non-standalone (NSA) mode is the only option currently being employed.

2. Subscriber and device protection:

Different methods to protect subscribers and device were reviewed e.g. public/private key pair

3. Network protection:

Ensuring data's integrity is vital for network protection. Hence, for this purpose, 5G is introducing/proposing a new architecture called "the security edge protection proxy" (SEPP).

4. New IP protocol stack:

Traditionally, each operator had used a propriety protocol for network management. 5GC changes this as it is opting an IP protocol stack for the task

5. Virtualization:

5G will operate differently than traditional network architecture. For this, it will use a cloud network rather than the operators.

6. Cloud Service:

Since cloud is a key 5G enabler, the architecture is designed in such a way to bring in elasticity and scalability.

7. Network Slicing:

In network slicing, we specify the network for different use cases while using the same hardware

8. e-Sim:

An eSIM is embedded into a system which does not require a separate SIM card. The eSIM profile is downloaded via HTTPs into eUICC, identified by its unique EID, globally.

9. Artificial intelligence & ML/DL

ML and DL are beneficial for automating the threat and fraud detection. Considering the enormous

data generated by 5G, it is feasible and somewhat reliable to mitigate known and unknown attacks in real-time.

In the study, various countermeasures based on intrusion detection systems were analyzed to enhance security. In addition, the research discusses authentication techniques specific to carrier networks, exploring their effectiveness in safeguarding communications. Furthermore, other potential security remedies related to emerging 6G technologies were also reviewed, providing an extensive overview of recent and future measures to protect network infrastructure.

Like DLT, Role of Quantum Computing, AI/ML, DLS and visible layer communication (RIS) and molecular communities were also reviewed. We have so many options of possible solutions but an important thing to keep in mind is that we have to provide both expanded communication which is a real challenge for cellular network developers.

As communication network has assumed a versatile role of just connecting two persons for conversation. Now it plays a pivotal role in various areas like Business (buying and selling), Banking, Education, Health, Agriculture.

As trust of all stakeholders in communication system is a must and to satisfy this, a robust secure highly hyper-connected widespread communication channel is needed of the hour.

By reviewing and analyzing all the security threats and available best practices we formulated a framework comprising of four steps:

1. Carry out critical analysis of all domains of upcoming 6G communication environment.
2. Comprehensive study of all emerging concepts of each domain.
3. Complete understanding of potential security challenges associated with emerging concepts.
4. Recommendation of suitable/potential solutions to address these security challenges, keeping in view of all best practices.

Keeping in mind the unique environment of upcoming 6G networks all important domains of its environment along with related emerging concepts in each domain were studied and after this best possible security mechanisms for a secure 6G were highlighted.

It is badly felt after reviewing the literature that more and more research is required for obtaining the best possible solution to meet emerging security challenges.

Bibliography

- [1] S. Kumar, G. Gupta, and K. R. Singh, "5G: Revolution of future communication technology," in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, Delhi, India: IEEE, Oct. 2015, pp. 143–147. doi: 10.1109/ICGCIoT.2015.7380446.
- [2] Nath, A. (2021) Best practices for 5G security, LinkedIn. Available at: <https://www.linkedin.com/pulse/best-practices-5g-security-amit-nath> (Accessed: 06 April 2024).
- [3] Liyanage, M., Zeadally, S. N. B., & Van Meter, R. D. (2020). A Comprehensive Guide to 5G Security. Wiley.
- [4] X. Peng, W. Yingyou, Z. Dazhe, and Z. Hong, "GTP Security in 3G Core Network," in 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China: IEEE, 2010, pp. 15–19. doi: 10.1109/NSWCTC.2010.12.
- [5] M. Ylianttila et al., "6G White paper: Research challenges for Trust, Security and Privacy." arXiv, Apr. 30, 2020. Accessed: Apr. 06, 2024. [Online].
- [6] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," IEEE Commun. Surv. Tutorials, vol. 23, no. 4, pp. 2384–2428, 2021, doi: 10.1109/COMST.2021.3108618.
- [7] Fonyi, Shane. "Overview of 5G Security and Vulnerabilities." The Cyber Defense Review, vol. 5, no. 1, 2020, pp. 117–34. JSTOR, <https://www.jstor.org/stable/26902666>. Accessed 6 Apr. 2024.
- [8] Rizvi, S.; Pipetti, R.; McIntyre, N.; Todd, J.; Williams, I. Threat model for securing internet of things (IoT) network at device-level. Internet Things 2020, 11, 100240.
- [9] Chorti, A.; Barreto, A.N.; Kopsell, S.; Zoli, M.; Chaffi, M.; Sehier, P.; Fettweis, G.; Poor, H.V. Context-aware security for 6G wireless the role of physical layer security. arXiv 2021, arXiv:2101.01536.
- [10] Lin, D.; Peng, T.; Zuo, P.; Wang, W. Deep-Reinforcement-Learning-Based Intelligent Routing Strategy for FANETs. Symmetry 2022, 14, 1787.
- [11] Abdel Hakeem, S.A.; Hussein, H.H.; Kim, H. Security Requirements and Challenges of 6G Technologies and Applications. Sensors 2022, 22, 1969.
- [12] Ahmed, S.; Hossain, M.; Kaiser, M.S.; Noor, M.B.T.; Mahmud, M.; Chakraborty, C. Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. In Data-Driven Mining, Learning and Analytics for Secured Smart Cities; Springer: Berlin/Heidelberg, Germany, 2021; pp. 23–47.
- [13] Vinodha, D.; Anita, E.M.; Geetha, D.M. A novel multi functional multi parameter concealed cluster based data aggregation scheme for wireless sensor networks (NMFMP-CDA). Wirel. Netw. 2021, 27, 1111–1128.
- [14] Shen, X.S.; Liu, D.; Huang, C.; Xue, L.; Yin, H.; Zhuang, W.; Sun, R.; Ying, B. Blockchain for Transparent Data Management Toward 6G. Engineering 2021, 8, 74–85.
- [15] W.; Christopoulou, M.; Xilouris, G.; Gür, G. Moving Target Defense as a Proactive Defense Element for Beyond 5G. IEEE Commun. Stand. Mag. 2021, 5, 72–79.
- [16] Long, Q.; Chen, Y.; Zhang, H.; Lei, X. Software defined 5G and 6G networks: A survey. Mob. Netw. Appl. 2022, 27, 1792–1812.

- [17] Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* 2021, 172, 102–118.
- [18] Partala, J. Post-quantum Cryptography in 6G. In *6G Mobile Wireless Networks*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 431–448.
- [19] Gui, G.; Liu, M.; Tang, F.; Kato, N.; Adachi, F. 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wirel. Commun.* 2020, 27, 126–132.
- [20] Catak, F.O.; Catak, E.; Kuzlu, M.; Cali, U.; Unal, D. Security Concerns on Machine Learning Solutions for 6G Networks in mmWave Beam Prediction. *arXiv* 2021, arXiv:2105.03905.
- [21] Ayaz, F.; Sheng, Z.; Tian, D.; Nekovee, M.; Saeed, N. Blockchain-empowered AI for 6G-enabled Internet of Vehicles. *Electronics* 2022, 11, 3339.
- [22] Hiller, J.; Henze, M.; Serror, M.; Wagner, E.; Richter, J.N.; Wehrle, K. Secure low latency communication for constrained industrial IoT scenarios. In *Proceedings of the 2018 IEEE 43rd Conference on Local Computer Networks (LCN)*, Chicago, IL, USA, 1–4 October 2018; pp. 614–622.
- [23] Xiong, L.; Zhong, X.; Xiong, N.N.; Liu, W. QR-3S: A High Payload QR code Secret Sharing System for Industrial Internet of Things in 6G Networks. *IEEE Trans. Ind. Inform.* 2020, 17, 7213–7222.
- [24] Chen, Y.-H.; Lai, Y.-C.; Zhou, K.-Z. Identifying Hybrid DDoS Attacks in Deterministic Machine-to-Machine Networks on a Per-Deterministic-Flow Basis. *Micromachines* 2021, 12, 1019.
- [25] Kazmi, S.H.A.; Masood, A.; Nisar, K. Design and Analysis of Multi Efficiency Motors Based High Endurance Multi Rotor with Central Thrust. In *Proceedings of the 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT)*, Virtual, 13–15 October 2021; pp. 1–4.
- [26] Sun, W.; Li, S.; Zhang, Y. Edge caching in blockchain empowered 6G. *China Commun.* 2021, 18, 1–17.
- [27] Khan, L.U.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. 6G wireless systems: A vision, architectural elements, and future directions. *IEEE Access* 2020, 8, 147029–147044.
- [28] Li, G.; Lai, C.; Lu, R.; Zheng, D. SecCDV: A Security Reference Architecture for Cybertwin-driven 6G V2X. *IEEE Trans. Veh. Technol.* 2021, 71, 4535–4550.
- [29] Elkandoz, M.T.; Alexan, W. Image encryption based on a combination of multiple chaotic maps. *Multimed. Tools Appl.* 2022, 81, 25497–25518.
- [30] Nath, A. (2021) Best practices for 5G security, LinkedIn. Available at: <https://www.linkedin.com/pulse/best-practices-5g-security-amit-nath> (Accessed: 06 April 2024).
- [31] 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.
- [32] Shen, X.S.; Liu, D.; Huang, C.; Xue, L.; Yin, H.; Zhuang, W.; Sun, R.; Ying, B. Blockchain for Transparent Data Management Toward 6G. *Engineering* 2021, 8, 74–85.
- [33] Shankar, K.; Taniar, D.; Yang, E.; Yi, O. Secure and Optimal Secret Sharing Scheme for Color Images. *Mathematics* 2021, 9, 2360.
- [34] Liao, S.; Sun, Y.; Cao, S.; Yang, L. A 23.8Tbps Random Number Generator on a Single

- GPU. In Proceedings of the 2020 International Conference on Space-Air-Ground Computing (SAGC), Beijing, China, 4–6 December 2020; pp. 33–37.
- [35] Tsavos, M.; Sklavos, N.; Alexiou, G.P. Lightweight Security Data Streaming, Based on Reconfigurable Logic, for FPGA Platform. In Proceedings of the 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 26–28 August 2020; pp. 277–280.
- [36] Al-Eryani, Y.; Hossain, E. The D-OMA method for massive multiple access in 6G: Performance, security, and challenges. *IEEE Veh. Technol. Mag.* 2019, 14, 92–99.
- [37] Lee, Y.U. Secure visible light communication technique based on asymmetric data encryption for 6G communication service. *Electronics* 2020, 9, 1847.
- [38] Mao, B.; Kawamoto, Y.; Kato, N. AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things. *IEEE Internet Things J.* 2020, 7, 7032–7042.
- [39] Ulitzsch, V.Q.; Park, S.; Marzougui, S.; Seifert, J.-P. A Post-Quantum Secure Subscription Concealed Identifier for 6G. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, San Antonio, TX, USA, 16–19 May 2022; pp. 157–168.
- [40] Partala, J. Post-quantum Cryptography in 6G. In *6G Mobile Wireless Networks*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 431–448.
- [41] Liu, J.; Yu, Y.; Li, K.; Gao, L. Post-Quantum Secure Ring Signatures for Security and Privacy in the Cybertwin-Driven 6G. *IEEE Internet Things J.* 2021, 8, 16290–16300.
- [42] Li, G.; Lai, C.; Lu, R.; Zheng, D. SecCDV: A Security Reference Architecture for Cybertwin-driven 6G V2X. *IEEE Trans. Veh. Technol.* 2021, 71, 4535–4550.
- [43] Soleymani, S.A.; Goudarzi, S.; Anisi, M.H.; Movahedi, Z.; Jindal, A.; Kama, N. PACMAN: Privacy-Preserving Authentication Scheme for Managing Cybertwin-based 6G Networking. *IEEE Trans. Ind. Inform.* 2021, 18, 4902–4911.
- [44] Suraci, C.; Pizzi, S.; Molinaro, A.; Araniti, G. MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System. *IEEE Internet Things J.* 2021, 9, 11524–11532.
- [45] Liu, Z.; Huang, F.; Weng, J.; Cao, K.; Miao, Y.; Guo, J.; Wu, Y. BTMPP: Balancing trust management and privacy preservation for emergency message dissemination in vehicular networks. *IEEE Internet Things J.* 2020, 8, 5386–5407.
- [46] Ibrahim, M.; Badrudduza, A.; Hossen, M.; Kundu, M.K.; Ansari, I.S. Enhancing security of TAS/MRC based mixed RF-UOWC system with induced underwater turbulence effect. *arXiv* 2021, arXiv:2105.09088.
- [47] Chorti, A.; Barreto, A.N.; Kopsell, S.; Zoli, M.; Chafii, M.; Sehier, P.; Fettweis, G.; Poor, H.V. Context-aware security for 6G wireless the role of physical layer security. *arXiv* 2021, arXiv:2101.01536.
- [48] Xiong, L.; Zhong, X.; Xiong, N.N.; Liu, W. QR-3S: A High Payload QR code Secret Sharing System for Industrial Internet of Things in 6G Networks. *IEEE Trans. Ind. Inform.* 2020, 17, 7213–7222.
- [49] Liu, Z.; Huang, F.; Weng, J.; Cao, K.; Miao, Y.; Guo, J.; Wu, Y. BTMPP: Balancing trust management and privacy preservation for emergency message dissemination in vehicular networks. *IEEE Internet Things J.* 2020, 8, 5386–5407.
- [50] Qin, P.; Zhu, Y.; Zhao, X.; Feng, X.; Liu, J.; Zhou, Z. Joint 3D-location planning and resource allocation for XAPS-enabled C-NOMA in 6G heterogeneous Internet of Things. *IEEE Trans. Veh. Technol.* 2021, 70, 10594–10609.

- [51] Khalid, W.; Yu, H.; Do, D.-T.; Kaleem, Z.; Noh, S. RIS-aided physical layer security with full-duplex jamming in underlay D2D networks. *IEEE Access* 2021, 9, 99667–99679.
- [52] Lanoue, M.; Bollmann, C.A.; Michael, J.B.; Roth, J.; Wijesekera, D. An Attack Vector Taxonomy for Mobile Telephony Security Vulnerabilities. *Computer* 2021, 54, 76–84.
- [53] Shrestha, R.; Omidkar, A.; Roudi, S.A.; Abbas, R.; Kim, S. Machine-learning-enabled intrusion detection system for cellular connected UAV networks. *Electronics* 2021, 10, 1549.
- [54] Soussi, W.; Christopoulou, M.; Xilouris, G.; Gür, G. Moving Target Defense as a Proactive Defense Element for Beyond 5G. *IEEE Commun. Stand. Mag.* 2021, 5, 72–79.
- [55] Xu, L.; Zhou, X.; Tao, Y.; Yu, X.; Yu, M.; Khan, F. AF Relaying Secrecy Performance Prediction for 6G Mobile Communication Networks in Industry 5.0. *IEEE Trans. Ind. Inform.* 2021, 18, 5485–5493.
- [56] Manogaran, G.; Rawal, B.S.; Saravanan, V.; Kumar, P.M.; Martínez, O.S.; Crespo, R.G.; Montenegro-Marin, C.E.; Krishnamoorthy, S. Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Comput. Commun.* 2020, 161, 248–256.
- [57] Soni, G.; Chandravanshi, K. Security Scheme to Identify Malicious Maneuver of Flooding Attack for WSN in 6G. In *Proceedings of the 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, 26–27 August 2021; pp. 124–129.
- [58] Wu, J. Security and Intelligent Management for Fog/Edge Computing Resources. In *Fog/Edge Computing for Security, Privacy, and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 213–234.
- [59] Lu, K.; Yang, H. Design of NOMA Sparse Signature Matrix for 6G Integrating Sensing and Communications Networks. In *Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, Norman, OK, USA, 27–30 September 2021; pp. 1–5.
- [60] Srinivasan, M.; Skaperas, S.; Chorti, A. On the Use of CSI for the Generation of RF Fingerprints and Secret Keys. *arXiv* 2021, arXiv:2110.15415.
- [61] Khan, L.U.; Saad, W.; Niyato, D.; Han, Z.; Hong, C.S. Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions. *arXiv* 2021, arXiv:2102.12169.
- [62] Ji, S.; Sheng, M.; Zhou, D.; Bai, W.; Cao, Q.; Li, J. Flexible and Distributed Mobility Management for Integrated Terrestrial-Satellite Networks: Challenges, Architectures, and Approaches. *IEEE Netw.* 2021, 35, 73–81.
- [63] Guo, Y.; Guo, Y. FogHA: An efficient handover authentication for mobile devices in fog computing. *Comput. Secur.* 2021, 108, 102358.
- [64] Abdullah, F.; Kimovski, D.; Prodan, R.; Munir, K. Handover authentication latency reduction using mobile edge computing and mobility patterns. *Computing* 2021, 103, 2667–2686.
- [65] Angjo, J.; Shayea, I.; Ergen, M.; Mohamad, H.; Alhammedi, A.; Daradkeh, Y.I. Handover Management of Drones in Future Mobile Networks: 6G Technologies. *IEEE Access* 2021, 9, 12803–12823.
- [66] Özkoç, M.F.; Koutsaftis, A.; Kumar, R.; Liu, P.; Panwar, S.S. The Impact of Multi-Connectivity and Handover Constraints on Millimeter Wave and Terahertz Cellular Networks. *IEEE J. Sel. Areas Commun.* 2021, 39, 1833–1853.
- [67] Chow, M.C.; Ma, M. A lightweight traceable D2D authentication and key agreement scheme in 5G cellular networks. *Comput. Electr. Eng.* 2021, 95, 107375.

- [68] Chaudhry, S.A.; Irshad, A.; Khan, M.A.; Khan, S.A.; Nosheen, S.; AlZubi, A.A.; Zikria, Y.B. A Lightweight Authentication Scheme for 6G-IoT Enabled Maritime Transport System. *IEEE Trans. Intell. Transp. Syst.* 2021, in press.
- [69] Vijayakumar, P.; Azees, M.; Kozlov, S.A.; Rodrigues, J.J. An Anonymous Batch Authentication and Key Exchange Protocols for 6G Enabled VANETs. *IEEE Trans. Intell. Transp. Syst.* 2021, 23, 1630–1638.
- [70] Hindia, M.N.; Qamar, F.; Abbas, T.; Dimiyati, K.; Abu Talip, M.S.; Amiri, I.S. Interference cancelation for high-density fifth-generation relaying network using stochastic geometrical approach. *Int. J. Distrib. Sens. Netw.* 2019, 15, 1550147719855879.
- [71] Bahache, A.N.; Chikouche, N.; Mezrag, F. Authentication Schemes for Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *SN Comput. Sci.* 2022, 3, 382.
- [72] Fang, H.; Wang, X.; Hanzo, L. Learning-aided physical layer authentication as an intelligent process. *IEEE Trans. Commun.* 2018, 67, 2260–2273.
- [73] Chen, Y.; Wen, H.; Wu, J.; Song, H.; Xu, A.; Jiang, Y.; Zhang, T.; Wang, Z. Clustering based physical-layer authentication in edge computing systems with asymmetric resources. *Sensors* 2019, 19, 1926.
- [74] Hao, Y.; Miao, Y.; Chen, M.; Gharavi, H.; Leung, V. 6G cognitive information theory: A mailbox perspective. *Big Data Cogn. Comput.* 2021, 5, 56.
- [75] Lee, D.; Sasaki, H.; Fukumoto, H.; Yagi, Y.; Shimizu, T. An evaluation of orbital angular momentum multiplexing technology. *Appl. Sci.* 2019, 9, 1729.
- [76] Zeng, S.; Mu, Y.; Zhang, H.; He, M. A practical and communication-efficient deniable authentication with source-hiding and its application on Wi-Fi privacy. *Inf. Sci.* 2020, 516, 331–345.
- [77] Gupta, D.S.; Islam, S.H.; Obaidat, M.S.; Hsiao, K.-F. A Novel Identity-based Deniable Authentication Protocol Using Bilinear Pairings for Mobile Ad Hoc Networks. *Adhoc Sens. Wirel. Netw.* 2020, 47, 227–247.
- [78] Huang, W.; Liao, Y.; Zhou, S.; Chen, H. An efficient deniable authenticated encryption scheme for privacy protection. *IEEE Access* 2019, 7, 43453–43461.
- [79] Ibrahim, M.Z.; Hassan, R. The implementation of internet of things using test bed in the UKMnet environment. *Asia-Pac. J. Inf. Technol. Multimed.* 2019, 8, 1–17.
- [80] Kamruzzaman, M. 6G-Enabled Smart City Networking Model Using Lightweight Security Module. *Res. Sq.* 2021, in press.
- [81] Nyangaresi, V.O.; Ogundoyin, S.O. Certificate Based Authentication Scheme for Smart Homes. In *Proceedings of the 2021 3rd Global Power, Energy and Communication Conference (GPECOM), Virtual*, 5–8 October 2021; pp. 202–207.
- [82] Zhang, L.; Zhang, Y.; Tang, S.; Luo, H. Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement. *IEEE Trans. Ind. Electron.* 2017, 65, 2795–2805.
- [83] Gope, P.; Sikdar, B. Privacy-aware authenticated key agreement scheme for secure smart grid communication. *IEEE Trans. Smart Grid* 2018, 10, 3953–3962.
- [84] Asim, J.; Khan, A.S.; Saqib, R.M.; Abdullah, J.; Ahmad, Z.; Honey, S.; Afzal, S.; Alqahtani, M.S.; Abbas, M. Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. *Appl. Sci.* 2022, 12, 3551.

- [85] Joshi, S.; Stalin, S.; Shukla, P.K.; Shukla, P.K.; Bhatt, R.; Bhadoria, R.S.; Tiwari, B. Unified Authentication and Access Control for Future Mobile Communication-Based Lightweight IoT Systems Using Blockchain. *Wirel. Commun. Mob. Comput.* 2021, 2021, 8621230.
- [86] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. A. Ibrahim, "Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions," *Symmetry*, vol. 15, no. 6, p. 1147, May 2023, doi: 10.3390/sym15061147.
- [87] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond recent advances and future challenges," *Security and Privacy*, vol. 6, no. 1, p. e271, Jan. 2023, doi: 10.1002/spy2.271.
- [88] E. Hajlaoui, A. Zaier, A. Khelifi, J. Ghodhbane, M. B. Hamed, and L. Sbita, "4G and 5G technologies: A Comparative Study," in *2020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Sousse, Tunisia: IEEE, Sep. 2020, pp. 1–6. doi: 10.1109/ATSIP49331.2020.9231605.