7-7-2021

Performance Analysis of 5G DDoS Attack Using Machine Learning

Sabira Khanam Shorna

PERFORMANCE ANALYSIS OF 5G DDoS ATTACK USING MACHINE LEARNING

by

Sabira Khanam Shorna

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of Master of Science

Major: Computer Science

The University of Memphis
August 2021

Abstract

Today, due to the increase in usages of huge communication devices and connections, network services are improving expeditiously. From 1G to 4G, the network aid unable to cover all the expectations required for a vast network. A scaling up new technology, 5G, provides more capabilities of connecting billions of devices simultaneously. In this study, to analyze the network performance of 5G, a couple of network parameters (frequency, distance) have been adjusted. Besides, Distributed Denial of Service attacks were tested on the proposed 5G network. The individual simulation outcomes were compared and generated multiple results of application throughput. From the results, increasing the DoS attacks reduces the application throughput drastically. Later the simulated data used to create a DDoS dataset for the classification purpose. Support Vector Machine (SVM), K-Nearest Neighbor(KNN), and Naive Bayes (NB) were employed for the classification where KNN performs impressively well over SVM and NB with high accuracy.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

IoT	Internet of Things
3GPP	3rd Generation Partnership Project
NR	New Radio
DDoS	Distributed Denial of Service
NIST	National Institute of Technology
NSA	Non-Standalone
SA	Standalone
LTE	Long Term Evolution
EPC	Evolved Packet Core
RF	Radio Frequency
RAT	Radio Access Technologies
SDN	Software Defined Networking
NFV	Network function virtualization
MIMO	Multiple Input Multiple Output
UE	User Equipment
BS	Base Station
CA	Carrier Aggregation

CHAPTER 1

Introduction

5G is the fifth-generation standard technology, dynamic in nature, comprised of fast, heterogeneous multi-tier networks, which is inevitably a great approach in today's demanding communication. This technology is committed to delivering coverage and services with a wide range of various aspects and devices, i.e., smartphones, tablets, IoT devices, smart cities, self-driving cars, etc. According to Cisco Annual Internet Report (2018-2019), the number of connected devices will be more than three times greater than the world population by 2023 [1]. Hence, the large volumes of traffic growth enhanced the demand for connections, which causes network difficulties rapidly. 5G network's main advantages are higher speeds with a more significant channel, massive network coverage, outstanding reliability, and availability for more individuals in an efficient manner.

Evolution of 5G

5G wireless cellular network has developed after 1G, 2G, 3G, and 4G. This technology is neither a replacement for another network like 4G or a complete fixed standard since it is still being developed. It is more like such types of technologies that will emerge and change over time. 5G follows the core infrastructure technical standards that are defined by the communication industry similar to earlier version 4G. Additionally, the technological methods and concepts for the network performance and service improvement other standards added to this core portion as required. Figure 1 shows the overall evolution of 5G with specific features. About 20 years ago, a wireless global standard industry called 3GPP (3rd Generation Partnership Project) defined the standard principles for 3G. The 3GPP releases a document every year to define the standard for

the next generation's network. In June 2019, a new release called Release 15 was established with a full definition of 5G NR (New Radio) standards with advanced services.

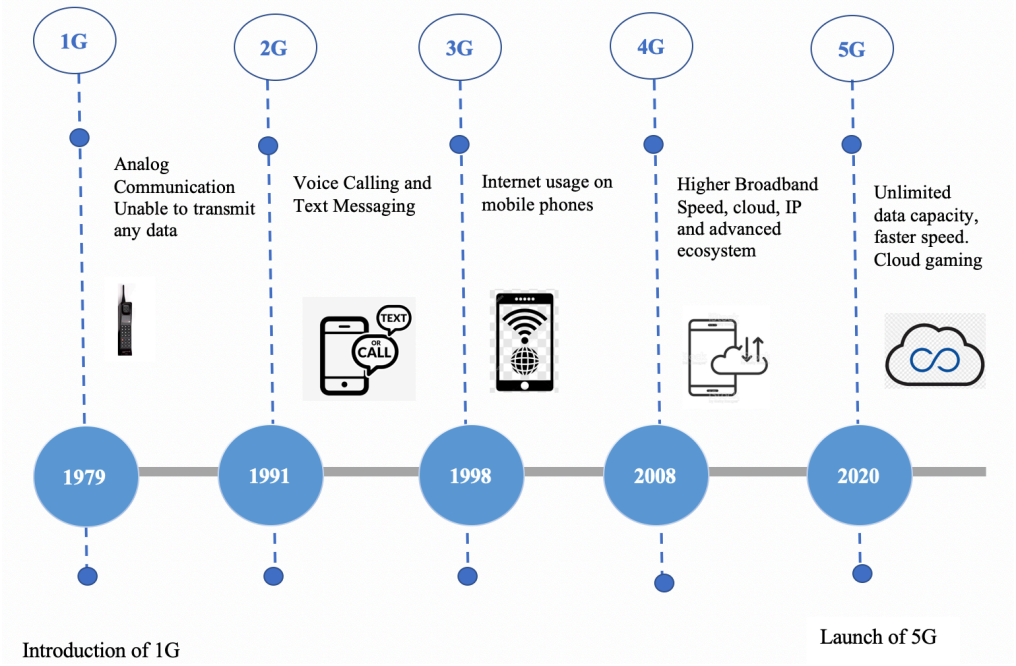


Figure 1: Journey to 5G

Source: https://www.digi.com/blog/post/what-is-5g-part-1-evolution-and-the-next-generatio

Currently, one of the major committed services of 5G is providing higher speed, reduces slow data transmission, secure communication. The key difference between the prior network generation and 5G is speed which is impressively great in contrast to 4G [2].

Major differences between the two network technologies are given in Table 1.

Table 1: Major distinguish between 4G and 5G

	4G	5G
Speed	Theoretical speed: can reach up to 100Mbps (in real-world 35 Mbps)	Theoretical speed: around 20Gbps (in real-world 50 Mbps to 3 Gbps) 100 times faster than 4G
Technology	Wimax, LTE	Developing
Latency	about 50 milliseconds	Expected to 1 milliseconds
coverage	Poor coverage	Solid performance, 100 cities in the US
Capacity	Usage spectrum from 600 MHz to 2.5 GHz	Spectrum is mmWave. Divided into three different band (lo, medium, high)
Features	Incredibly fast download speeds, paved the way for HD Streaming. HD streaming, social media, complex gaming, interactive apps like Uber	Ultra-fast internet, low-latency and improved reliability. High speeds, home internet, AI–based networking, automated sensors

Features and Benefits of 5G

The primary reason for the invention of the 5G NR is the explosive growth in the demand for wireless broadband, particularly video, and the large number of IoT devices that communicate over the internet. Therefore, the 5G network assured that it would provide data at an approximate speed greater than 10 Gbps and more comprehensive bandwidth technologies such as sub-6 GHz and mmWave (Millimeter Wave).

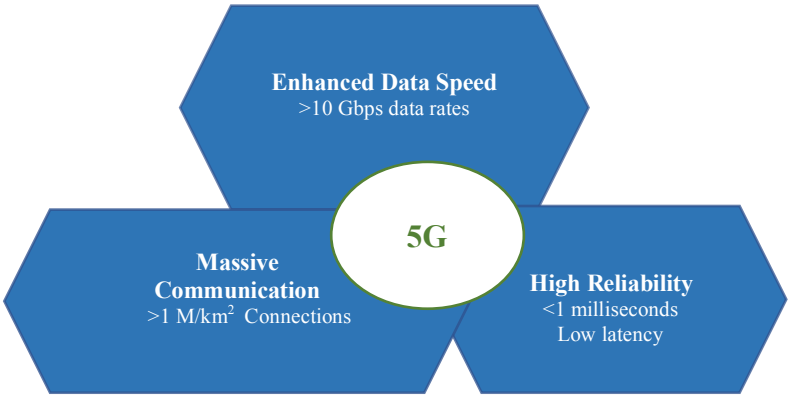


Figure 2: Core features of 5G NR

The ultra-low latency will be as low as one millisecond and extremely high device density around greater than 1million devices per square kilometer area. Among these features, low latency is crucial, which refers to the time taken for each device to react to each other over the network. The above Figure 2 shows the core objectives of 5G NR. As 5G emerged, many IoT devices can be connected by the higher bandwidth and faster throughput. Major areas of the 5G applications are given below:

- Autonomous Vehicle – this is one of the most anticipated applications of 5G which can be implemented with the combination of vehicle technology, high network speed, data throughput, and machine learning. As 5G assists with features of low latency, a vehicle will able to respond about 10-100 times faster than the current conventional network.
- 5G IoT devices in Traffic management- Intelligent transportation system and traffic management started planning to apply vehicle to vehicle and vehicle to infrastructure communications.

- 5G IoT application in Industry – In industry, synchronized robotics activities require wireless flexibility, deployment of applications that can be covered by the 5G.
- Virtual Reality (VR) and Augmented Reality (AR) – Application like video conference with more interactive gatherings, identify parts of a machine using 5G AR goggles require low latency during data transmission. 5G also allows highly responsive industrial application facilities.

Besides, now, many other applications such as drones, health areas, high definition streaming can be implemented with the 5G network. [3]

Security issues of 5G

Due to the extensive use of virtualization technologies, distributed architectures drastically increase the complexity of core network configuration, network resource management, network component optimization (i.e., channel, path) of 5G. With the arrival of new devices and connections in the 5G network, ensuring less cumbersome and providing excellent communication is highly promising in recent times [4].

A proper analysis of the cyber-attack in 5G NR is required to attain assurance in the network's security. The wireless association CTIA mentioned that the number of connected devices in the US only enlarge by 10% in 2019, more than 139 million. During this COVID-19 pandemic, it's even more notable. In communication, connected devices are frequently used to launch DDoS attacks to reduce application throughput. Hence, mobile operator's organizations need to keep an eye on their top layer of security infrastructure, traffic pattern, and capacity to thwart possible ruin from both incoming and outgoing attacks. DDoS attacks endangered to 5G core requirement's ability, including high-bandwidth, low-latency services. Many IoT devices are involved in the network, which is one of the main reasons for overwhelming network traffic.

Thus, the impact of the DDoS attacks on the overall network services of 5G NR is crucial. The conventional DDoS mitigation schemes may not significantly work well due to the different structures of the network (multiple devices with real-time communication). An organization needs to build security safeguards while launching a new communication infrastructure like 5G [5].

Indeed, the rapid growth of communication and the number of the device increases around the world remarkably. Therefore, the likelihood of cyber-attacks also tends to go high for the 5G NR and become a severe concern for the network. Generally, there are a few primary concerns for a different area of 5G NR infrastructure and architectures such as Distributed Routing, Virtualization of Network, Bandwidth Expansion, Presences of IoT, and smart devices with a lack of security. The report from NIST [6] focuses on the security aspects of 5G infrastructure and architecture particularly 5G NSA and SA security. For 5G NSA, the main objective was to configure the LTE EPC's security features in a robust way that the infrastructure will provide a remedy for possible cyber complexities in the network. The 3GPP system provides Cybersecurity features for improving the 5G NR significantly. Due to the nature of RF communications, the 5G NR network may face such complications as false base station reports, risks posed by legacy RAT's, internet-based threats for core architecture, etc. In the case of infrastructure securities, trusted hardware, visibility, and compliance by monitoring configuration changes, subscriber policy should take into account the mitigate the risk rate in the network. Currently, the followings are some 5G security issues that can pose potential threats:

- Susceptible to Denial of Services threats – As 5G NR consists of all the previous versions architectures, it inherits all the earlier vulnerabilities. The researcher found that 4G LTE is sensitive to DoS threats hence 5G NSA will be accessible to DoS too.

- Hacking- 5G core network based on the SDN and which uses protocol likes HTTP and REST API protocols extremely.

- More flexibility, more errors - Due to facilities to connect more devices in the network, it requires more robust configurations. However, the security experts figure out that critical core network configuration flaws due unable to ensure secure configuration from every angle. Administrative activities such as monitoring the large network are difficult to handle since SDN and NFV are implemented for network slicing in 5G NR.
  A group of researchers from the Korea Advanced Institute of Science and Technology11 ran a fuzzing test of a 4G network by sending specially crafted messages to check how equipment handles non-standard data. Analysis of two mobility management entities (MMEs) revealed 51 vulnerabilities caused by incorrect protocol implementation by equipment manufacturers. The same test can be done for 5G, which has the potential to contain similar issues. To find out how equipment handles non-standard data, an experiment on 4G by sending crafted messages ran by a group of researchers from the Korea Advanced Institute of Science and Technology [7].

The outcome of the test showed, 51 vulnerabilities induced by the incorrect implementation of protocols.

- Millions of connected IoT devices – Due to poor detection methods and malware analysis, the number of attacks in IoT devices increase which leads to increased threats in 5G too.

Apart from this, another problem is blockage- trees, leaves, glass, the physical body can substantially entirely damage a millimeter-wave signal. Since people are moving while communicating, it would possibly create obstructions in regular signal transmission. People will refrain from using such types of blocked services if it happens frequently. To address this problem, one of the possible solutions is a great number of base stations. Though the handover process (connection with one base station to another) among a massive number of base stations may lead to an undesirable delay. Connecting two or more base stations will provide 10 times better than massive MIMO which offer 10 times better cellular frequencies as well as a spectrum.

Motivation

Every new generation of networks is invented to reduce the security risks of communications. During the development of the 5G, a couple of known issues including diameter security considered. However, the bandwidth expansion and new virtualization technologies bring security issues in 5G NR. Despite all the advanced facilities of the 5G, it is still required to deal with challenges of standard implementation, proper configurations, and ensuring a 5G security infrastructure by establishing an efficient security and privacy management process.

Currently, many cyber-security researchers and specialists are confronted with difficulties to resolve DDoS attacks issues in 5G network since the structure of the networks is unlike others. The scholars run DDoS attack simulations applying either real-life data or tested based on earlier attack features. Due to cost and maintenances issues, it is not handy to work and observe the 5G NR network performance in real life. A good number of simulation platforms are available to operate the 5G NR and runs accordingly, including MATLAB, NetSim, OMNET++. However, each simulation software may vary due to problem context. For instance, to work on the 5G core system configuration such as numerology, frequency, signal bits, MATLAB is appropriate. On the other hand, for an end-to-end communication simulation, NetSim provides many packages, including customized options.

5G network allows a massive number of smart and intelligent devices during communication which in turn brings complexities as well as degrade network regular performance. To anticipate and observe the network behavior, 5G administrative sections (controller) need to learn the network anomalies or attack information in advance. Hence, a great diverse 5G DDoS dataset requires considering 5G core network parameters that could create a potential impact on the network performance. Therefore, at first, we need to figure out which 5G network parameters hamper the network performance. Moreover, A dataset that contains information on the 5G DDoS attacks, as well as the 5G core parameters, is necessary for monitoring the 5G network behavior. Due to the lack of a rigid 5G DDoS attack public dataset the proper analysis of 5G security and privacy is still challenging. Hence, this work's primary intention is to analyze the 5G security area by generating a dataset and classify it with the machine learning techniques that could overcome the security concerns of the network.

Objective

In the communication, services, and performance of a particular network depend on the context of the connections and several network components. Since 5G NR inherited all the previous versions, it is problematic to examine the proper reasons that hinder all the regular services fluently. Though 5G NR provides a larger bandwidth to cover the surge of connected devices, it still lacks the technique to identify and eradicate unusual behavior from the network. Even increasing frequency will not work well unless we cannot figure out how the core parameters will impact a certain situation. Hence, for better knowledge regarding 5G NR core parameters should take into account to analyze and discover the unexpected case in the network. The major objectives of this work are given below:

- The primary consideration of this work is to identify the situation and analysis the 5G network performance after modifying the 5G NR parameters.
- Determine the parameters of 5G NR that create an impact for reducing the application throughput significantly.
- Alongside, generate DDoS attacks in the proposed 5G NR using a simulation tool to observe the network application throughput's rate on multiple scenarios.
- Compare scenario and application throughput results considering both parameters adjusting and DDoS attacks to analyze the network performance.
- Collect the benign and attack traffic to create a dataset for classification using Machine Learning.

Contribution

The main idea of this work is to observe and analyze the network performance of 5G NR while modifying its parameter (distance, frequency, numerology). Moreover, DDoS attacks had introduced at the 5G network to figure out how they could also impact the network performance and effect on end devices application throughput.

This study develops by using the NetSim simulation tool to generate normal and attack traffic in 5G NR. Besides, accumulate the traffic information for both benign and attack by modifying some 5G NR network parameters (distance, frequency). The simulation results generate information regarding the parameter settings and attack types. Later, the traffic data applied to create the 5G DDoS dataset for further analysis.

Integration of Machine Learning and Artificial Intelligence in 5G multiple aspects (network configurations) can play a vital role and improve the respective problematic sector in 5G [4]. The Machine Learning schemes, Support Vector Machine (SVM), and KNN have been utilized here for the classification. This dataset can be applied for detection as well as mitigation purpose in the future. This work's key contribution is to identify the need for a 5G DDoS attack dataset due to the lack of a public dataset.

This study is organized in the following manner: reviewing the existing related works of 5G network parameter settings and DDoS attacks—detailed background and objectives of the analysis given in the next section. A work description has presented the methods and tools used for the simulation. This section also provides different types of Numerology of 5G NR and the most common DDoS attacks. Later, multiple attack scenarios, including parameter adjusting, are shown and then described for each example. In addition, it discussed the traffic simulation's results and analyzed the outcomes regarding the parameters.

CHAPTER 2

Literature Review

At present times, the user wants faster data transmission speed and secure services. 5G NR promise to deliver all the basic as well as advanced facilities in contrast to prior. This technology allows users to high-definition and volume data within a second.

5G Technology

5G can handle larger traffic to cover the massive demand of the devices. To attain this, 5G NR brings technologies like mmWave, small cells, massive MIMO, beamforming, full-duplex. However, these technologies are not yet confirmed and still developing.

Millimeter-Wave- In the previous network, 4G LTE, the same frequency bands used for a large number of users even increases the number of devices in the network. Hence, less bandwidth is available for everyone, resulting in increased delay services as well as connection dropped. Millimeter waves consist of frequency range from 30 to 300 GHz. This wavelength can vary from 1 to 10 mm in contrast to current radio waves used for the intelligent devices (lengthwise tens of centimeters). The one common flaws of mmWave are the signal cannot pass through obstacles (buildings, trees). Hence, it requires additional technology that can communicate from user equipment to the base station.

Small Cells – These are small portable base stations with minimal power. To overcome the blockage difficulties such as signal dropped, many(thousands) base stations like this can be

installed throughout the coverage area. However, in rural areas, a massive number of small cell base stations are difficult to established successfully.

Massive MIMO - To handle the mobile traffic, 4G LTE has a few ports for antenna where eight used for transmitters and the rest four for receivers. However, 5G NR base stations have approximately a hundred ports, which means a single array can hold more antennas. Thus, increases the base station's capacity of sending and receiving signals for more individuals at a time. Massive MIMO is a type of system that combines two or more transmitters and receivers to transfer data at once. It is one of the promising features of 5G. However, to handle large traffic loads installing more antennas will generate signal interferences.

Beamforming- It is a traffic signaling system for the base stations which find out the effective data delivery path for a specific user. There are multiple ways to implement this concept based on the nature of the 5G networks. During transmission, the signal can be impaired by obstacles that eventually attenuate the signal strength. In such a situation, rather than broadcasting the signal to many users, beamforming delivers a signal with an assigned beam that is dedicated to pointing to the specific user.

Full Duplex – The transceiver of 5G able to transmit and receive data at the same time with the same frequency bands, which is known as a full-duplex. For personal devices, the researcher needs to design a circuit which can provide a path for both incoming and outgoing signals, so the signal could not conflict while transmitting and receiving signal simultaneously. However, signal interference also occurred in full-duplex when transmitted and received signals both close to each other. [8]

5G numerology

A little while back, at the beginning of 2016, the 3GPP has been working on the standardization of a new RAT called 5G NR, considering all the features and services. The 5G NR frame consists of units of 10 ms (milliseconds), and each sub-frame is defined in units of 1ms. Sub-frame slots are constituted of 14 OFDM symbols, and the time interval depends on the type of sub-carrier spacing. The following Figure 3 shows the frame structure of the 5G NR

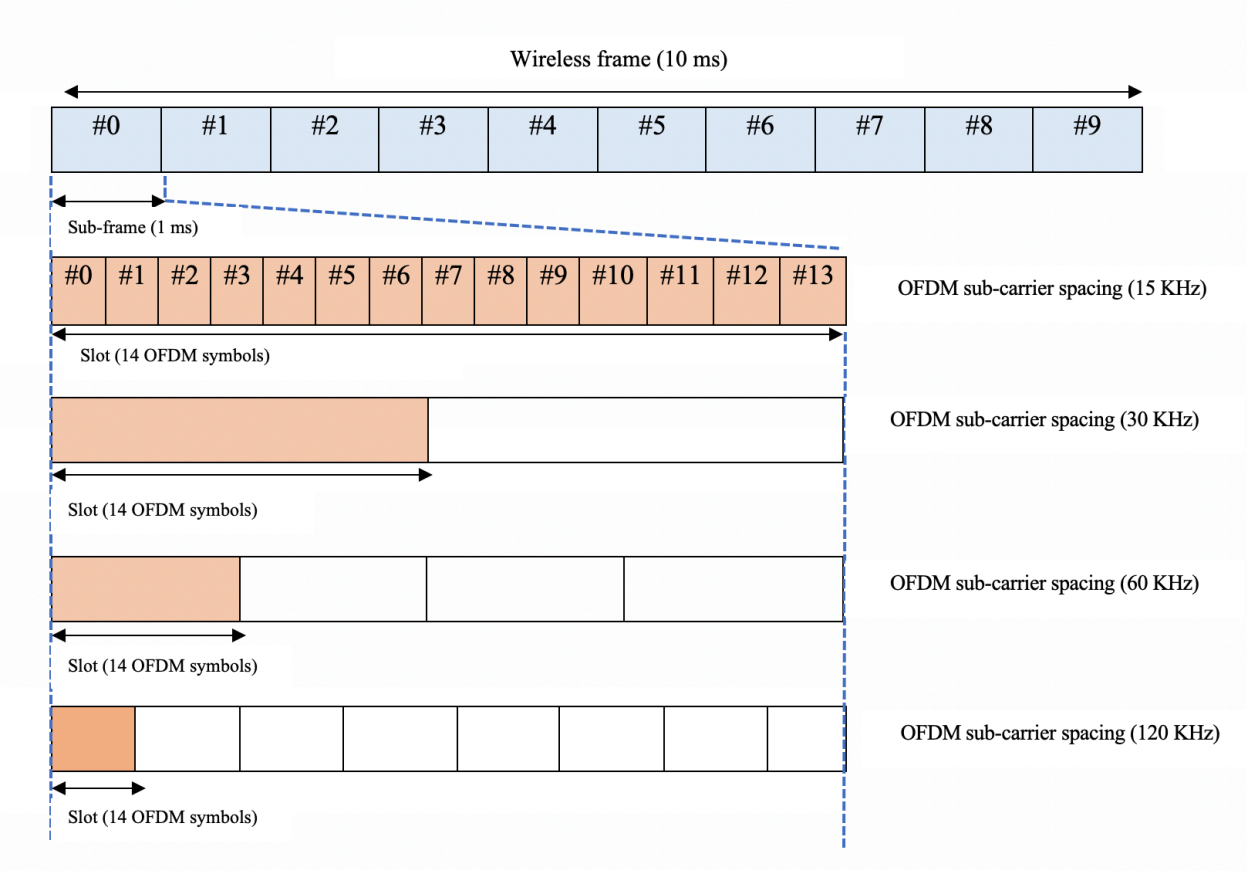


Figure 3: General frame structure of 5G NR Source: NTT Docomo

According to 3GPP specifications, numerology refers to one kind of subcarrier spacing type. Since there is only one subcarrier spacing in 4G LTE 15KHz, need no specific terminology for

indication [9]. Contrarily, 5G NR has various type of subcarrier spacing numerology μ as follows:

Table 2: 5G NR supported transmission numerology

μ	$\Delta f = 2^{\mu}.15$[KHz]	Cyclic prefix
0	15	Normal
1	30	Normal
2	60	Normal, Extended
3	120	Normal
4	240	Normal

Different types of 5G numerology have a different impact on the system structure as well as interference depending on the system conditions. In this paper the authors present a depth description of 5G numerology and emphasizes on the frequency range should not be the only parameter for the numerology consideration of 5G. Therefore, 120 KHz sub-carrier spacing may not be a good option for the mmWave. The trade-off between inter-carrier interference (ICI) and inter-symbol interference (ISI) performs better in 60 KHz sub-carrier. [10]

Related Study

A denial of Service (DoS) attack defines an attack that attempts to make a system or service unavailable for a specific time. When multiple sources in the network correlate with each other in order to generate an attack (DoS), it becomes known as DDoS attack. DDoS is the most common security threat for all sorts of network communication. Even after 5G NR provided such excellent services, including higher speed and scalability, it remains an ever-growing threat to

hampering the regular network performance of 5G. DDoS refers to an attack consisting of a number of connected nodes trying to overwhelm the network by attacking a single node within a time interval to send a specified number of messages. In this case, the single node will be the victim, and the many systems should attack it in that network. Thus, such an attempt to make a system inaccessible to the intended user, for instance, unable to access a website. A complete DDoS attack holds all the available network or system resources, which in turn causes slowdown or server crash.

Several concerns are studied in the deployment of 5G; among them, security is vital [11]. Currently, in the 5G NR network, providing secure communication for each individual is one of the major challenging issues that must be addressed. Such type of works has attracted many researchers to explore more. [12]

Generally, there are three essential components of security for 5G NR:

1. All the security issues and requirements of the earlier generations still apply in 5G.
2. Due to the increase of the number of users and heterogeneous connected devices in the network demand high user privacy.

New techniques, architectures, and services like network softwarization, SDN, NFV, multi-access edge computing, and network slicing will propagate new kinds of security and privacy threats. [13]

Cybersecurity scholars generally focus on two schemes to resolve 5G challenges. One is related to figure out the security commitment of the core 5G NR (carrier level deployment). Another one is to overcome the concern regarding security at the edge point of the communication (end-to-end) [14].

A good amount of work and research is conducted and still going in the 5G NR core network to provide seamless communication and secure connections. This section mainly focuses on the work related to 5G core network parameter modifying and DDoS attacks. ML (Machine Learning) and AI (Artificial Intelligence) based approaches are already gain attention in the purpose of DDoS analysis, including detection and mitigation. A single or combination of a couple of ML techniques provides new insight into the diverse area of 5G components during unpredictable network dynamics and conditions. Therefore, immense research and work will bring a secured 5G infrastructure from each perspective (edge point and core level) to achieve cost-effective, more reliable, and scalable, secure communication around the world. Hence, a study related to ML and AI for 5G NR also considers for this section.

Machine learning techniques can be applied in multiple domains of the 5G network in terms of performance and security. Among the four areas can be generalized:

(1) ML-enhanced SON. (Machine Learning enhanced self-optimization Network) which consists of Data Network, Core Network Management Plane including (Control Panel (CP)/User Panel (UP)), Access Network (CP/UP), UE (User Equipment). ML can be applied by collecting data like location of UE, resource allocated per UE from Access Network and core traffic nature, resource utilization data from Core Network. Therefore, ML will generate outcomes in network parameter optimization, coverage, capacity and quality of services, traffic classification, etc.

2) ML-enhanced network slicing- Different network structures and resource management schemes are associated with different slices. By applying ML in the 5G network, slicing can predict slicing performance, automated service design, and evaluate multiple schemes for end-user satisfaction.

(3) Traffic classification- ML applied to monitor packets, data, and network flow in real-time and provides high-level network analytics.

(4) Security- preventing attacks and frauds by recognizing user patterns in the network and tagging certain events to prevent similar attacks in the future.

The primary consideration of this work [15] is to design an intelligent authentication system to enhance 5G and beyond 5G technology's security performance. Machine learning parametric and non-parametric methods (supervised, unsupervised, and reinforcement learning techniques) have been applied to improve and ensure intelligent authentication activities during communication. An automatic, advanced defense system designed to ensure end-to-end protection in the 5G network. The authors introduced a noble approach by applying software-defined security with machine learning techniques. One of the major focuses of this work is converting network flows into images then using the CNN (Convolutional Neural Network) method for analysis and better accuracy in anomaly detection. [16]

Another approach [17] has been implemented under the Software-defined 5G architecture. This work observes traffic monitoring status and capture network uncertainties in a global view. Based on traffic flow detection, it incorporates and combines multiple security function modules and detects intrusions efficiently. Machine learning algorithms Random Forest has been applied to select a subset of typical traffic features and classify the network flows done by combining k-mean++ and Adaboost algorithms.

Due to the scarcity of proper large 5G traffic datasets, a method has been proposed to gather data. In this method, a raytracing simulator combined with a vehicle traffic simulator has been utilized to generate 5G propagation channel data to investigate beam-selection techniques on

vehicle-to-infrastructure using millimeter waves. Deep learning in classification, regression, and reinforcement learning has been applied for evaluation and analysis. Moreover, machine learning for beam-selection to predict the best beam pairs in the context of mmWave to cellular systems. [18]

This paper represents a significant number of practical solutions for the 5G domain from an ML perspective. Moreover, it illustrates some convincing proposals where ML can assist core 5G network requirements, underline specific use cases, and focus 5G services with limitations. Several types of research in supervised, unsupervised, and reinforcement learning proposals have been mentioned and discussed here. [19]

In 5G network slicing, dynamic network resource allocation (compute, memory, and bandwidth resources) problems arise during a single network infrastructure is divided into (virtual) multiple slices to meet the demands of different users with varying requirements. A deep reinforcement learning framework has been introduced to overcome dynamic decoupled resource allocation issues, and the evaluation result improves performance compared to a baseline equal-slicing strategy [20].

Due to the rapid growth of devices in the 5G domain, complicated network configuration has increased, and handling millions of traffic flows is still challenging. To classify mobile applications accurately at the initial state, a comprehensive scheme incorporated with various state-of-the-art machine learning (ML) algorithms, big data analytics platforms, SDN, and NFV have been studied. These combinational schemes have been applied for developing future 5G Self-optimization network SON applications (data collection, storage, analytics, and virtualization). Moreover, Network QoS (Quality of Services) control for traffic application

based on Software Defined Networking (traffic classification) has been implemented and provide satisfactory improvement. [21]

The capacity of connected devices in 5G NR is better than other network generations like 4G LTE. Hence, the increasing number of devices in the network is also responsible for attempting suspicious activities to disrupt the network performance as well as regular transmission. A work studied several DDoS attacks and proposed an attack detection framework in 5G with Deep Neural Network. The authors applied their framework to industry datasets in which the framework performed with high accuracy of 99.69%. Machine learning techniques like extreme Gradient Boosting and others are used to improve the network 5G SDN network performance. The primary concern of [22] is to analyze a couple of Machine Learning techniques to mitigate the DDOS attacks for the security purpose of SDN. Similarly, another framework detection of DDoS attack in SDN has used with several ML techniques i.e., Support Vector Machine (SVM), Artificial Neural Network (ANN), K-Nearest Neighbors (KNN), and Naïve Bayes (NB) for the classification. The results show KNN works better with high accuracy [23].

To analyze the 5G NR network performance with modifying parameters (bandwidth, distance) and DDoS attack, identify and study the changes influenced by the parameter adjustment is the major goal of this work. Several simulations have been accomplished based on the proposed 5G NR network and create both normal and malicious traffic datasets that are eventually used for classification with ML techniques. The experiment outcomes conclude that distance creates impact depending on the distance between the mobile node and Base Stations in 5G even with a better bandwidth.

CHAPTER 3

Methodology

5G NR maintains a cell site system by partitioning the area into sectors and sending the encoded data over the radio waves. With a wired or wireless backhaul connection, each cell site should be connected to a network backbone. This network uses the OFDM (Orthogonal Frequency-Division Multiplexing) to reduce interference, a similar 4G LTE encoding schemes for modulating digital signal over many various channels. The 5G NR conveys similar networking principles of 4G LTE. In case of greater scalability, the 5G NR structure can enhance OFDM, allowing more users to access the network effectively. This network produces larger bandwidth by developing the usage of spectrum resources (from 3GHz to 100 GHz). 5G NR can handle both the lower band (sub-6 GHz) and mmWave (24 GHz and more) [4].

There are two types of standards for 5G NR: NSA earlier version and Standalone. NSA provides two new radio frequency ranges from:

- FR1 (Frequency Range 1): This band ranges from 450 MHz to 60000 MHz, overlapping 4G and calls as sub-6 GHz.
- FR2 (Frequency Range 2): It ranges from 24 GHz to 52 GHz and is known as the mmWave frequency band.

Types of Attack

On the internet, to shut down a service or website from legitimate users, cybercriminals induce DDoS attacks easily by sending too many service requests to a particular target on that network. Targets can be some industries such as financial and medical services, including public sectors. An effective DDoS attack means the user's unable to access the services they need. A few high-

profile industries suffered lost revenues as well as their reputation during the DDoS attacks. There are different types of DDoS attacks occurred in recent times.

Among them, these are most likely to happen:

1. SYN Flood
2. UDP Flood
3. ICMP Flood
4. HTTP GET Flood

SYN Flood: This is a common form of DDoS attack where an attacker immediately launches a TCP (Transmission Control Protocol) connection request to flood the DNS (Domain Name System) server. Generally, TCP connection is starting by a client through a three-way handshake of the message:

- At first, by sending an SYN(synchronize) message to the server-client starts the request.
- Then server accepts the request as an acknowledgment through sending back SYN-ACK to the client
- The client responds that with an ACK and finally establishing the connection.

For every communication, this three-way exchange communication is the essential thing for establishing a connection. A protocol named TCP is applied for such a procedure. When the server receives an SYN request then responds over SYN-ACK and holds the communication open until it receives an acknowledgment from the client. However, in the case of SYN Flood, the client acknowledgment never appears and consumes the server's resources up to the connection times. Numerous incoming SYN requests to the target server use up all the other available server resources, leading to a successful SYN Flood DoS attack.

To generate SYN Flood attack, TCP_SYN packets were considered to trigger every 1000 microseconds for the simulation. Hence, TCP_SYN packets are created and sent every 1000 microseconds and open the connection between the client and the target.

UDP Flood: Like SYN Flood, this is another type of DoS attack where the attacker sends a huge number of UDP (User Datagram Protocol) packets to the target system to overwhelm the target. Hence, the target can no longer handle its legitimate client request. In this work, the attack time interval is 0.001*seconds for the target to launch the UDP request.

ICMP Flood: This DoS attack is also known as ping flood, in which the attacker attempts to overwhelm the target's resource by sending a large number of ICMP echo requests.
Three DoS attacks SYN Flood, UDP Flood, ICMP Flood, have considered this work's simulation.
5G NR network that is expected to start gradually in 2019 eventually made a revolution in the coverage of huge connected devices communication. In a 5G network (cellular), there are two types of subsystem (1) radio access network and (2) core mobile network.

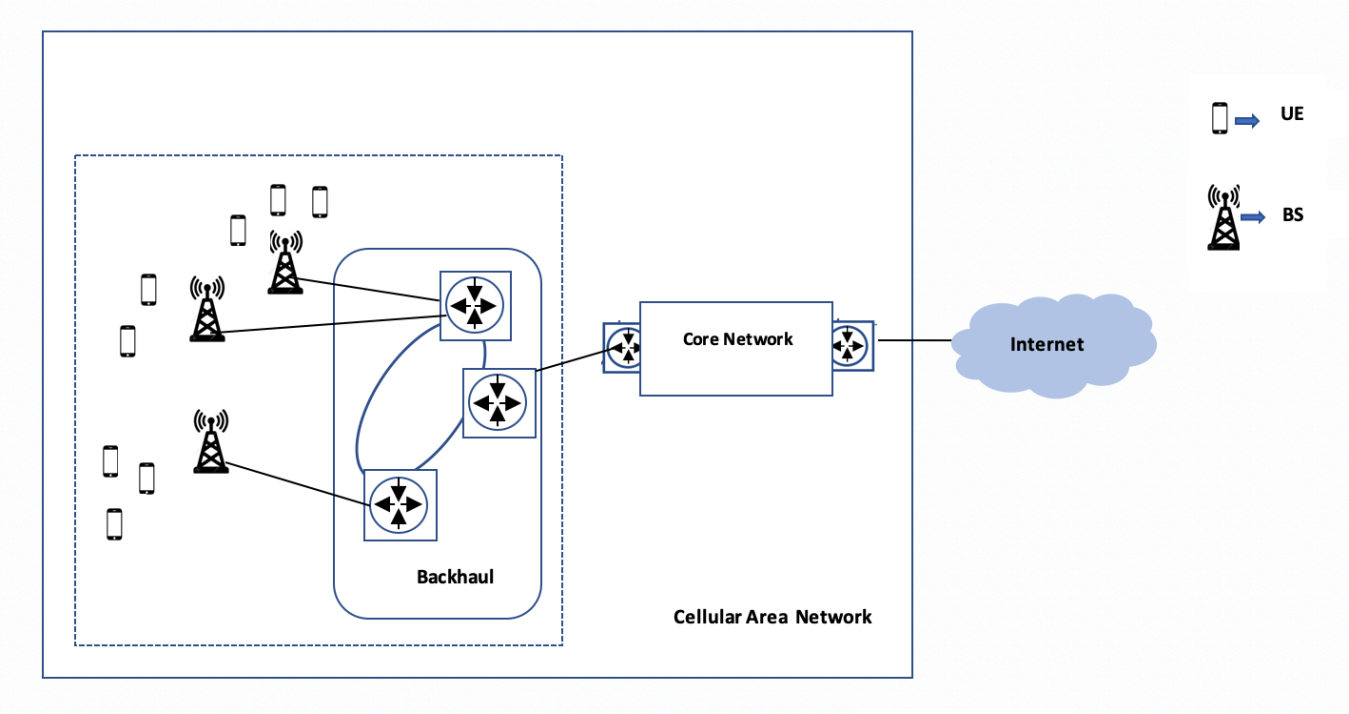


Figure 4: 5G general architecture

Each radio access network consists of Base Station (gNB) and UE (User Equipment) supported by the backhaul network. The cellular network comprises radio access and core mobile, which establish the DDoS attack's possible target connection, shown in Figure 4. The role of BS is to work as a radio transmitter/receiver and act as a hub in the communication network. According to the 3GPP specification, backhauls 5G core network is the central point of the whole network. A detail about 5G network component is described [24].

Workflow Description

To analysis the network performance for 5G NR, a few parameters have been chosen for each sample scenario. Later, create DDoS attacks and compare the network performance. Stored the traffic information to create a dataset which eventually used for classification. To complete the work, these are some significant steps as follows:

1. Firstly, design a customized 5G NR network with a couple of nodes such as UEs, BS, Router, and connections. Figure 5 shows the proposed, designed network for this work. This network consists of two UEs, one gNB (BS), one Router, one EPC, and two Wired nodes with a couple of connections together.

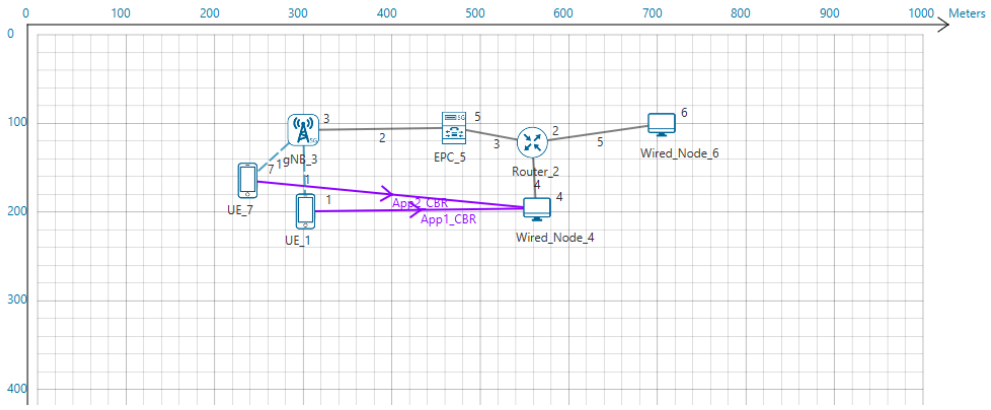


Figure 5: Proposed 5G network

2. Run the designed network by considering the default parameters (i.e., frequency, bandwidth, distance, etc.)
3. Store the results such as packet tracer, event tracer, application throughput regarding the change of parameters.
4. Generate some DDoS attacks and capture those data traffics for comparison.

5. Accumulate the packet and event information for creating the dataset.
6. Apply machine learning techniques upon datasets for the classification and record the accuracy.

The following Table 3 shows the Selected features for the dataset collected from the packet and event traffic outcomes.

Table 3: Selected features for the dataset

No.	**Name**	**Comment**
1	datapath_id	Identity of data
2	flow_id	Identity of the data flow
3	ip_src	Source IP Address
4	tp_src	Source port
5	ip_dst	Destination IP Address
6	tp_dst	Destination port
7	ip_proto	protocol
8	packet_type	Types of packet (TCP, ICMP, UDP)
11	flow_ duration_sec	Time of the flow data
12	flags	SYN-ACK. Only used for TCP
13	packet_count	Number of packet
14	byte_count	Number of bytes
15	packet_count_per_second	Each packet in second
16	byte_count_per_second	Each byte count in second
17	label	Normal or Attack

There are 20 features consider for this dataset among then 17 majors are mentioned. These features are aggregated from the normal and attack traffic event and packet log information regarding the simulation context.

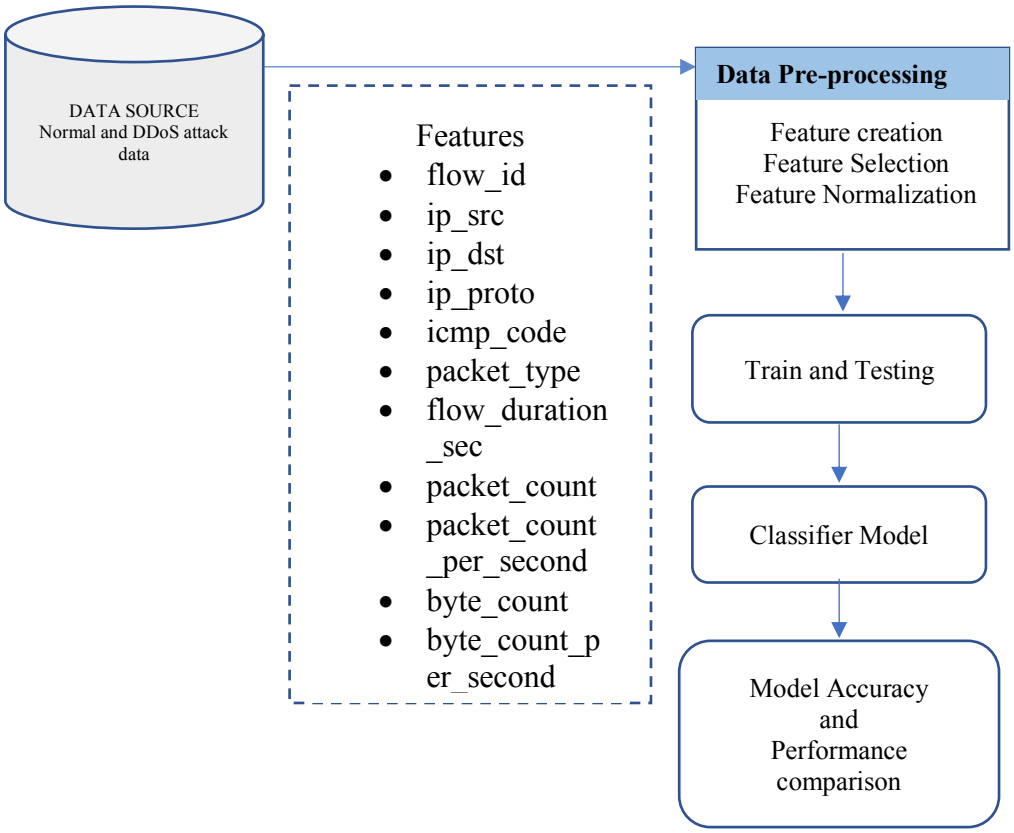


Figure 6: General steps of feature selection and applying machine learning model

The above Figure 6 represents the general steps for the classification procedure. In the beginning, raw data were normalized to achieve better classification results. These data are actually a 10ms simulation time outcomes. After completing the data preprocessing phase, data were split into train and testing purposes and eventually used for classification to find out the model classification accuracy.

CHAPTER 4

Result and Discussion

The core 5G network performance may vary for several reasons. For instance, the distance between node (UEs) and BS can significantly slow down the data transfer and receiving rate of end-to-end communication. Thus, it causes many hinders in the regular transmission. Moreover, to degrade the performance of the network services, a DDoS attack applies in several ways to hold the network resources as well as creates disruptions in the communication. A system like bots is currently used for such types of attacks that serve in a distributed fashion [25]. DDoS attacks are considered as one of the most frequent threats for 5G NR. Since many connected devices increase as the coverage increases, it leads communication maintenance more complex and cost-effective in terms of security. This section showed and described the multiple cases tested by adjusting some parameters of 5GNR and creating DDoS attacks in the designed 5G network. Later, the simulations produce metrics along with packet and event information. These traffic information for both normal and DDoS attack scenarios, including parameter modifying, have been selected for the dataset. After following the data processing procedure, including normalization, ML techniques were applied for the classification.

Simulation Configuration

In this age of innovation, wireless technology is advancing and opening the door to many possibilities. A new global wireless standard, (5G) has intended to convey high-speed information and data, ultra-low latency, expanded network capacity, availability, and designed to connect everything including machines, entities, and devices together virtually.

Since 5G inherits all the previous versions of global wireless standards, most of the techniques and services have overlapped. In 5G researchers, and developers are continuing their investigation in the aspects of some 5G components and services like mmWave transmission, massive MIMO, beamforming, non-orthogonal multiple access (NOMA). Apparently, for the assessment and to investigate a simulation of 5G in real life is quite computationally complicated and expensive.

To address this issue, a good number of simulator techniques, approaches have been introduced and being developed i.e. NYUSIM, MATLAB 5G toolbox, OMNet++, Network Simulator-3(ns-3), NetSim and so on. The deployment of each simulation technique provides services according to the requirements and desired application. For instance, MATLAB 5G toolbox basically great for link level simulations whereas NetSim focus work like system level or application level simulations. To study 5G NR behavior and network performances, simulation tool NetSim version 12.2 considered for this work. This simulator provides features like application model analysis, network design and planning, simulation testing and verification with an interactive GUI (Graphical User Interface). This simulator can be applied in various areas including academic, industry and defense to design, simulate, analyze, modify and observe the performances of different networks and it is available in three versions Academic, Standard and Pro.

NetSim provides a full package of 5G NR mmWave library and features including end-to-end, packet and event level simulation of 3GPP standards. This tool also supports all layers of protocol, Wireless protocols, Routing Algorithms, Metrics, Animation, traffic information, interactive simulation via GUI or through files etc. With this tool, both GUI and command line executions can be possible regarding the experiment context. Moreover, packet and event trace

file generated from each simulation results can be used for simulation analysis. In NetSim, user can also use their custom code (python), implementation details and merged with another one platform i.e. MATLAB according to the planning. For the design and planning of the network drag and drop options are available. Each device or node has a particular configuration window such as set up frequency, distance, assign protocols in different layers (network, applications), capture packet results through Wireshark etc.

Parameter Settings

The common parameter used for the simulation is mentioned in Table 5.1. The runtime for the simulation is set to 10s. The whole simulation work is done by the NetSim version 12.2. Figure 5.1 shows the designed 5G NR network. This network consists of 2 UEs (User Equipment), one gNB BS (Base Stations), 1 EPC (Evolved Packet Core), which are used to accumulate data traffic from end devices like 4G LTE, 1 Router and 2 Wired_Node, and a couple of connections. The solid lines represent wired whereas dotted wireless.

For the application throughput analysis, data, voice, video can be used in the NetSim. In this work, CBR (Constant Bit Rate) had chosen to determine the application rate.

Following Table 4 shows the parameters for proposed 5G NR configurations.

Table 4: Common parameters for the simulation

Parameter	Value
UEs	2
Malicious UE's	2
Frequency	FR1 and FR2
CA Type	INTER_BAND_CA, INTRA_BAND_CONTIGUOUS_CA
Numerology	0, 2
Distance from gNB	50-400 meter
Propagation Model	URBAN_MACRO

In the above table the number of UEs are four where two are malicious, frequency range considered as FR1 and FR2 knows as lower band and upper band respectively.

To increase the bandwidth, CA concepts used in both LTE advanced and 5G NR. Two spectrum usages techniques FDD (Frequency Division Duplex) and TDD (Time Division Duplex) can be used for CA. The NetSim simulator provides a couple of CA options including INTER_BAND_CA, INTRA_BAND_CONTIGUOUS_CA. Each of the band gives a flexibility to choose particular numerology, bandwidth and propagation model as required. Major key feature of 5G NR is sub carrier spacing is no longer fixed with 15 KHz, it is scales by $2^{\mu} \times 15$ KHz for different aspects. The Numerology for the 5 NR are consists of 0, 1, 2, 3 in category with different frequency. Propagation model such as URBAN MACRO, Macro Cellular, can select according to the desired application design.

Application throughput for this 5G network can found in the application metrics after simulation for the corresponding cases. The metrics also hold information related to the total number transmitted payload (bytes), which is equal to the product of "Transmitted Packets" and "Size of the Packets," which can be defined as follows:

$$Application\ Throughput\ (MBPS) = \frac{Sum\ of\ total\ received\ application\ layer\ payload * packet\ size}{Simulation\ time}$$

Case Study: Normal Scenario

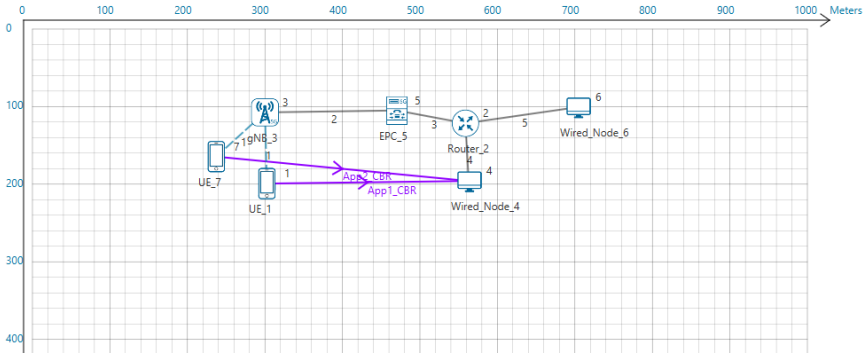


Figure 7: Proposed 5G network in Normal Scenario

The above Figure 7 is representing as the normal case for the simulation. The parameters for this are found in the following Table 5. In this table, two UEs (Node 1 and Node 7) configured regarding the frequency ranges and numerologies.

Table 5: Parameter and Application throughput in Normal Case

Case No.	Scenario	Node	Distance from gNB (meter)	Frequency Band	Numerology	Bandwidth(Channel) (MHz)		Application Throughput(Mbps)
						CA_1	CA_2	
1	Normal	UE_1	100	FR1	0	5	10	11.842352
2	Normal	UE_7	50	FR1	0	5	10	11.848848
3	Normal	UE_1	100	FR1	2	40	100	12.523376
4	Normal	UE_7	50	FR1	2	40	100	12.548048
5	Normal	UE_1	100	FR2	2	100	100	23.560896
6	Normal	UE_7	50	FR2	2	100	100	23.565568

The experimental simulations show that the application throughput rate for this normal case (without any attacks) is better for the upper frequency bound FR2.

The graph of the Application and Link throughput is given below:

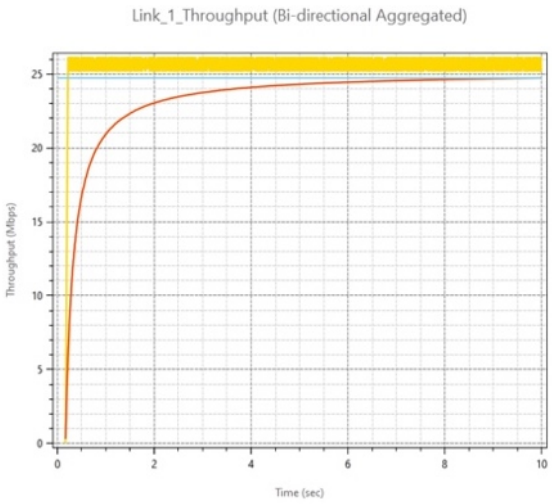


Figure 8: Normal scenario application throughput

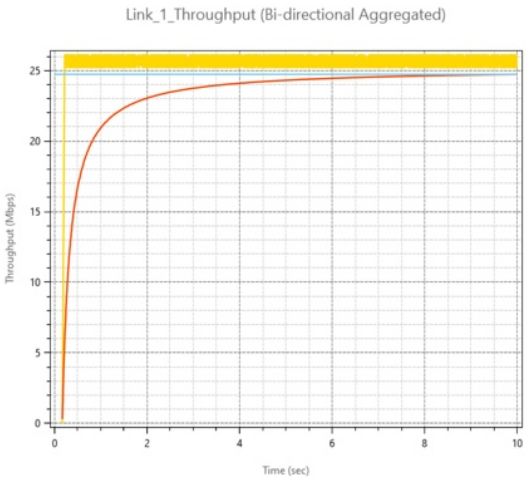


Figure 9: Normal scenario link throughput

In the above Figure 9 represents the link throughput for the bi-directional way. In the Grid, both Figure 8 and 9, line X axis shows for the Time (sec) and Y axis as Throughput (Mbps). The red line shows the cumulative moving average, and the blue line for average time.

The following Figure 10 shows that the distance has changed from the BS(gNB) to UEs (UE_1, UE_7) by keeping the rest of the parameter the same as earlier.

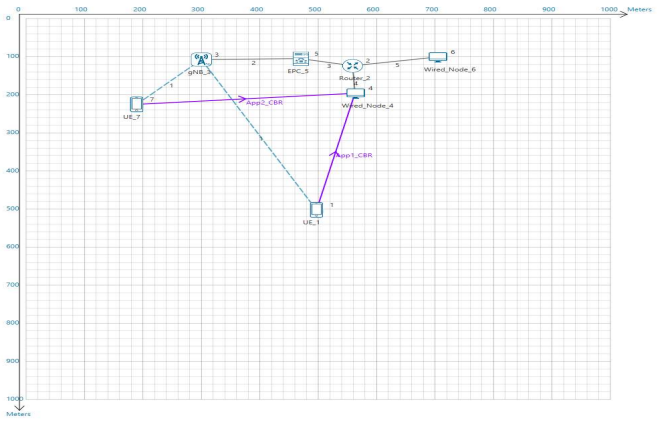


Figure 10: 5G network in normal scenario with distance change

Table 6 holds the parameters for this testing case. In contrast to previous simulation for frequency range FR1 and FR2 the throughput rate eventually dropped due to distance change.

Table 6: Parameter and Application throughput in Normal Case (Distance change)

Case No.	**Scenario**	**Node**	**Distance from gNB (meter)**	**Frequency Band**	**Numerology**	**Bandwidth(Channel) (MHz)**		**Application Throughput(Mbps)**
						CA_1	**CA_2**	
1	Normal	UE_1	400	FR1	0	5	10	5.45224
2	Normal	UE_7	120	FR1	0	5	10	11.840016
3	Normal	UE_1	400	FR1	2	40	100	15.087056
4	Normal	UE_7	120	FR1	2	40	100	23.552720
5	Normal	UE_1	400	FR2	2	100	100	5.448720
6	Normal	UE_7	120	FR2	2	100	100	5.442880

Case Study: DDoS Attack Scenario

Figure 11 and Figure 12 illustrates the TCP SYN_Flood and ICMP_Flood, UDP_Flood as DoS attack with two malicious nodes (UE_6, UE_8). Moreover, distance of both UEs changed for this case, for example UE_1 (Node) distance from the BS (gNB) here is 400 meters instead of previous 100 meter.

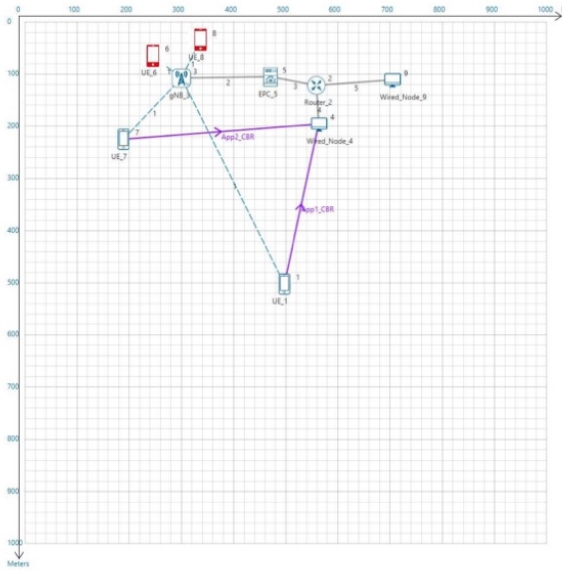


Figure 11: 5G network with malicious node for SYN_Flood attack.

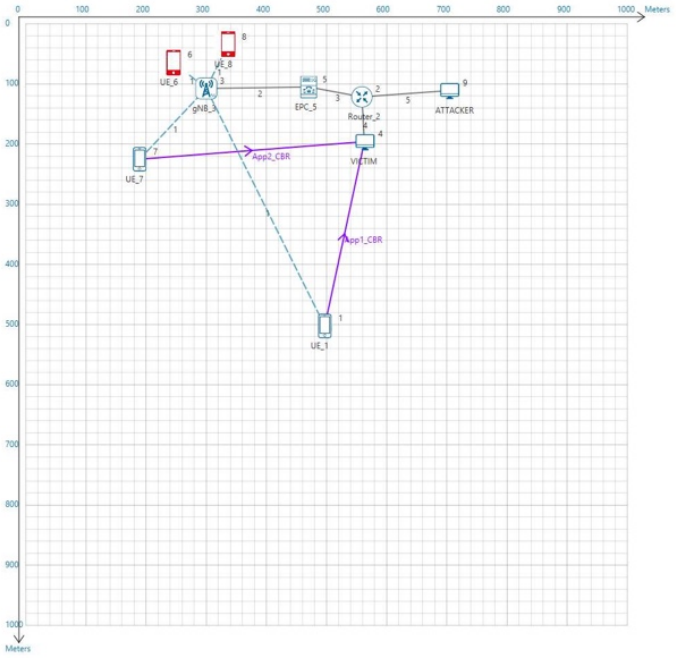


Figure 12: 5G network in DDoS attack (TCP, ICMP, UDP attack).

Table 7 the DDoS attack scenario with distance changes for both UEs shows that application throughput reduces for applying the attack. For instance, the application throughput for UE_1 here is 4.847200Mbps which found 5.45224 Mbps without DDoS attack in Table 6.

Table 7: Parameter and application throughput in DDoS case (Distance change)

Case No.	Scenario	Node	Distance from gNB (meter)	Frequency Band	Numerology	Bandwidth(Channel) (MHz)		Application Throughput(Mbps)
						CA_1	CA_2	
1	DDoS	UE_1	400	FR1	0	5	10	4.847200
2	DDoS	UE_7	120	FR1	0	5	10	10.988544
3	DDoS	UE_1	400	FR1	2	40	100	14.700448
4	DDoS	UE_7	120	FR1	2	40	100	23.549072
5	DDoS	UE_1	400	FR2	2	100	100	5.376304
6	DDoS	UE_7	120	FR2	2	100	100	5.375136

After the competition of the simulations, a couple of metrics such as TCP, IP, IP_Forwarding, UDP will generate. For instance, application metrics include Application Id, name, source id, destination id, the total number of packets transmitted from the source, number of packets (bytes) received at the destination, total payload, etc. Moreover, corresponding packet and event traffic data for both normal and attacks scenario will have produced. For this work, the simulation runs for a short time due to testing purposes. However, more traffic data can be aggregate depending on the time you want to simulate, which eventually helps to generate a large dataset. From the result of the above simulation, we could conclude a couple of matter as follows:

1. For benign traffic, when modifying the distance of the node (UEs) from the BS (gNB), the overall application throughput reduces. For instance, FR1 before distance change the node UE_1 application throughput 11.842352. When changed the distance with the same

network configuration, it reduces to 5.45224. Therefore, it seems distance from the node (UE) to BS (gNB) creates a great impact in terms of application data rate.

2. With the DDoS attack, this node (UE_1) application rate scale down to 4.847200 for frequency range FR1. Thus, distance from the Base Station could degrade network performance more than the simulated DDoS attacks even with a higher bandwidth rate based on this designed 5G network.
3. In frequency range FR2 with the distance change, results show that in shorter distance the high frequency works better (data rate better than usual) the FR1. However, when it for long-distance FR1 work better for the Urban propagation model.

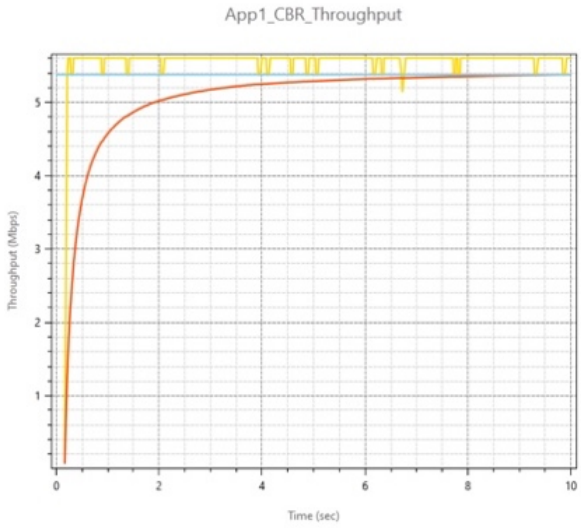


Figure 13: DDoS attack scenario application throughput attack.

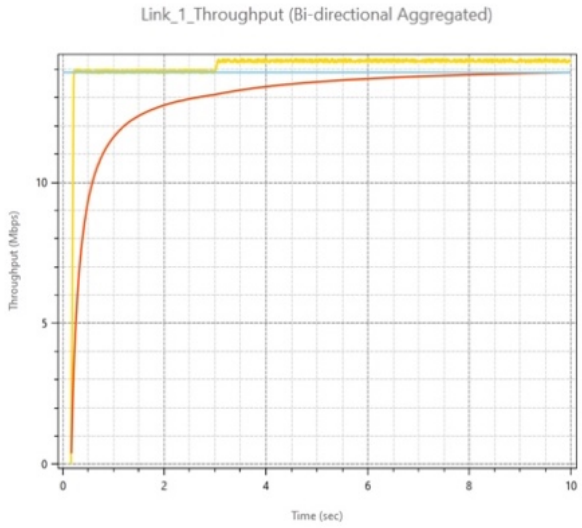
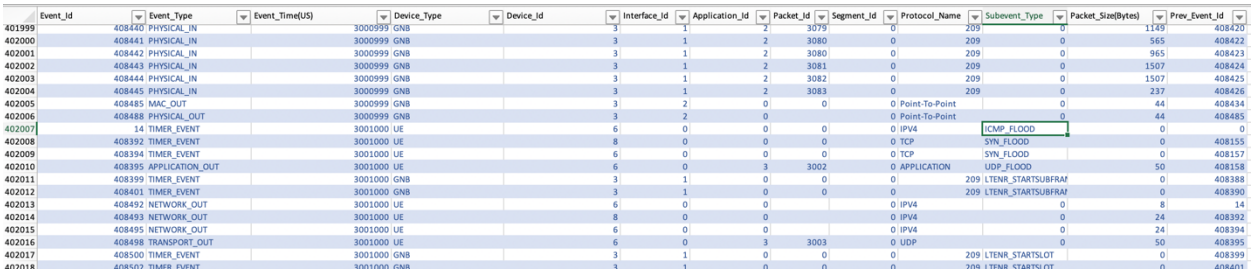


Figure 14: DDoS attack scenario link throughput.

In addition, the network performance derogates depending on the distance from the node to the BS and application throughput rate getting below while inducing some DDoS attacks. The traffic dataset for both normal and malicious have stored and then used the machine learning model for the classification purpose. The above Figure 13 and 14 shows the application throughput for both application and link after DDoS, dropped in comparison to earlier simulations outcomes.

The below Figure 15 shows the DDoS traffic information as event tracer. The attacks are identifying as SYN_FLOOD, ICMP_FLOOD and UDP_FLOOD in the Subevent_Type category. From this event traffic some features like Event_type, Protocol _Name, Packet_Size selected for the dataset.



	Event_Id	Event_Type	Event_Time(US)	Device_Type	Device_Id	Interface_Id	Application_Id	Packet_Id	Segment_Id	Protocol_Name	Subevent_Type	Packet_Size(Bytes)	Prev_Event_Id
401999	408440	PHYSICAL_IN	3000999	GNB	3	1	2	3079	0	209	0	1149	408420
402000	408441	PHYSICAL_IN	3000999	GNB	3	1	2	3080	0	209	0	565	408422
402001	408442	PHYSICAL_IN	3000999	GNB	3	1	2	3080	0	209	0	965	408423
402002	408443	PHYSICAL_IN	3000999	GNB	3	1	2	3081	0	209	0	1507	408424
402003	408444	PHYSICAL_IN	3000999	GNB	3	1	2	3082	0	209	0	1507	408425
402004	408445	PHYSICAL_IN	3000999	GNB	3	1	2	3083	0	209	0	237	408426
402005	408485	MAC_OUT	3000999	GNB	3	2	0	0	0	Point-To-Point	0	44	408434
402006	408488	PHYSICAL_OUT	3000999	GNB	3	2	0		0	Point-To-Point	0	44	408485
402007	14	TIMER_EVENT	3001000	UE	6	0	0	0	0	IPV4	ICMP_FLOOD	0	0
402008	408392	TIMER_EVENT	3001000	UE	8	0	0	0	0	TCP	SYN_FLOOD	0	408155
402009	408394	TIMER_EVENT	3001000	UE	6	0	0	0	0	TCP	SYN_FLOOD	0	408157
402010	408395	APPLICATION_OUT	3001000	UE	6	0	3	3002	0	APPLICATION	UDP_FLOOD	50	408158
402011	408399	TIMER_EVENT	3001000	GNB	3	1	0	0	0		209 LTENR_STARTSUBFRAI	0	408388
402012	408401	TIMER_EVENT	3001000	GNB	3	1	0	0	0		209 LTENR_STARTSUBFRAI	0	408390
402013	408492	NETWORK_OUT	3001000	UE	6	0	0		0	IPV4	0	8	14
402014	408493	NETWORK_OUT	3001000	UE	8	0	0		0	IPV4	0	24	408392
402015	408495	NETWORK_OUT	3001000	UE	6	0	0		0	IPV4	0	24	408394
402016	408498	TRANSPORT_OUT	3001000	UE	6	0	3	3003	0	UDP	0	50	408395
402017	408500	TIMER_EVENT	3001000	GNB	3	1	0	0	0		209 LTENR_STARTSLOT	0	408399

Figure 15: DDoS attack traffic event information.

Machine Learning model

There are a good number of machine learning classification models employed for the classification. K-Nearest Neighbors (KNN), Naïve Bayes, and Support Vector Machine schemes were used in this work. In the case of classification problems, these algorithm works well. Moreover, it is simple, easy to explore, and needs fewer system resources or configurations to run.

K-Nearest Neighbors (KNN)- In ML, a supervised algorithm refers that depends on labeled input data to learn a function for the corresponding output at the time of facing unlabeled data. KNN is one of the common supervised algorithms in ML. It is easy to understand and implement that can be applied for problems like classification and regressions. This algorithm works by assuming close proximity principles, which are similar points to each other. When a new input comes in, the algorithm determines a new data class by searching at its closest K neighbors. A few distance functions like Manhattan, Minkowski, and Euclidean distance are considered to find the distance between two data points. Data classification and class labeled detection can be found by the similarity between the sample. The distance of the newly arrived data and the data in the training set was estimated individually considering the distance function. By selecting the k size dataset, the classification has done. For this classification, k has considered as 2.

Naïve Bayes- This is a probabilistic ML algorithm used for the class category based on Bayes Theorem. Bayes theorem is a simple concept of conditional probabilities in which the probability of an event occurring given that by assumption, another event has occurred. In this algorithm, a fixed size of training data is used for the system with a class. The main principle of this algorithm is each pair of features being classified is independent of each other. In many aspects, it has been successfully applied and specifically works well in Natural Language Processing (NLP). The accuracy of NB depends on the increasing rate of the number of training data. The more training data, the algorithm can detect the actual category of the test data better. For this work, NB with Gaussian kernels is used.

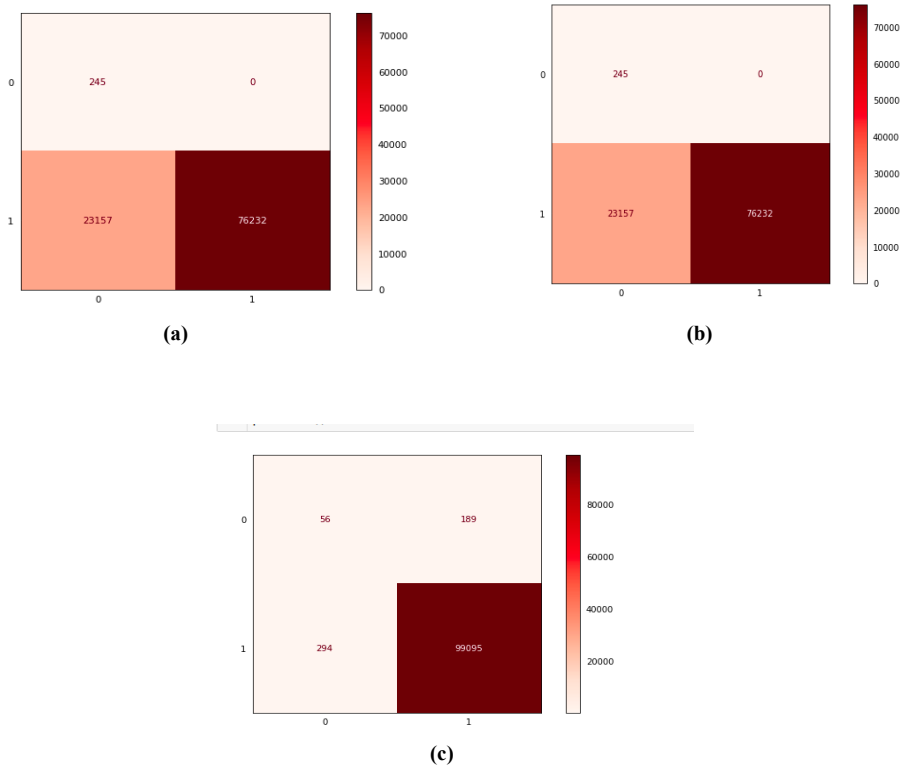


Figure 16: Confusion Matrix of (a) KNN (b) NB and (c) SVM

Support Vector Machine: SVM is another supervised learning approach that is used for classification and regression analysis. The basic idea of this algorithm is based on deciding an appropriate hyperplane with N-dimensional space where N is the number of features (decision functions) that distinctly classify the data points, i.e., the maximum distance between data points of both classes. SVM with the linear kernel used for the classification model. The following Figure 16 shows the confusion matrix of the corresponding ML algorithms.

Model Performance

After completion of the classification, the overall performance among ML techniques are given in Table 8.

Table 8: Classification model performance

Model	Accuracy (%)	Precision (%)	F1-score (%)	Recall (%)	Learning and Predicting Time (hh: mm: ss)
KNN	99.9	99.9	99.9	98.9	0:10:47
NB	76.65	51.5	45.3	67.7	0:01:23
SVM	99.78	97.7	98.1	97.6	0:07:35

From the above confusion matrix and classification model comparison table, we can conclude that KNN works progressively well than others. However, the performance of the classification model basically depends on the type of dataset chosen. Different datasets with various dimensional may attain different results. For instance, in most cases, KNN works better in low-dimensional space, whereas SVM acts well on higher-dimensional space. Moreover, the performance also depends on the size of k in KNN and the selection of hyperplane as well as kernel function in SVM. For example, the linear kernel of SVM requires less time to run but comes with less accuracy than the rbf or Gaussian kernel.

CHAPTER 5

Conclusion

This work's primary focus is to identify the parameters that significantly impact the 5G network and create a DDoS attack dataset. However, there are several DDoS datasets exist, but the public 5G DDoS attack yet has scarcity. After modifying the 5G parameters, the simulation results represent that network performance (application throughput) deteriorates while mobile nodes move away from the Base Station even with higher bandwidth. Due to the limitation of the simulation system and resources, the simulation was considered for a little short time. This dataset is not fully well informative and organized yet. It still needs to consider a couple of more features, especially 5G core network parameters, to increase the robustness of the dataset. To do classification, applied three machine learning methods on the created datasets. The classification model results represent KNN achieves 99% accuracy over SVM and NB. In addition, to explore 5G network performance and create a more robust dataset for 5G DDoS ATTACK detection and mitigation purpose, improving the current dataset is a future aim of this work. While 5G is developing and gradually implemented in multiple areas, the researchers have started the research with future possibilities of 6G. Theoretically, 6G (sixth generation) offers a network operating band at the THz with massive spectrum resources, pervasive network coverage for intelligent devices, dynamic spectrum access, and so on. NYU (New York University) WIRELESS research community rigorously working on the fundamental and advanced issues of wireless communication as well as the development of the next generation (6G and Beyond) network such as 5G and 6G applications, 6G testbeds. 5G and beyond networks open a great number of research directions including THz communication and sensing, low latency network issues, disruptions (signal) in 5G regular transmissions, privacy, and security.

References

1. Cisco Visual Networking Index: Forecast and Trends (2018–2023). Available on: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. (Accessed time: April 2021).
2. 4G vs. 5G: The key differences between the cellular network generations. Available on: https://www.businessinsider.com/4g-vs-5g. (Accessed time: 11 June 2021).
3. 5G Applications and Use Cases. Available on: https://www.digi.com/blog/post/5g-applications-and-use-cases. (Access time: 12 June 2021).
4. A Brief Introduction To 5G Technology. Available on: https://medium.com/the-shadow/a-briefintroduction-to-5g-technology-b50c0f453f4.(Accessed time: Feb 2021).
5. DDoS attacks and 5G: everything you need to know. Available on: https://www.allot.com/blog/ddos-attacks-5g-everything-need-know/.(Accessed time: Feb 2021).
6. Mike Bartock et al., "5G CYBERSECURITY Preparing a Secure Evolution to 5G". Available on: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/5G-pse-project-description-final.pdf , NIST, April 2020.
7. 5G SECURITY ISSUES, Available on: https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf. (Accessed time: May 2021).
8. Everything You Need to Know About 5G, Available on: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g. (Accessed time: 11 June 2021).

9. 5G/NR – Numerology. Available on: https://www.sharetechnote.com/html/5G/5G_Phy_Numerology.html . (Accessed time: Feb 2021).
10. Josue Flores de Valgas et. al, "Flexible Numerology in 5G NR: Interference Quantification and Proper Selection Depending on the Scenario". Volume 2021, Article ID 6651326, (10 Mar 2021). Available on: https://doi.org/10.1155/2021/6651326 .
11. Rabia Khan et al., " A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions", IEEE commun. Surv. Tutor. 22(1). (2020) 196-248.
12. Lalit Chettri, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems", IEEE Internet of Things J. 7(1) (2020) 16-32. Available on: https://ieeexplore.ieee.org/document/8879484 .
13. G.C. Amaizu et. al, "Composite and efficient DDoS attack detection framework for B5G networks", Elsevier B.V, Volume 188, 28 January 2021. Available on: https://www.sciencedirect.com/science/article/pii/S1389128621000438 .
14. 5G Will Change Your Expectations for Performance. Available on: https://www.forbes.com/sites/forbestechcouncil/2020/12/16/5g-will-change-your-expectations-for-performance/ .(Accessed time: Feb 2021).
15. He Fang et. al. "Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks". Published: IEEE Wireless Communication (Volume: 26, Issue: 5, October 2019). Available on: https://ieeexplore.ieee.org/document/8883130 .

16. Jordan Lam, Robert Abbas, “Machine Learning based Anomaly Detection for 5G Networks”. Available: https://arxiv.org/pdf/2003.03474.pdf.
17. Jiaqi Li et. al, “A Machine Learning Based Intrusion Detection System for Software Defined 5G Network”. Available: https://arxiv.org/pdf/1708.04571.pdf .IET Research Journals, pp. 1–6, 2017.
18. Aldebaro Klautau et. al, “5G MIMO Data for Machine Learning: Application to Beam-Selection Using Deep Learning”. Published: 2018 Information Theory and Applications Workshop (ITA), IEEE.
19. Manuel Eugenio Morocho-Cayamcela et. al, “Machine Learning for 5G/B5G Mobile and Wireless Communications: Potential, Limitations, and Future Directions”. Published: IEEE Access (Volume: 7), Page(s): 137184 – 137206, 2019.
20. Jaehoon Koo et. al, “Deep Reinforcement Learning for Network Slicing with Heterogeneous Resource Requirements and Time Varying Traffic Dynamics”. Published: 2019 15th International Conference on Network and Service Management (CNSM).
21. Luong-Vy Le et. al, “Applying Big Data, Machine Learning, and SDN/NFV for 5G Early-Stage Traffic Classification and Network QoS Control”. Available on: https://doi.org/10.14738/tnc.62.4446. Transactions on Networks and Communications, 6(2), 36, 2018.
22. Hassan A. Alamri et. al., “Machine Learning for Securing SDN based 5G Network”, IJCA (0975-8887), Volume 174-No. 14, January 2021.
23. Huseyin Polat et. al., “Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models”, MDPI, Sustainability 2020.

24. Junseok Kim et al., “3GPP SA2 architecture and functions for 5G mobile communication system”, ICT Express, 3 (1), (2017) 1-8. Available on: https://www.sciencedirect.com/science/article/pii/S240595951730019X.
25. Mathias Kjolleberg Forland et. at., “Preventing DDoS with SDN in 5G”. Available on: https://ieeexplore.ieee.org/document/9024497. 2019 IEEE Globecom Workshops (GC Wkshps).
26. Lam J, et al., “Machine Learning based Anomaly Detection for 5G Networks.” Available: arXiv preprint arXiv:2003.03474. 2020 Mar 7.
27. L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M.G. Pérez, and G. M. Pérez, “A self-adaptive deep learning-based system for anomaly detection in 5G networks,” IEEE Access, vol. 6, pp. 7700–7712, 2018. doi: 10.1109/ACCESS.2018.2803446.
28. H. Lauer and N. Kuntze, “Hypervisor-based attestation of virtual environments,” in 2016 Intl IEEE Conferences on Ubiquitous Intelligence Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), July 2016, pp. 333–340.
29. B. Jaeger, “Security Orchestrator: Introducing a Security Orchestrator in the Context of the ETSI NFV Reference Architecture,” in 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug 2015, pp. 1255–1260.
30. Mantas, G., Komninos, N., Rodriuez, J., Logota, E., & Marques, H. (2015). Security for 5G communications. Available on: https://openaccess.city.ac.uk/id/eprint/13047. Fundamentals of 5G Mobile Networks. (pp. 207-220). John Wiley & Sons, Ltd. ISBN 9781118867464.