SECURITY AND THREATS ANALYSIS ON 5G WIRELESS NETWORKS

BY

TUSHER CHANDRA GHOSH
ID: 201-25-877

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science and Engineering

Supervised By

Dr. Md. Ismail Jabiullah
Professor
Department of Computer Science & Engineering
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH

MAY 2021

@Daffodil International University

APPROVAL

This Project/internship titled **"SECURITY AND THREATS ANALYSIS ON 5G WIRELESS NETWORKS"**, submitted by Tusher Chandra Ghosh, ID No:201-25-877 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of MSC in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 03.06.2021.

BOARD OF EXAMINERS

Chairman

Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Md. Ismail Jabiullah
Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Sheak Rashed Haider Noori
Associate Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Shamim H Ripon
Professor
Department of Computer Science and Engineering
East West University

@Daffodil International University

DECLARATION

I hereby declare that, this thesis has been done by me under the supervision of **Professor Dr. Md. Ismail Jabiullah**, Professor of Department of CSE of Daffodil International University. It is also declared that neither this thesis nor any part thereof has been submitted anywhere else for the award of any degree, diploma or other qualifications.

Supervised by:

Professor Dr. Md. Ismail Jabiullah
Professor
Department of CSE
Daffodil International University

Submitted by:

Tusher Chandra Ghosh
ID: 201-25-877
Department of CSE
Daffodil International University

@Daffodil International University

Acknowledgment

The scientific and technological cycle, as well as industry changes, are in full oscillation almost the world. Next-generation information and communication technologies continue to amplify and the Internet of Everything (IoE) takes shape, 5G takes the centrum turn as a critical information infrastructure that enables such improvements and drives the digital conversion of both our economy and society. Accelerator the progress of 5G and thickening its converged application in various aspects of our economy and society will have multifaceted and profound impacts on the economy, politics, society, culture, and many other areas. It will reproduce the global reshape and innovation landscape of the global economic structure. Most of the countries in the world consideration 5G as a top priority in their economic technological innovation and development and consider it to be a major strategical direction for advancing their competitiveness. Global mobile Suppliers Association (GSA), as of October 2019, 348 telecom operators in 119 countries or regions around the world had invested in 5G, of which 61 had already launched commercial 5G services according to market statistics. Everything has two sides. While 5G has benefited the people and society, it also networks security risks. The Second World Internet Conference that fostering cybersecurity is the attached responsibility of all international society. The international community should strengthen dialogue and cooperation based on trust and mutual respect with a view to building a secure, open, peaceful, and collaborative cyberspace with security in mind. 5G security is not just a problem of a few countries, every country can face this problem. We should embrace the concept of open and cooperative cybersecurity. To work to enhance our objective and mutual trust, to deepen cooperation, and to jointly improve 5G security protection to address 5G security risks.

Abstract

We are going to enter the world of the 5G network. There are many advanced features in the 5G network. The more new features come, the more security will be required, for all these new features. This paper is a survey for 5 generations of wireless network security, complete and thorough our current cellular network. This paper starts with a rethink of 5G wireless networks circumstantial as well as on the new pretension and motivations of 5G wireless security. The effective offensive and security services with the thought of new service necessity and new use cases in 5G wireless networks are then summarized. The recent improvement and the existing design for the 5G wireless security are presented based on similar security services including authentication, availability, data confidentiality, key management and privacy. Use of 5G networks such as Internet of Things (IoT), Large Multiple-Input Multiple-Output (MIMO), Peer-to-Peer Communication (P2P), Big Data and Cloud Computing. Based on the development of this protection and research, new 5G mobile wireless protection has been explained. New strategies for future mobile wireless networks also need to be developed. Summarizes future directions and goals in 5G security systems.

TABLE OF CONTENTS

@Daffodil International University

@Daffodil International University

LIST OF FIGURES

@Daffodil International University

LIST OF TABLES

@Daffodil International University

CHAPTER 1

Introduction

1.1 Introduction

The improved version of the 4th generation mobile network or the next step is the 5G mobile network. Which is called the 5th generation mobile network system. The 5th generation mobile network is not just an advanced mobile network, it is going to be a groundbreaking transformation of future generation wireless networks based on it. 5th generation mobile network, a system with many new service capabilities. As technology advances, so do insecurity, new protection is needed to survive insecurity. We should study threats and safety concerns. [1] With a 42 percent bandwidth growth rate, we will necessity 2,000 Mbps per household in 2020 and 67 67,000 Mbps per household in 2030! Even in case of bandwidth want slows to 25 percent per year after 2010, the requisite rates will be more than 300 and 3,000 Mbps, gradually, so there is a need for 5G Mobile Telecommunication. From 4G networks to 5G networks, the main goal of researchers is to have new devices for device-to-device communication (D2D) [7], as well as huge multiple inputs, as well as new services for multiple networks inputs, output (MMIMO) and much more. To put it better, the foundation of the future wireless network is the 5G network. Because 5G is not just advanced technology, it has many features like data rate up to 20 Gbps, 1-millisecond delay, 1000x bandwidth per unit field, 10-100x number of attached devices, 99.999% availability, 100% cover, 90% network power usage. Reduced, and ten years battery life for under power devices.[2] Improved mobile broadband, mission-critical communication, IoT, automated vehicle communication, big data, Radio Access Network (RAN), smart city, industrial automation and much more. More future services of 5G are unknown today. 5G's modern technology, modern architecture, modern applications modern security problems and solutions are needed.

1.2 Motivation

The world is getting smarter day by day. For this reason, the safety issue needs to be raised quickly. This thesis discusses the security and threats of future 5G wireless networks. 5G network is faster than the speed of 4G network. The 5th generation wireless network technology is capable of taking steps multi-Gbps data speeds (signal speed between your phone and tower) and ultra-low latency. 5G internet speeds will be extraordinary. A lot of Multiple devices can be connected together through this wireless network. Large files and videos can be sent very easily. One of the effects of the start of 5G is the detonation of the use of Internet of Things (IoT) devices. 5G network devices typically manage with limited resources (such as limited battery life) and require exalted-performance network links to communicate with cloud-based servers. Previously, the limitations of mobile networks built it impossible for these devices to use Mass practically. IoT devices can receive the

advantage of mobile network connectivity with high speed and low projection over 5G networks. 5G design means less power consumption. Additionally, the ability of 5G devices to support much higher densities causes that many IoT devices can be effectively placed in one place without negatively affecting each other's network connection. As a result, 5G makes it possible to install a wide range of IoT devices, particularly in remote areas where network connectivity is not available or valuable.

1.3 Rationale of the Study

In the case of the development of 5G, countries have different concerns as well as general concerns. It is critical that countries seek common goals while addressing each other's core interests and address common challenges so that 5G technology can better benefit the entire world. We work with all parties to uphold the concept of cooperation and mutual trust, accelerate international standards for 5G protection, establish an evaluation and certification system based on mutual trust and recognition, further strengthen industry flow and flow, and ultimately global 5G protection. Increase confidence in development. I am trying to develop a security model, this model will come in handy for future network security.

1.4 Research Questions

Q.1: What is the procedure of 5G wirless network system?

Q.2: How to work Network intrusion detection system (NIDS)?

Q.3: How to improve the impact of security-related issues using my proposed security model?

1.5 Expected Output

This is not the first time that articles have highlighted security and technology issues related to 5G wireless networks. You have undoubtedly seen countless 5G network-related ads at various online, magazine, television and network international summits. Fifth-generation wireless technology commonly named 5G. Based on existing telecommunications infrastructure to promote 5G bandwidth and capabilities and alleviate network-generated delays. However, 5G also carries and brings in new risks that must be searched to ensure safe and secure use by the public and private sectors, together with everyday citizens. Together, S&T and the Cybersecurity and Infrastructure Protection Agency (CISA) are working to do just that. In my view, 5G is the individual most critical infrastructural make the world has seen over the last 25 years and demands that we focus today on securing the future mobile wireless network with the future development of cloud computing, automation and artificial intelligence.

1.6 Report Layout

The following response consists of five chapters. Chapter 1 is the introduction, which highlights the motivation and goals behind the thesis. It has six sections. Section 1.1, 1.2, 1.3, 1.4, 1.5 and 1.6, titled introduction, motivation, the rationale of the study, research questions, expected output and report layout. Chapter 2, titled background, prerequisites information relevant to the thesis and is divided into six sections. Section 2.1, 2.2, 2.3, 2.4, 2.5 and 2.6, titled introduction, best fit review works, different types of face detection algorithm, research summary, the scope of the problem and challenges respectively.

Chapter 3 illustrates the details of this thesis experiment spanned over eight subsections. Section 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7 and 3.8 explains each phase of the recognition, i.e. introduction, research subject and instrumentation, data collection procedure, proposed system algorithm, working flow diagram of the proposed system, face recognition, convolutional neural network (CNNs) and implementation requirements.

In chapter 4 has mentioned the experimental results and discussion of that result. It has five sections. Section 4.1, 4.2, 4.3, 4.4 and 4.5 titled introduction, empirical results calculation, descriptive analysis, proposed system analysis report and summary.

Finally, chapter 5 has four sections titled summary of the study, conclusion, recommendation and scopes for future research.

Before the ending, there is a reference to reading materials that are referred to during this research.
Finally ended this thesis by described the appendix. It has five sections. Section 01, 02, 03, 04 and 0.5 titled programming segments, publications from this study, upcoming publications, contact details (monthly) report with supervisor and research materials used in this study.

CHAPTER 2

Background

2.1 Introduction

It is possible but difficult to provide data protection to users on existing networks, largely due to low bandwidth, and broadcasting issues. Attacks on the OSI model's physical seam and media access control level tend to be more prevalent on existing networks. Our current network does not provide end-to-end security in cryptography. Traffic between phones and base stations is simply encrypted, but there is no encryption when transmitting data over a wired network. Our current network security is limited to users and devices only. Future wireless networks will require new technologies, such as minimal communication delays, and high energy efficiency (EE). 5G will not only provide us with an advanced wireless network, but also our new security problems. High-end devices will not always work on the same protocol. Cloud computing, smart apps, Internet of Things (IoT) will all require separate protocols.

Computer viruses, Rogue security software, Trojan horse, Adware and spyware, DOS and DDOS attack, Phishing, MIM attacks are the most common network security threats in the current scenario. Network security attacks are usually divided into two parts. One is an active attack and the other is a passive attack. For passive attacks, hackers are always monitoring and scan systems for Weaknesses or entry points that allow them to break off information without variation any of it. Traffic Analysis, Non-evasive eavesdropping and control of transmissions, Emphasis on prohibition (encryption) not detection are the most common attributes. Traffic analysis and salvation of message contents are the main types of inactive attacks. Inactive attacks are totally destroying the privacy of users and Data Confidentiality. An effective attack endeavors to change system possessing or outcome their activities. Effective attacks involve some modification of the data stream or the creation of false statements. Masquerade, Modification of messages, Repudiation, Man in The Middle (MITM), Replay and Denial of Service are mostly common invasion symptoms in active attacks. Many methods are being used to deal with these attacks. These methods can be classified into two types, the cryptographic method and the Physical Level Protection (PLS) method. Asymmetric key cryptography and symmetrical key cryptography cryptographic methods are currently entity used at various levels of 5G wireless networks. Only one secret key is using to both encrypted and decrypt electronic information or data for Symmetric encryption. One private central is used to decrypt the data and one public is used to encrypt the data for asymmetric Key Cryptography. Cryptographic systems depend on the complexity of the algorithm. SDN and NFV discord from traditional networks. For SDN Data transmission is individual from data management, Unified software centralizes network

management, Physical network possessing are virtualized. Physical Level Protection (PLS) can play a key role in protecting 5G wireless networks. There is a lot of research running on 5G wireless networks. Physical Level Protection (PLS) will have less complexity with greater scalability so it will be suitable for 5G.

2.2 Best Fit Review Works

After reviewing around 50 papers here selected only 20 papers. From the selected papers the most related works are as follows.

Table 1: Best Fit Review Works

S.no.	Title	Year	Journal/Conference	Benefits	Drawbacks	Limitations
01	Wireless Network Security: Vulnerabilities, Threats and Countermeasures	2008	International Journal of Multimedia and Ubiquitous Engineering	Numerous opportunities to increase productivity and cut costs	It is not suitable for recognition of the new network	Only computer security risk
02	Security Threats and Challenges in Future Mobile Wireless Networks	2018	2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)	Availability, Authentication, Data Confidentiality, and Integrity	It does not provide any security model	Not working for all wireless network
03	Security Threats of Wireless Networks: A Survey	2015	International Conference on Computing, Communication and Automation (ICCCA2015)	Integrity Attacks, Integrity Attacks, Data Replay, Authentication Replay.	It does not identify the attacks	Not working for all wireless network
04	Overview of 5G Security Challenges and Solutions	2018	IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)	Improved the Internet networks	It does not identify the information	Not working for all wireless network
05	A Survey of Vehicular Ad-Hoc Network Security	2018	Convergence Security Department, Kyonggi University, Iui-dong, Yeongtong-gu, Suwon-si, Gyeonggi, South Korea	analysis on previous studies on Vehicle Security	It does not identify the information	Not working for all wireless network
06	Detection and Prevention against RTS Attacks in Wireless LANs	2017	978-1-5090-4448-1/17/$31.00 ©2017 IEEE	Increasing usage of wireless has raised its importance and hence the network performance is a very important factor that	It does not identify the information	Not working for all wireless network

				needs to be maintained and improved.		
07	Network Slicing in 5G and the Security Concerns	2020	Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020) IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2	Network slicing is one of the concepts of next-generation networks that is gaining traction in its application to 5G communication.	It does not identify the information	Not working for all wireless network

2.3 Overview of 5G Network

The 5th generation wireless system, abbreviated 5G, is a state-of-the-art wireless network that was unveiled in late 2016. [1] Initially included in 5G technology: millimeter wave bands (26, 24, 36, and 60 GHz) were Able to deliver speeds of 20 gigabits (gigabytes/second) [2]; Large range MIMO (Multiple Input Multiple Output - 64-258 antenna) which is capable of delivering at least 10 times the performance of 4G. "[3] [4] [5]" Low-band & Mid-band 5G Uses waves from 600 MHz to 6 GHz, typically 3.5-4.2 GHz.

3GPP has set the general definition of 5G through its December 15, 2016 release [15]. Many prefer the ITU's IMT-2020 definition, [9] which refers to the use of high-frequency bands for higher speeds.

The millimeter-wave system is designed to achieve a maximum download speed of 20 gigabytes/second. [10] The average speed limit is 3.5 gigabytes/second. [11] With an extra large MIMO antenna, the approximate median bandwidth of the 3.5-4.2 GHz band band is 490 megabytes per second. [11] When the same bandwidth and antenna configuration are used. [12]

2.3.1 5G general network architecture

5G has usually inherited the same network architecture old in 4G, including the access network, core network, and applications on the upper layer (as shown in the figure below). However, to meet the several business needs of 5G mobile Internet and mobile IoT, 5G has also resulted remarkably by introducing new innovative technologies to both the core network and the access network.

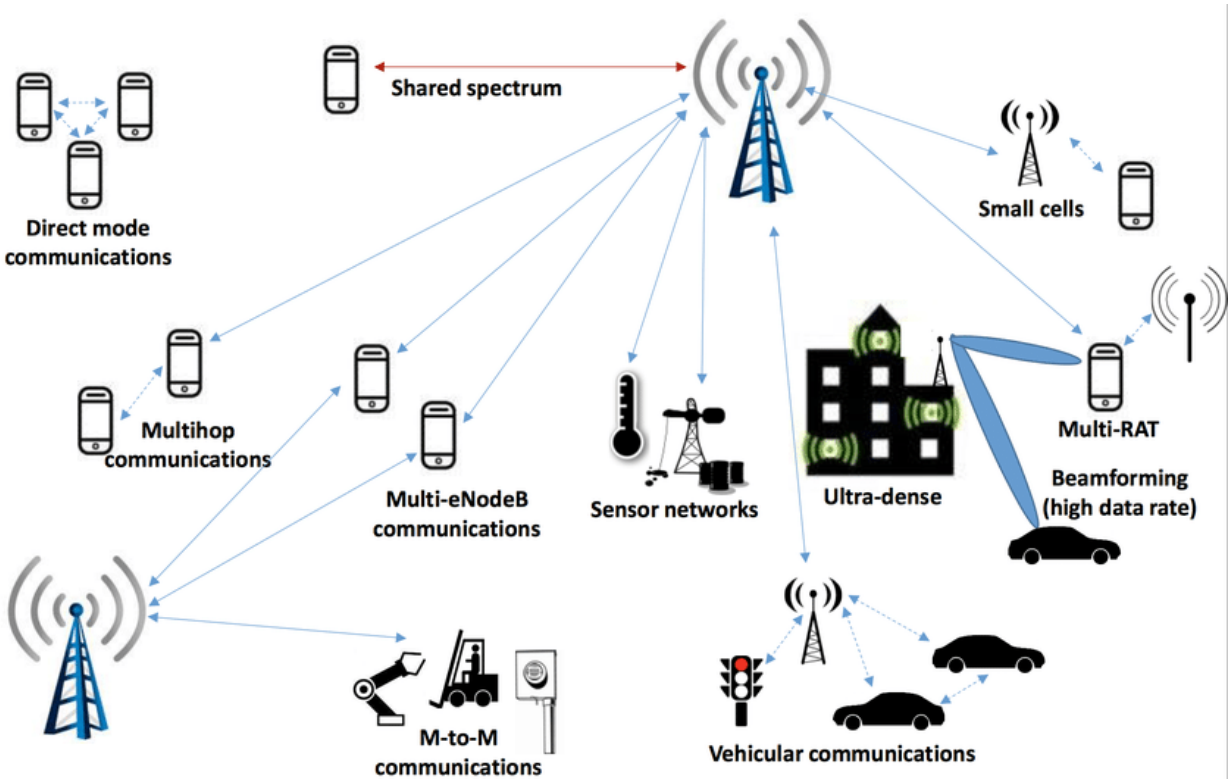

Figure 1: 5G Network Architecture

2.3.2 Service-Based Architecture (SBA).

In 5G SBA, the network functionality of a network function existence is provided as a service towards external request (from other network functions).Various network functions and services communicate with each other through standard APIs(Application Programming Interfaces) to assistance on-demand configuration and restructuring of network functions, thereby progressing the flexibility and openness of the core network. 5G SBA is an important means for quickly meeting the needs of vertical industries in the 5G era.

2.3.3 Network Function Virtualization (NFV)

5G uses virtualization technology to decode the software and hardware of dedicated network components to form a unified virtual infrastructure based on which network function is built. Its advantages include centralized control, dynamic configuration, efficient provisioning, intelligent deployment of resources, which shortens the business innovation cycle for network operations.

2.3.4 Network Slicing

Network slicing can be taken advantage of by combining different network functions and features by separating individual networks into multiple logical networks. In this way, multiple business situations can be supported simultaneously.The advantage of this is the use of improved network resources and the separation of network resources in different business situations. Edge Computing. Multi-Access Edge Computing (MEC) provides

users with computing and data processing capabilities across networks. It improves network data processing efficiency and provides the necessary protection in less virtual, higher traffic management and vertical industries.

2.3.5 Network Capability Exposure(NCE)

Capacity exposure in 5G third party applications allows third parties to design customized network services according to their own needs, supporting the expression of network capabilities through AIPI.

2.3.6 Key Technologies of the Access Network

Using flexible system design for 5G access networks allows it to support multiple services and situations. Also, the adoption of new channel coding schemes and larger MIMO technology helps it to deliver higher data-rate transfers and better coverage.

Also, the third generation partnership project (3 GPP) has clearly defined the interfaces between the access network and the main network, which have been shown to have different functions and clear boundaries. Industry Expert 2 has expressed their opinion that the functional boundary between the access network and the main network remains unchanged despite the installation of several core network functions on the 5G end. And to further improve security, a security gateway can be placed between the core network (including the edge computing part) and the access network. With all of this in mind, operators have an effective way to diversify their provider selection access and core network products to improve network resilience.

2.4 5G security framework

5G protection includes both end-to-end communication security within the network (e.g. between devices and gateways) and protection for applications running through the network. The reliability and security of mobile communication networks are specially considered from the very beginning. After decades of joint efforts by the mobile industry, the security architecture of mobile communication networks has become very stable and well-planned.

5G has adopted the same layered and domain-based security architecture that is also used in 4G. It is specified in the 3 GPP 5G Security Standard - "Security Architecture and Methods of 5G System 3" - which uses accurately the same security level as 5G 4G - Transport Level, Home Stratum / Serving Stratum and Application Stratum - detached from every layer. In the case of other security domains, the 5G security framework has added a new 'SBA' domain to the overall security domains based on 4G-network access protection, network domain protection, user domain protection, application domain protection, visibility and security configuration.

2.5 Scope of the Problem

Provides stronger protection capabilities than 4G, including 5G:

SBA domain security: In response to the security risks posed by the new 5G SBA, 5G SBA uses extensive registration, identification and authorization protection measures and protocols to ensure domain protection.

Enhanced protection of user privacy: 5G networks use encryption schemes because of transmitting user identities. This prevents attackers from using plain text transmission of the user's identity to illegally search for the user's location and location through the air interface.

Enhanced integrity protection: 5G networks provide secure encrypted protection of user aircraft data via radio interfaces to ensure the morality of user aircraft data and to prevent such data from entity spread in any way.

Enhanced inter-operator roaming security: 5G networks can provide an end-to-end safeguard for inter-operator signals of network operators and prevent man-in-the-middle attacks used to obtain sensorial inter-operator data.

Unified authentication framework. In 4G networks, separate entrance technologies are used with separate authentication methods and processes. This makes it hard to assure the continuation of the authentication method between different networks. 5G has overcome this problem by adopting a seamless authentication framework, which integrates multiple authentication methods of different access.

In short, 5G SBA provides standardized solutions and robust security protection systems to meet the growing security needs of privacy protection, authentication and approval.

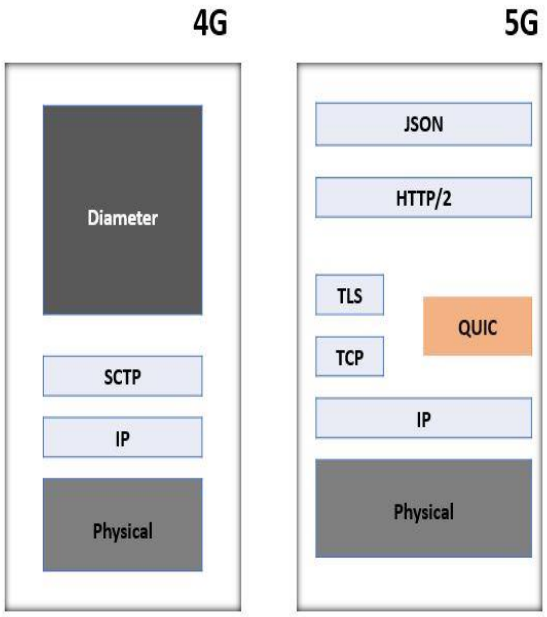

Figure 2 : Different types Network Structure

2.6 Challenges

New network architectures

Unlike its predecessors in 5G network infrastructure. It protects against the delivery of a hardware-based and centralized switching and a software-defined digital routing system. The former hub and spoke designs allow the implementation that all activities on any network can be subject to cyber hygiene practice at hardware choke points. This is not the case with 5G networks. 5G networks are based on a software-defined network where the work spreads across the entire network to digital web routers. As a result, it is impossible to use or allow checkpoints on security inspections and controls. Since this must be secured, it is vital to identify new ways to ensure that cyber hygiene practices are being observed.

Software virtualization

Virtualization of 5G network technology in high-level network functions leads to more complex cybersecurity vulnerabilities. In older networks, physical equipment was designated to perform such tasks. Most of the activities are developed and performed on the basis of Internet Protocol common language and popular operating system. As a result, it is easier for cybercriminals to attack software and manipulate activities that could cause harm. Hackers will try to compromise with virtualized software functions because they can be remotely controlled instead of physical devices, thus highlighting the need for improved and more sophisticated security solutions. Criminal actors or country-states will target virtualized software, but it is clear that standardized building systems and blockchain protocols provide tools to criminalize malicious users. So, cybersecurity solutions need to be developed to deal with them.

Expanded bandwidth

5G networks have a dramatic bandwidth spread. This increased bandwidth provides attackers with new ways to run cyber-attacks. One of the most important infrastructural requirements for the implementation of 5G network is physical, short-range, low cost and installation of small cell antennas in the area covered by 5G network. Since these are the epicenter of the attack, anyone who controls them can control some aspects of the network. Cell sites need 5G capabilities because they share their dynamic spectrum in order to be effective. These allow multiple data streams to share the same bandwidth in "slices" and each slice contributes its own degree of cyber risk. This means that cybersecurity practices must become more dynamic as 5G shows more software that allows network functions to change more rapidly. Also, cybersecurity should be dynamic depending on the uniform approach to the minimum common elements.

IoT proliferation

There are in the meantime plans to carry on implementing a comprehensive list of IoT-based petitions. These range from military operations, transportation, public security, healthcare and use in smart city centers. Devices allow individuals and organizations to lead critical processes. However, adding a few million IoT devices also reveals numerous weaknesses. All devices are hackable. It incorporates optimal controls, accesses the latest security patches, and expands the need to ensure that it is protected using powerful anti-malware / antivirus solutions.

Despite it, there are numerous instances where vendors fail to help their devices. Lack of this help fails to reduce vulnerabilities. It provides strong motivation for hackers to develop new exploits and hack into their networks. As the world continues to embrace 5G networks, new approaches need to be adopted to ensure that vendors prioritize IoT protection earlier on releasing and installing devices on networks.

CHAPTER 3

Research Methodology

3.1 Introduction

5G is a key data infrastructure and an important foundation for digital transformation. As such it not only presents a new landscape for the IOE, but all countries must face new challenges and risks. It calls on all parties to work together toward the common goal of free and cooperative security and to view and respond to 5G security risks in a comprehensive and purposeful way.

3.2 Looking at 5G security from an improvement perspective

5G marks the latest milestone in the development of information technology and this historic dedication to global IT development. It is not reasonable to delay the development of 5G on the basis of purely security risk. Instead, we must take security risks from a development perspective, manage the relationship between development and security properly, and ensure that the two move in parallel. With a more flexible security protection system than 4G, 5G is able to provide more powerful communication protection capabilities. 3 GPP will increase Defense 4 in response to emerging attacks and security threats and achieve integrated progress in both 5G security and development.

3.3 Looking at 5G protection from a system perspective

Information technologies are changing at an increasing rate. Previously decentralized and distinct networks are now becoming highly interconnected and interdependent. 5G technology is integrating and infiltrating different fields and security risks are closely linked to different entities. Faced with this kind of risk, 5G needs to be viewed and addressed in detail from a system perspective. The development of 5G technology and related application situations are wide, open, challenging and diverse. Against this background, it is necessary to clarify the different responsibilities and obligations of different organizations in different links of the industrial chain such as network operators, equipment providers and industrial application service providers. However, it must be noted that the responsibilities of a link should not be overemphasized or increased. Strengthen cooperation and coordination between different organizations, governments, standardization agencies, initiatives, research institutes and users to take initiatives, clarify the security responsibilities of all parties and also build a 5G security administration system where multiple entities participate.

3.4 Looking at 5G protection from an objective perspective

Each network technology has its own security risks and vulnerabilities and 5G networks are no exception. The best way to deal with such risks is to analyze and look at them from an objective point of view. As 5G integrates with new technologies and applications such as IoT and AI, more complex security challenges will inevitably arise. Such challenges can only be effectively overcome by conducting a comprehensive assessment of 5G security risks from an objective and unbiased technical perspective. 5G security risks can be gradually addressed through industrial innovation and technological research and development based on already existing mature processes and technological response systems. Magnifying, complicating or even politicizing security issues of a technological nature, labeling enterprises with different tags or adopting non-market methods will in no way contribute to an effective solution to the 5G security problem.

3.5 Looking at 5G protection from an objective perspective

Countries may face challenges in their status, network development stage, or real challenges, but most countries remain on the same page when it comes to security risk challenges and the need to further strengthen the administration of cybersecurity spaces. Overall, the international community is increasingly embracing the idea that we are all in the same boat and that we are all partakers of the same future. Likewise, 5G security is a global challenge that no country is free of. We are moving towards today's world ified standards typed by 5G from multiple standards of the past and the 5G process is a prime example of what can be achieved through innovation through collaboration between countries. In the field of security, countries need to work together to strengthen innovation and collectively build peaceful, secure, open and cooperative cyberspace.

CHAPTER 4

Security Analysis

4.1.1 Eavesdropping and Traffic Analysis:

In an eavesdropping invasion, the invader passively listens to network communications to profit access to personal information, such as node identification numbers, subduing updates, or application-sensitive data. The cryptography technique is the grade defense against eavesdropping attacks. A traffic analysis attack depends on what the invader hears on the network. The invader does not have to give and take the original data. Even if the data has encryption, the traffic analyst can read that data. Here the encryption algorithm plays the most significant role. Due to limited computing power, IoT, HetNet, sensor networks, cannot effectively process standard cryptographic keys. For 5G, physical layer security (PLS) can play a good role in addressing these issues.

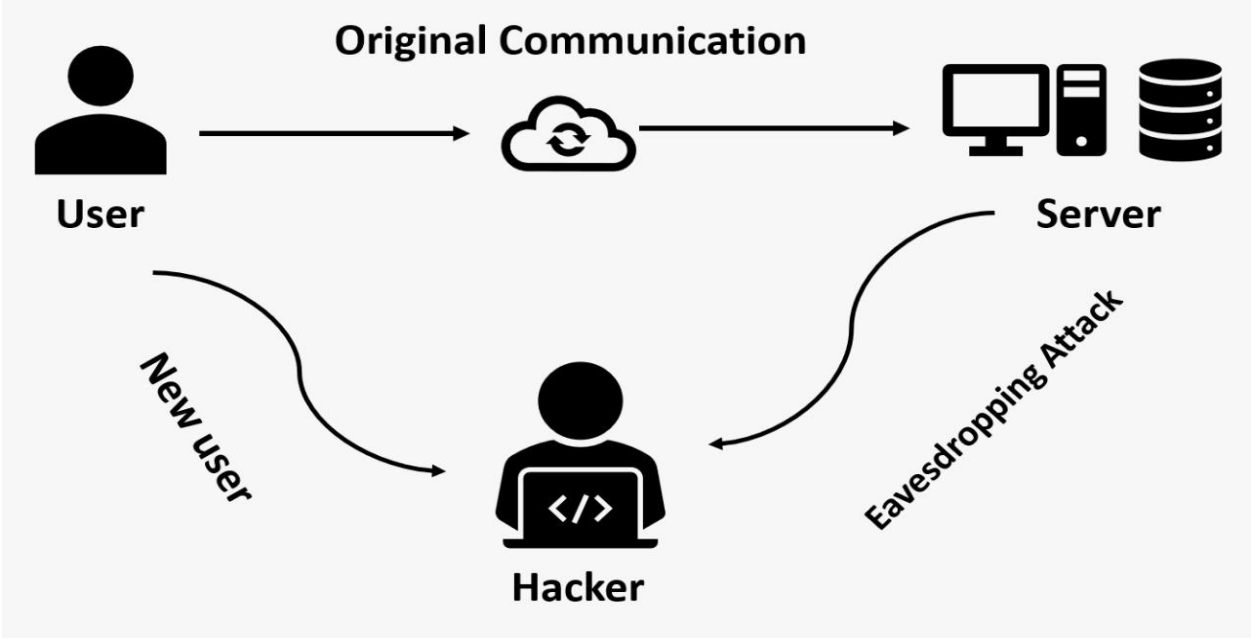

Figure 3: Eavesdroppong Attack

4.1.2 Phishing:

A phishing attack is an attempt to deceive a user into disclosing their personal information using social engineering to get their login credentials and credit card numbers. Email phishing scams, Spear phishing and Suspicious URL are mostly used. If users access or save their personal data on their computer, it is difficult for security systems to provide protection for that data and devices. The easiest solution to avoid this phishing is to be aware. When a mail arrives, check it out more than once. Be careful with messenger information, and verify

well before giving credit card information. In the figure, a Phishing website and email interrupt the communication between two authorized people.

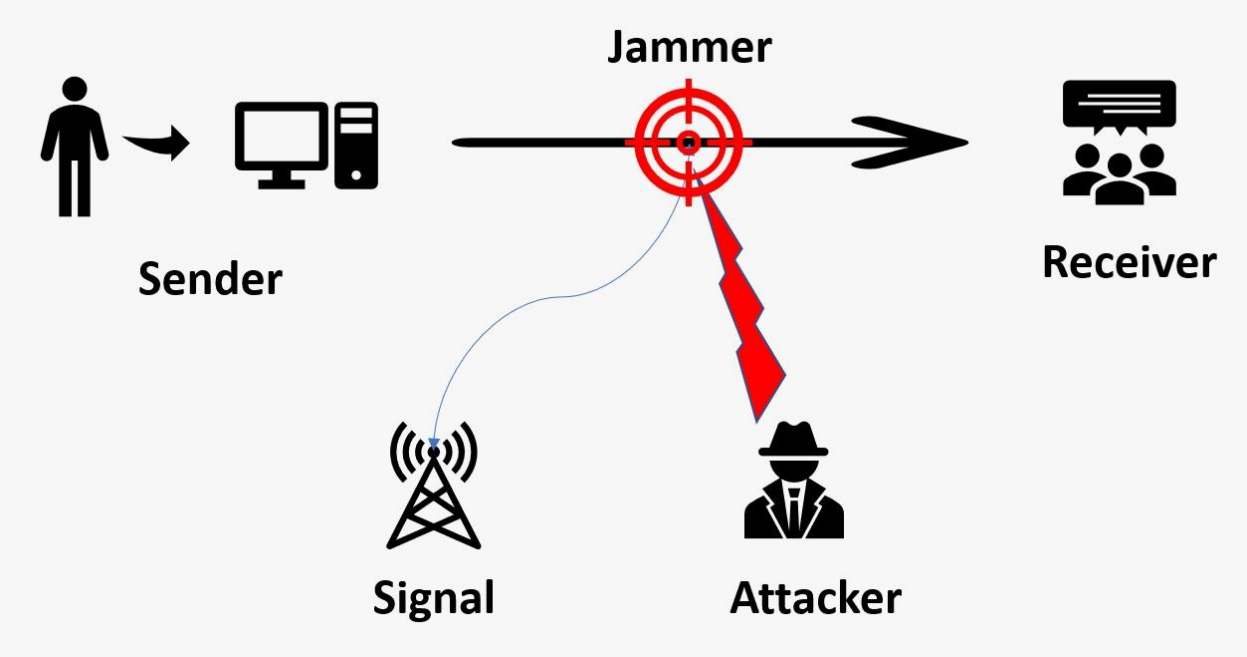

Figure 4: Jammer Attack

4.1.3 Man-in-the-Middle (MITM):

Man-in-the-Middle (MITM) is a hacking system that targets you and your web browsing. For example, you are accessing your bank account using a public WiFi. When you click on login with login details, Wi-Fi will steal your data on the way to the server. Most of the time when using public WiFi, this method is to be a victim of Mobile Banking Hack. It can also happen that when you go with a link to a specific website, it will go to the original site through DNS cache positioning

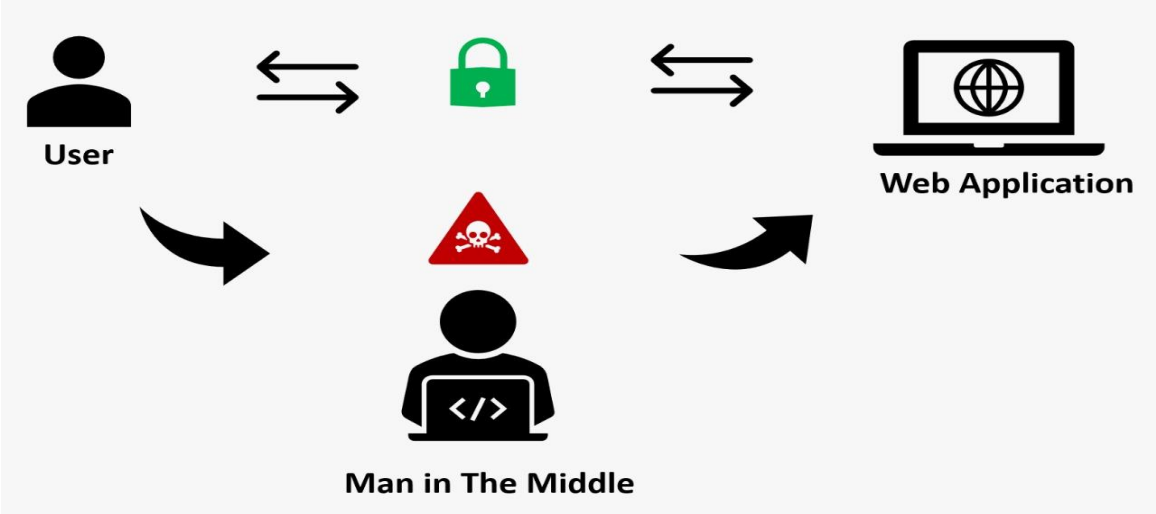

Figure 5: Man in The Middle Attack

without going to a clone or phishing website where your information will go into the hands of hackers. Fig.2 shows MITM attack models. In this attacks compromises Data Confidentiality, Integrity, and availability that's why it's called active attacks.

4.1.4 DoS and DDoS:

Denial of Service Attack (DoS) is an effort to terminate or suspend a host service connected to the Internet temporarily or indefinitely. Denial of Service Attack is the act of temporarily or indefinitely disconnecting a particular Web site or server from the Internet with the help of a device and an Internet connection. 5G wireless network DOS can be attacked due to high density. Using DOS can cause battery, memory, sensor, radio or CPU attacks.

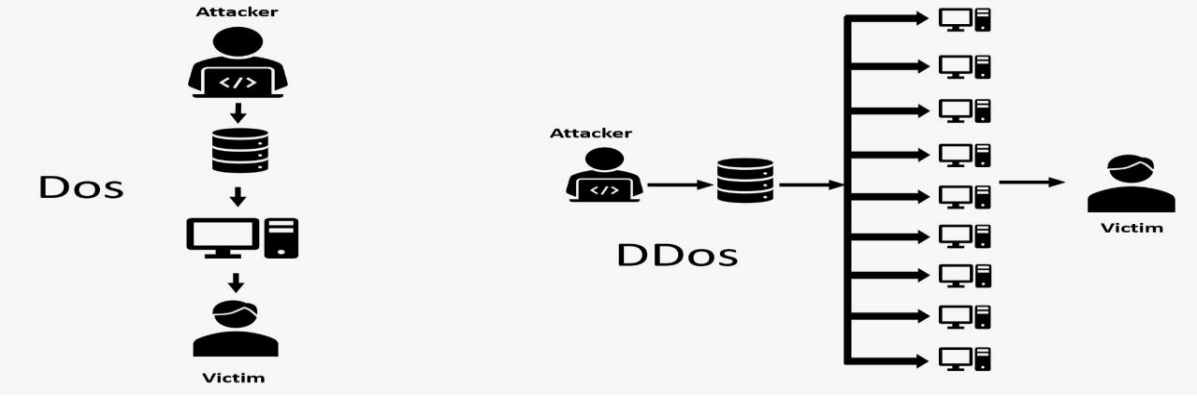

Figure 6: Dos & DDos Attack

4.2 5G Wireless Networks Security Services

As new features are available in 5G, new security is required to protect them. We discuss here six types of safety services: authentication, confidentiality/privacy, availability, error handling, and integrity and encroachment detection.

4.2.1 Authentication:

Authentication is the method of identifying a user's identity. It is the mechanism of attending to an incoming request with a set of identifying credentials. The authentication system can usually be done in two ways, identification and actual authentication. This type of authentication is important for identification and actual authentication to avoid previously mentioned attacks. In current wireless networks, it is used only between the user equipment and base stations. In addition to user equipment and base stations on 5G wireless networks, other systems also need to be covered.

4.2.2 Confidentiality/privacy:

Privacy consists of two aspects: privacy and confidentiality. Data privacy helps fight passive attacks, by protecting the data entrance to intentional users only and stopping the access from unauthorized users. Because it is very much needed in 5G, users will have personal information, security information, health applications, vehicle data, and financial information. Cryptographic methods can be used to protect the privacy of information. Data can be encrypted using private key encryption, as the sender and receiver use a private key. Secure key distribution method must be used here. Physical layer security systems can be used to combat jamming and eavesdropping attacks.

4.2.3 Availability:

Availability is defined as where a legitimate user can request this service anytime, anywhere. It is necessary to evaluate how strong the system is whereas facing different attacks on 5G. The availability attack is a common effective attack. Due to the 5G wireless network, the user will be able to use his data anytime anywhere. DoS attack is one of the major attacks on availability. Which may prevent legitimate users from accessing the Service. Using jamming can disrupt legitimate user communication links. With the growing use of IoT nodes, it will be very hard to fight in opposition to jamming and DOS-type attacks. Ensuring the availability of 5G wireless network service will be a big challenge.

4.2.4 Error handling:

Engineering and security challenges are the main part for error handling. TCP usually works to establish a reliable connection between the network and the machine. When a TCP connection is disconnected, requests and responses are not received between the nodes participating. Need to develop a framework to handle the error. Error types need to be defined, logged and monitored.

4.2.5 Integrity:

We use one-time passwords for any verification. No protection was provided whether the message was duplicated or altered. The goal of 5G is to provide connectivity anytime, someplace and in any way and to protect applications that are nearly related to people's daily lives. TOTP (Time Based One-Time Password): The system can be used to understand the transparency of data in 5G.

4.2.6 Intrusion detection:

In today's world the security of network wireless systems is a matter of great concern. This view is equally important if some attackers succeed in bypassing defenses such as authentication, Access control etc., which should be taken into considerat

CHAPTER 5

Experimental Results and Discussion

5.1 Introduction

We will now talk about existing security research activities and technology perspectives on 5G. Then we will talk about the existing security system. We will take a brief look at the cases in the new security systems and new technologies on 5G wireless networks.

5.2 Experimental Results

5.2.1 HetNet:

A heterogeneous network (HET NET) provides a service through a wireless LAN. The service is able to be maintained while switching to the cellular network. A heterogeneous wireless network (HWN) is a particular part of a HetNet. An HWN has lots of features for example increased reliability, improved spectrum efficiency, Energy Efficiency (EE), and increased coverage. HetNet has an elevated density of short cells. Performance problems can occur due to very frequent changes between various cells. Average received signal power (ARSP) policy is proposed to deal with attacks on the HetNet.

5.2.2 D2D:

Direct device-to-device (D2D) contact refers to direct contact between devices without data traffic to any infrastructure node. The D2D system is widely expected to be the key to the future of 5G wireless networks. D2D is a highly improved user data rate and per area capacity increased, extended coverage, reduced latency, increased spectral efficiency and enhanced value and power efficiency. This leads to a tendency to have jamming attacks. Considering the support of the network D2D users and eNodeB are proposed.

5.2.3 Massive MIMO:

Using a large number of antennas we can acquire high power skills and spectrum skills for the network. This can rise the security of the network, but these huge antennas interfere with each other, resulting in inconsistent performance. Eavesdropping attacks can become major intimidation to the Mimo system. Physical layer systems can play an important role in 5G from these attacks.

5.2.4 IoT:

Due to the narrow computing capacity of IoT nodes, security services on 5G IoT devices need to be skill and lightweight. Each IoT node is decorated with a sensor to detect interference. The centralness of each IoT node is considered to measure the importance of the node through the centrality network. Decentralized intervention measurements were culled at the Fusion Center at regular intervals in a common control channel.

5.2.5 Network intrusion detection system (NIDS): A network-founded encroachment detection system (NIDS) is used to obey and analyze network traffic to defense the system from network-founded threats. A NIDS reads all internal packets and searches for any questionable patterns. When a threat is detected, depending on its speed, the system may take out steps such as notifying the administrator or preventing the source IP location from accessing the network. Different types of encroachment detection systems (IDS) are available; the two prime types are host-founded access systems (HBIS) and network-founded penetration systems (NBIS). Additionally, there are IDSs that find movements by looking for specific signatures of well-known threats. An IDS compliment, or a part of it, in a larger safety system that includes firewalls, anti-virus software, and so on.

Table 1: Analysis Report of the Proposed System

4G with respect to what is needed.	Need to increase network resilience and availability against signal-based threats, including overload due to unforeseen circumstances.
	Precise protection design is required for use. For which data can be exchanged with extremely little delay.
	Provide public safety protection and mission-critical communication (resilience and high availability), Users can accept or deny this authorization on an app-by-app basis.
Requirements from radio access	System development against smart jamming attacks
	Development of 5G network BTS node system security system.

5.3 Summary

5.3.1 5G Wireless Network Architecture:

The basic goal of 5G is to provide fast, dependable mobile data services to network users. The opportunity to payoff a wide range of wireless services has been further expanded on 5G networks. Creating data access points in 5G creates integrated, flexible, and virtual RAN relationships with new interfaces. The Third Generation Partnership Project (3GPP) covers telecommunications technologies, together with RAN, core transport networks and service capabilities. 3GPP provides complete method specifications for 5G network architectures that provide much more service-oriented services than previous generations by a common framework for services that are authorized to use these methods are modularity, reusability and self-connection of network functions.

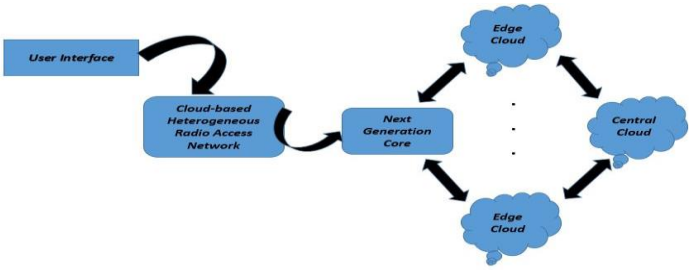

Figure 7: 5G wireless Architecture

5.4 Proposed for 5G Wireless Security Architecture:

3GPP SA3 5G R15 protection standards exist, work is underway to develop 5G R16 safety standards. Security standards need to be developed at the same pace as the 3GPP architecture and the wireless standard in order for 5G standards to continue to advance at all technical levels. The 5GR15 standards define protection architecture and protection standards for EMBB fields, covering standalone (SA) and non-standalone (NSA) architectures. Based on the 5G R15 protection architecture, 5G R16 and R17 standard MMTC and protection systems are being developed for URLLC situations. The 5G architecture is categorized and categorized by domain in design. Virtual Evolved Packet Core 5G architecture has the following security domains:

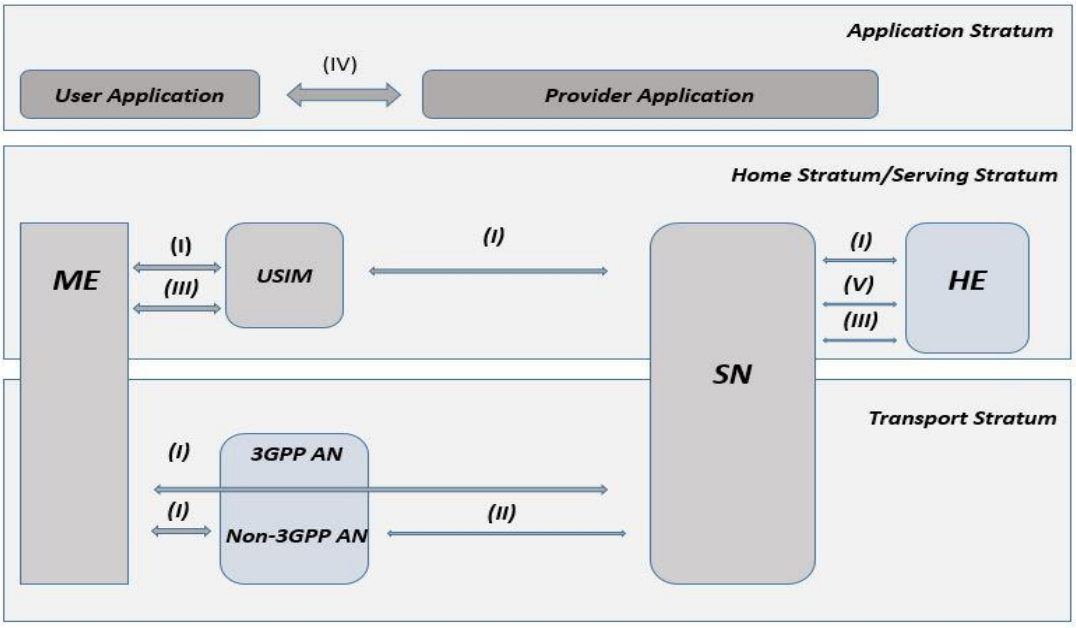

Figure 8: 5G Wireless Security Architecture

(I) (NAC) Network access security, (II) (NDS) Network domain security, (III) User domain security Application, (IV) Domain security, and (V) SBA domain security.

(NAC) Network access security:

Network Access Control is a system of network management and security that applies the security principles, compliance, and management of access control to a network. It is a network solution that enables only accessible, authenticated and trusted endpoint devices and nodes to access network resources and infrastructure. It monitors and controls their activity once they are in the network. Network Access Control is also known as Network Access Control (NAC).

(NDS) Network domain security:

Converting a hostname (e.g. www.example.com) to a computer-friendly IP address (e.g. 192.168.1.1) in the process of DNS resolution. Each device on the Internet is given an IP address, and that address is needed to find the appropriate Internet device - such as the street address used to search for a specific home. When a user wants to load a webpage, an IP address is provided instead of a DNS hostname, which allows Internet users to access specific sites.

User domain security:

A set of security materials that defend user entry to mobile devices. Mobile devices use internal security systems such as pin codes to confirm security among the Universal Customer Identity Module (USIM) and mobile devices.

Application domain security:

A set of defensive materials that enable applications to securely interchange messages between supplier domains and user domains. The security exercises of the application domain provide tenacity and application providers for the entire mobile network.

SBA domain security:

A set of security materials that qualify the SBA architecture's network Components to communicate safely with the server network domain and other network domains. These prominences cover the security views of discovery, network function registration, and approval, as well as the security of service-based interfaces. SBA Domain Protection 5G is a new security feature. An SBA forms the basis of a 5G core network. To ensure security within the UAE at SBA, security measures such as Transport Layer Security (TLS) and Open Authorization (OUT) are needed.

CHAPTER 6

Conclusion and Future Work

6.1 Summary of the Study

5G mobile network system is going to be the next generation advanced wireless network system. There is a lot of work going on with the 5G network but the work process is at an early stage. There are many new research opportunities in terms of security in 5G networks. Being a very new and emerging technology, there are several directions for the future. The tries to give an idea of what can be done to make communication between 5G more reliable and secure than before. In this research paper, we have described a few topics in detail; we need to do a lot of work to provide protection, especially in the case of intrusion detection techniques.

6.2 Conclusions & Future Work

This proposed system has made an effort to represent Security and Threats Analysis on 5G Wireless Networks.

The 5G wireless network is prospective to be able to provide high performance of newer applications. In this research paper, we have submitted a detailed presentation on research on 5G wireless networks in recent times. We discussed security measures such as authenticity, availability, information confidentiality, availability, key management and confidentiality. We need to think about new security measures because of applications like HetNet, IoT, mMIMO, D2D and intrusion detection techniques. With security in mind, we've raised a 5G wireless security architecture. Due to the improved service of 5G mobile wireless network, the industry is going to change radically. Software-Defined Networks (SDN), Mobile Cloud Computing, Network Slicing, Network Function Virtualization (NFV), Mobile Cloud Computing will bring new challenges for networks. I hope that this work of mine will contribute to the implementation of security on 5G wireless networks in the yonder future.

References

[01] “5G security recommendations package #2: network slicing”, NGMN Alliance, April, 2016.

[02] “5G SECURITY”, ERICSSON WHITE PAPER, June, 2015.

[03] “The Road to 5G: Drivers, Applications, Requirements and Technical Development”, GSA, November, 2015.

[04] J. Zhang, W. Xie, and F. Yang, “An Architecture for 5G Mobile Network based on SDN and NFV”, 6th International Conference on Wireless, Mobile and Multi-Media (ICWMMN2015), 2015, pp. 87-92.

[05] M. Dabbagn, B. Hu, M. Guizani, and A. Rayes, “Software-Defined Networking Security: Pros and Cons”, IEEE Communications, vol. 53, no. 6, pp. 73-79, 2015.

[06] L. Wei, R. Q. Hu, Y. Qian, and G. Wu, “Energy Efficiency and Spectrum Efficiency of Multihop Device-to-Device Communications Underlaying Cellular Networks”, IEEE Transactions on Vehicular Technology, vol. 65, no. 1, pp. 367-380, 2016.

[07] M. Agiwal, A. Roy and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey”, IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617-1655, 2016.

[08] J. Qiao, X. S. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, “Enabling Device-to-Device Communications in Millimeter-Wave 5G Cellular Networks”, IEEE Communications Magazine, vol. 53, no. 1, pp. 209-215, 2015.

[09] “Understanding 5G: Perspectives on future technological advancements in mobile”, GSMA Intelligence, December, 2014.

[10] M. J. Wang, Z. Yan “A Survey on Security in D2D Communications”,Mobile Networks and Applications, vol. 22, no. 2, pp. 195-208, 2017.

[11] C. Kolias et al., “OpenFlow-Enabled Mobile and Wireless Networks”, Open Networking Foundation, 2013

[12] “5G scenarios and security design”, HUAWEI, 2016.

[13] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends”, Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, 2016.
[14] “5G network architecture - a high-level perspective”, HUAWEI WHITE PAPER, July, 2016.

[15] http : //www.3gpp.org/news events/3gpp news/1786 5greqssa1

[16] K. Gai, M. Qiu, L. Tao, and Y. Zhu, “Intrusion detection techniques for mobile cloud computing in heterogeneous 5G”, Security and Communication Networks, vol. 9, no. 16, pp. 3049-3058, 2016.

[17] M. Xu, X. Tao, F. Yang, and H. Wu, “Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks”, IEEE Communications Letters, vol. 20, no. 11, pp. 2272-2275, 2016.

[18] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, “Physical Layer Security for 5G Non-orthogonal Multiple Access in Large-scale Networks”, 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1-6.

[19] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, “Secure transmission with artificial noise in millimeter wave systems”, IEEE Wireless Communications and Networking Conference, 2016, pp. 1-6.

[20] Q. Xu, P. Ren, H. Song, and Q. Du, “Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations”, IEEE Access, vol. 4, pp. 2840-2853, 2016.

[21] N. I. Bernardo, and F. De Leon, “On the trade-off between physical layer security and energy efficiency of massive MIMO with small cells”, International Conference on Advanced Technologies for Communications (ATC), 2016, pp. 135-140.

[22] Y. Luo, L. Cui, Y. Yang, and B. Gao, “Power control and channel acces for physical-layer security of D2D underlay communication”, International Conference on Wireless Communications & Signal Processing (WCSP), 2015, pp. 1-5.

[23] S. A. M. Ghanem, and M. Ara, “Secure Communications with D2D cooperation”, Communications, Signal Processing, and their Applications (ICCSPA), 2015 International Conference on, 2015, pp. 1204-1219.

[24] I. Abualhaol, and S. Muegge, “Securing D2D Wireless Links by Continuous Authenticity with Legitimacy Patterns”, 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5763-5771.

[25] K. Fan, Y. Gong, Z. Du, H. Li, and Y. Yang, “RFID Secure Application Revocation for IoT in 5G”, IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 175[26] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An efficient pseudonymous
authentication scheme with strong privacy preservation for vehicular communications”, IEEE Trans. Veh. Technol., vol. 59, no. 7, pp. 3589- 3603, 2010.

[27] Y. Li, B. Kaur, and B. Andersen, “Denial of service prevention for 5G”, Wireless Personal Communications, vol. 57, no. 3, pp. 365-376, 2011.

[28] N. P. Nguyen, T. Q. Duong, H. Q. Ngo, Z. H. Velkov, and L. Shu, “Secure 5G Wireless Communications: A Joint Relay Selection and Wireless Power Transfer Approach”, IEEE Access, vol. 4, pp. 3349-3359, 2016.

[29] C. Zhang, J. Ge, J. Li, F. Gong, and H. Ding, “Complexity-Aware Relay Selection for 5G Large-Scale Secure Two-Way Relay Systems”, IEEE Transactions on Vehicular Technology, vol. 66, no. 6, pp. 5461-5465, 2017. -181.

[30] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A Survey on Cyber Security for Smart Grid Communications”, IEEE Communications Surveys and Tutorials, vol. 14, no. 4, pp. 998-1010, 2012.

[31] “An analysis of the security needs of the 5G market”, SIMalliance, 2016.

[32] Y. Wang, Z. Miao, and L. Jiao, “Safeguarding the Ultra-dense Networks with the Aid of Physical Layer Security”, IEEE Access, vol. 4, pp. 9082- 9092, 2016.

[33] A. Zappone, P. H. Lin, and E. Jorswieck, “Artificial-noise-assisted energy-efficient secure transmission in 5G with imperfect CSIT and antenna correlation”, IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2016, pp. 1-5.

[34] E. A. Elrahman, H. L. Khedher, and H. Afifi, “D2D Group Communications Security”, 2015 International

Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), pp. 1-6, 2015.

[35] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-Layer Location Privacy Privacy-Preserving Access Point Selection Mechanism in NextGeneration Wireless Networks", 2015 IEEE Conference on Communications and Network Security (CNS), 2015, pp. 263-271.

[36] E. Dubrova, M. Naslund, and G. Selander, "CRC-Based Message Authentication for 5G Mobile Technology", IEEE Trustcom/BigDataSE/ISPA, 2015, pp. 1186-1191.

[37] W. Trappe, "The challenges facing physical layer security", IEEE Communications Magazine, vol. 53, no. 6, pp. 16-20, 2015.

[38] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and Robust Security-Aware D2D-assist Data Transmission Protocol for MobileHealth Systems", IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 662-675, 2017.

[39] M. H. Eiza, W. Ni, and Q. Shi, "Secure and Privacy-Aware CloudAssisted Video Reporting Service in 5G Enabled Vehicular Networks", IEEE Transactions on Vehicular Technology, vol. 65, no. 10, pp. 7868- 7881, 2016.

[40] M. Labib, S. Ha, and W. Saad, and J. H. Reed, "A Colonel Blotto Game for Anti-jamming in the Internet of Things", 2015 IEEE Global Communications Conference (GLOBECOM), 2015, pp. 1-6.

[41] W. Baker et al., "Data breach investigations report", Methodology, vol. 36, pp. 1-63, 2011.

[42] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks", IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, 2016.

[43] X. Duan, and X. Wang. Renzo, "Fast Authentication in 5G HetNet through SDN Enabled Weighted Secure-Context-Information Transfer", 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1-6.

[44] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G Wireless Communication Network Using Physical Layer Security", IEEE Communications Magazine, vol. 53, no. 4, pp.

20-27, 2015.

[45] Z. Yan, P. Zhang, and A. V. Vasilakos, “A security and trust framework for virtualized networks and software-defined networking”, Security and Communication Networks, vol. 9,

SECURITY AND THREATS ANALYSIS ON 5G WIRELESS NETWORKS

ORIGINALITY REPORT

20%	13%	7%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	cyberexperts.com Internet Source	5%
2	Shailesh Pramod Bendale, Jayashree Rajesh Prasad. "Security Threats and Challenges in Future Mobile Wireless Networks", 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2018 Publication	3%
3	Submitted to Daffodil International University Student Paper	2%
4	www-file.huawei.com Internet Source	2%

5	Dongfeng Fang, Yi Qian, Rose Qingyang Hu. "Security for 5G Mobile Wireless Networks", IEEE Access, 2018 Publication	2%
6	hdl.handle.net Internet Source	1%
7	digitalcommons.usu.edu	

@Daffodil International University

16	Internet Source	Submitted to RDI Distance Learning Student Paper
8	www.techopedia.com Internet Source	
9	www.viavisolutions.com Internet Source	
10	Submitted to DeVry University Onlline Student Paper	
11	Submitted to Gusto International College Student Paper	positive-tech.com
12	Submitted to International School of Management and Technology Student Paper	
13	Submitted to Open University of Mauritius Student Paper	
14	David Soldani. "5G and the Future of Security in ICT", 2019 29th International Telecommunication Networks and Applications Conference (ITNAC), 2019 Publication	
15	dspace.daffodilvarsity.edu.bd:8080 Internet Source	

@Daffodil International University

1%

<1%

1%

1%

<1%

<1%

<1%

<1%

<1%

<1%

<1%

@Daffodil International University

17 Internet Source

18 Submitted to University of New South Wales
Student Paper

19 Submitted to Kaplan College
Student Paper

20 Submitted to Queen Mary and Westfield College
Student Paper

21 scholarbank.nus.edu.sg
Internet Source

22 Hongzhi Guo, Jie Zhang, Jiajia Liu. "FiWi- Enhanced Vehicular Edge Computing Networks: Collaborative Task Offloading", IEEE Vehicular Technology Magazine, 2018
Publication

23 Mohamed Abomhara, Othman O. Khalifa, Omar Zakaria, A.A. Zaidan, B.B. Zaidan, Hamdan O. Alanazi. "Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview", Journal of Applied Sciences, 2010
24 Publication

Xenakis, C.. "Security in third G

@Daffodil International University

e n	puter Communications, 20040501 Publication	<1%
e r a t i o n M o b i l e N e t w o r k s " , C o m		<1% <1% <1% <1% <1% <1% <1%

@Daffodil International University

Exclude quotes Off Exclude bibliography Off

@Daffodil International University

Exclude matches Off

@Daffodil International University