International Journal of Advanced Technology and Engineering Exploration, Vol 8(82)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2021.874340

Research Article

Analysis of performance vulnerability of MAC scheduling algorithms due to SYN flood attack in 5G NR mmWave

Bhargabjyoti Saikia[1] and Sudipta Majumder[2]*
Senior Assistant Professor, Department of ECE, DUIET, Dibrugarh University, Assam, India[1]
Senior Assistant Professor, Department of CSE, DUIET, Dibrugarh University, Assam, India[2]

Received: 01-July-2021; Revised: 19-September-2021; Accepted: 22-September-2021

Abstract
Fifth-Generation (5G) New Radio (NR) Millimetre Wave (mmWave) is a kind of 5G network that operates in the 24GHz to 100GHz frequency range. It offers several opportunities as well as numerous challenges. One of the most prominent challenges that a 5G network faces is an intrusion. Intrusion is possible because of existing vulnerabilities in the 5G NR mmWave network architecture. We exploited one such vulnerability to create Synchronise (SYN) flood intrusion into the network. The SYN flood intrusion is a Denial of Service (DoS) intrusion. The intruder involved in the SYN flood, depletes the network's available resources. As a result, it denies genuine User Equipment (UEs)/nodes access to the network services and resources. Since this attack produces many open connections with the server, it slows down Media Access Control (MAC) schedulers' ability to assign available channels to the user equipment. In this article, we proposed a method to exploit existing vulnerabilities of the 5G NR mmWave network to carry out SYN flood attacks. Further, we investigated the effect of the attack on the performance of the MAC schedulers, such as proportionate fair and round robin MAC schedulers. With the addition of SYN flood attack UEs/nodes, we observed that the throughput for proportional fair and round robin MAC schedulers drops dramatically. In the event of an attack, the throughput drops by 2.34% to 37.7%. However, in the event of a SYN flood attack, network delay and jitter increase. The performance of the network suffers as a result.

Keywords
SYN flood attack, Proportional fair scheduler, Round robin scheduler, Throughput, Delay, Jitter.

1.Introduction
The Fifth-generation (5G) network will cover most of the UK, US, and many other countries over the next few years. The main advantage of the 5G network is the speed upgrade. The Fourth-Generation (4G) network has a maximum real-world download speed of almost 100 Megabits per second (Mbps) which is 30 times faster than the Third-Generation (3G) network. But, the download speed in 5G is 10 Gigabits per second (Gbps). The 5G divides the geographical area of this network into two small sections known as cells. All devices in a cell are connected to the internet via a network of smaller antennas. Radio waves are used to communicate between antennas and devices. The 5G network employs two types of bands. They are low band frequencies that use 602 to 850 MHz sequences and high band frequencies that use 20 to 100 GHz.

The 5G low-band cell towers have nearly identical coverage areas and range as 4G towers. However, the coverage area for high band 5G (also known as Millimetre Wave (mmWave) or mmW) is minimal. The internet speed in the high band 5G coverage area is much faster than in the low band 5G coverage area.

Quality of Service (QoS) is a critical 5G parameter. The 5G network thrives on increasing spectral efficiency. Latency reduction is essential for this. 5G necessitates the handling of various types of traffic and a diverse set of devices. The QoS requirements for these devices are distinct. The 5G increases the prospects in areas such as healthcare. Clinical communication, telehealth, exterior operations and in-hospital retail are the few use cases of 5G in hospitals. The 5G has many applications in the manufacturing sector. The applications include process automation, remote monitoring of production assets, collaborative robotics and analytics to predict breakdowns. The 5G can facilitate Vehicle-to-Vehicle (V2V) and Vehicle-

*Author for correspondence

to-Infrastructure (V2I) in transportation. A truly autonomous self-driving car can be possible with 5G.

The mentioned applications of the 5G network are critical and time-sensitive. A slight disruption of the 5G service can raise havoc. Quality of service degradation of 5G can potentially create a financial loss. Many people and organizations have tried and successfully carried out attacks, even in 4G. These attacks resulted in performance deterioration of the network. Tu et al. [1–3] have provided new security threats in 4G Long-Term Evolution (LTE) networks. They have demonstrated that SMS threats can propagate towards SMS powered services, causing several attacks. The authors have also shown [2] that an attacker can manipulate the radio resource states, which can cause the user's battery power drainage 5 to 8 times faster. Bhattarai et al. [4] also demonstrated various security threats to 4G LTE networks. They have shown that jamming attacks happen in the 4G network. These attacks have a significant effect on the performance of 4G LTE networks.

Similarly, researchers like Li et al. [5] have shown that the spoofing attack is possible in 5G due to vulnerabilities in the Physical Layer. Sánchez et al. [6] have highlighted the security issues related to the 5G wireless network. We can arrive at a hypothesis that there are still many vulnerabilities in the 5G network. The cybercriminals or attackers can exploit the 5G network vulnerabilities to intrude into the network. These vulnerabilities should be discovered, analyzed, and remedied before malevolent individuals or organizations exploit them. Vulnerabilities exist in the 5G New Radio (NR) mmWave because it is a relatively new technology. This urgency of finding vulnerabilities motivates us to carry out this study.

The study's main objective is to investigate vulnerabilities of the 5G NR mmWave network, especially at the transport and network layer. We have focused on these two layers because routers and firewalls are implemented here. The other objective is to check how the attackers use the uncovered vulnerabilities and their consequences on the network's performance. We found a vulnerability in the 5G NR mmWave. Thus, exploiting it, we created a Synchronise (SYN) flood attack. Also, as per the research objective, we further investigated the effect of the SYN flood attack on the network. We used network performance parameters like throughput, jitter and delay for performance evaluation. Also, we explored other parameters like the number of half-open connections and required overhead transmission for performance evaluation of the network under attack.

We have divided the research articles into the following sections. The section named literature review provides the related studies of the research. The methodology section gives the details of the methods of experiments and justification of the approach. The Result section offers all the findings in tabular and graphical form. Then, we have a discussion section to discuss our findings and their impacts. In the conclusion and future work section, we summarized the important find and related future work. Finally, in the reference section, we mentioned all the referred research articles.

2.Literature review

In this section, we have summarized all the research articles that give a theoretical base for the research and help us determine the nature of our research. We studied the vulnerabilities of the radio network. The first jamming attack was reviewed. Jamming attacks are a kind of DoS attack. In this type of attack, hostile entities intentionally disrupt networks to prevent lawful communication. Jamming uses deliberate radio interference to disrupt wireless communications. It does so by overdoing the communicating medium, prompting the transmitter to wait when it detects a collision in wireless medium or a damaged signal received at the receivers. The physical layer is the most common target of jamming attacks, but cross-layer attacks are also conceivable in 5G [7–9]. The Deep Neural (DN) network can make radio networks like 5G highly vulnerable to adversaries raising severe security and robustness concerns [10].

Adversarial attacks or evasion attacks are caused by the vulnerability of 5G NR mmWave, that an attacker can create malicious inputs by minimally interrupting an original input. Hence, the deep learning system wrongly uses these inputs to classify input signals [10, 11]. These wrong classifications of signals are not "common white noise" but a distinct attribute in the feature space that leads to the incorrect model outputs [12–23].

Data poisoning attack is possible by predicting the behaviour of the transmitter and its attempt to misrepresent the spectrum-observing data and its spectrum. The adversary manipulates the data used for the transmitter's decision-making mechanism. It is done with the help of the adversary's transmission when the channel is idle. The transmitter node gathers data from spectrum sensors. Then, it feeds it into its

machine learning system. Meanwhile, the adversary develops a cognitive engine based on another DN network model. The DN model forecasts when the transmitter will be able to transmit successfully. The malicious node, then launches a data poison attack. The attack intends to trick the transmitter into sending erroneous data [24].

The attacker attacks by changing the channel occupancy status. The occupancy status of the channel is changed from idle to busy. When compared to data transmission jamming, this attack uses less energy and is harder to detect. The intrusion is effective and significantly decreases the transmitter's throughput [25–29].

Wireless signals are processed using machine learning algorithms to make informed decisions like authentication at the physical layer of the 5G NR mmWave network. Attackers can exploit wireless signal classifiers for creating a membership inference attack. Attackers modify the training data set of the machine learning model by changing device-level information, like data characteristics and channel information, like the environmental conditions.

The malicious nodes can utilise the stolen information to exploit the machine learning model's flaws via some malicious machine learning technique. The attackers use a membership inference attack against a deep learning-based classifier. The classifier receives the RF fingerprints signals based on device, channel characteristics and waveform. The attacker develops a surrogate classifier with the help of the spectrum information. After that, the attacker develops an inference model. The inference model is used to determine if the particular signal can be used in the training data on the receiver's side [30].

Trojan (backdoor or trapdoor) attacks, many applications in wireless communications. A deep learning classifier uses modulation and many features to categorise wireless signals. An adversary modifies the data used for training purposes. It adds a small number of trojans into training data samples. These modified training data can change phases of the actual training data set. Also, it can change the label of the training data set, resulting in a change of target label. The attack forces the deep learning classifier to train using the poisoned training data. As a result, the malicious or attacking node transmits signals with the same phase shift as that data inserted in the data set used for training.

It is easy for a receiver to classify a non-triggered or clean signal. But it cannot do the same for triggering signals. This malicious trigger makes the attack very difficult to detect and makes it near stealthy. This attack is effective across various channel conditions. It is not easy to avert such an attack by simply filtering the training data set or doing random phase fluctuations. Outlier detection mechanisms, based on activation, can be combined with clustering and statistical techniques to detect this attack. The clustering technique can detect the attacks despite a few samples being poisoned, and hence, it can detect trojan attacks [31].

Another type of attack that uses vulnerabilities of networks is jamming attacks. It works at the Media Access Control (MAC) layer. Jamming attacks have been investigated in various kinds of wireless networks. Researchers in [32–34] investigated the attacks 802.11 networks. Similarly, authors in [35–38] and [7–11], [24–39] have investigated the attacks in sensor networks, multi-hop networks, and other network models respectively.

Sadeghi and Larsson [40] have described how black-box adversarial attacks are carried out and their impact on the transmission system's block error rate. A study on deep learning-based power distribution and adversarial attacks was published by Manoj et al. [41]. Similarly, in Zhong et al. [42] and Wang et al. [43] published a detailed analysis of jamming attacks and their defence mechanisms.

Thus, various types of attacks are possible due to different vulnerabilities of the 5G NR mmWave network. As mentioned, a jamming attack uses the vulnerability at the physical layer or MAC layer to carry out attacks. The adversarial attacks use the vulnerabilities of deep learning systems. Similarly, a data poisoning attack happens when the attacker uses the vulnerabilities of the DN network model, which occurs at layer 3 of the network. Many attackers can modify the training data set of the network's machine learning model, causing a membership inference attack. In a trojan attack, the attacker adds a small number of trojans into training data samples forcing the deep learning classifier to train using the poisoned training data. Black box attacks, deep learning-based power distribution, and adversarial attacks can be carried out using the network's vulnerabilities. All these attacks work at different layers of the network Transmission Control Protocol/ Internet Protocol (TCP/IP) model, and researchers have shown that vulnerabilities exist in the architecture of 5G NR

mmWave. Vulnerabilities should be discovered, analyzed, and remedied before malevolent individuals or organizations exploit them.

The primary goal of this research is to contribute to the efforts made by scholars to find vulnerabilities in the 5G NR mmWave network and fill in the gaps left by them. To achieve the goal, we have studied and analysed the transport layer of the TCP/IP reference model of the 5G NR mmWave and found a severe vulnerability there. Attackers could exploit the vulnerability at the transport layer. Using that vulnerability, we carried the SYN Flood DoS attack and demonstrated its effects on popular MAC schedulers in the 5G NR mmWave network. We investigated the mentioned attack on a network using the proportional fair and round robin MAC schedulers.

To carry out the research, we created simulation test-bed frameworks with identical parameters except for attack nodes. The simulation framework 0 consists of a zero number of SYN flood attack nodes. Simulation framework 1 consists of one number of SYN flood attack nodes. Similarly, simulation framework 2, simulation framework 3 and simulation framework 4 consists of two, three and four attack nodes, respectively. Then, we experimented and evaluated each simulation framework with a proportional fair MAC scheduler and round-robin scheduler for performance measurement and network evaluation. We considered essential network metrics like throughputs, jitter, and delay for network performance evaluation for SYN flood attacks.

3.Methods

The primary 5G NR mmWave components are user equipment, evolved packet core, access point, router, wired node, wireless node and next-generation node B (gNB). These components work together for communication between user User Equipment (UE) and a wired node. We have used a network simulator called NetSim version 12.02 for the simulation purpose. The simulation software has various tools which help to simulate 5G NR mmWave technology. UE is one of the tools. UEs are the user equipment that people use to communicate with others. Mobile is an example of UE. We also have gNB. It is similar to that of eNB of LTE networks. It acts as an intermediary between UE and The Evolved Packet Core (EPC). The EPC connects the gNB with the New Generation (NG) core. An EPC consists of a Packet Gateway (PGW), Secure Web Gateway (SWG) and Mobility Management Entity (MME). *Figure 1* shows the flowchart of our research method to analyse the performance, vulnerability of the MAC scheduling algorithm due to the DoS attack in 5G.

As shown in *Figure 1*, designing and setting up the 5G NR mmWave module is the initial task. We designed and implemented the DoS attack, once we set up the module with the help of UEs, gNB and router. The DoS attack is a SYN flood attack.

A SYN flood attack is also known as a half-open assault. It's distributed DoS attack that uses all available server resources to render a server unavailable for genuine traffic. The attacker can overflow all unutilised ports on a targeted machine (server) by continuously sending initial connection request (SYN) packets. It causes the targeted device not to reply to any request or reply. Every UEs use the handshake step of a TCP connection for connection establishment.

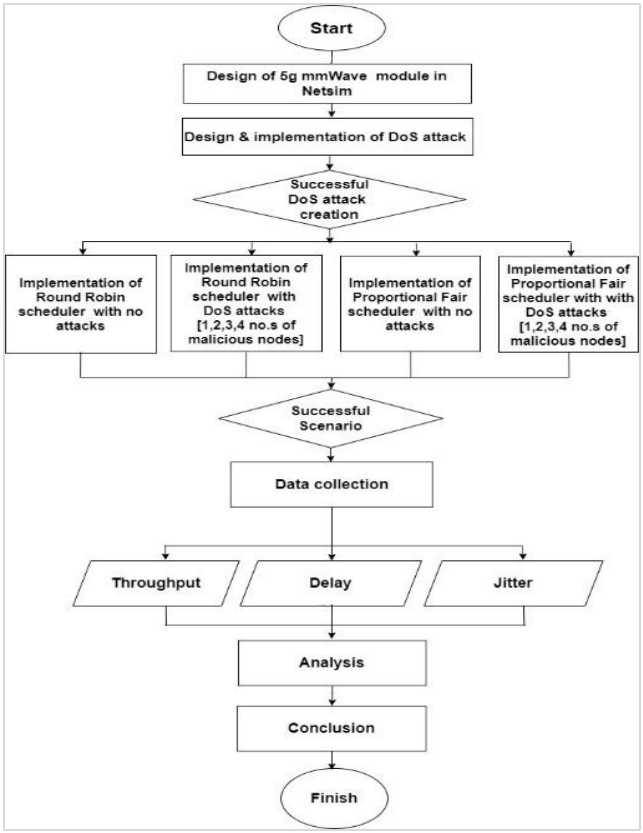

Figure 1 Flow chart of research method

A TCP connection goes through three distinct stages under normal circumstances to establish a connection, which is as follows:

1. In 5G NR mmWave, a UE first sends a special packet known as SYN packet to the wired node that acts as a server [*Figure 2*].
2. The wired node (server) acknowledges the communication by sending a packet of type SYN/Acknowledgement (ACK) in reply to the initial packet.
3. Finally, the wired node's (server) packet is acknowledged as the client sends an ACK packet. The TCP connection opens when an exchange of packets, as mentioned in steps 1 & 2, is done and gets in a position to receive and send more data [*Figure 2*].

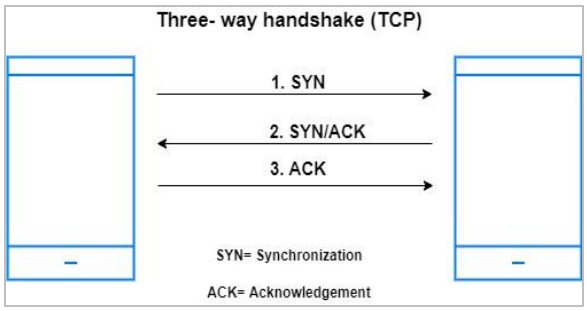

Figure 2 Three-way TCP handshake

The malicious UE needs to register itself with the gNB of the 5G NR mmWave to carry out intrusion in the network. The following steps were performed for malicious UEs' registration with the gNB.:

1. The malicious or attacking UE read and accepted the attachment data from the core network and sent back its attachment data/reply.
2. Then gNB sent packets for measurement of 5G NR Synchronisation Signal Blocks (SSBs), which include New Radio Physical Layer-Specific Signals (NRPSS) and New Radio Secondary Synchronisation Signals (NRSSS).
3. After reading the valid measurement report, gNB started the Radio Resource Control (RRC) reconfiguration process. It sent RRC_connection-reconfiguration_setup to the malicious UEs.
4. The malicious UEs, after receiving RRC_connection-reconfiguration_setup packet, sent their reply back to gNB.
5. Once the gNB received the reply, it sent back Addition_Request_acknowledge to the malicious UEs.
6. After receiving Addition_Request_acknowledge packet, the malicious UEs can send SYN packets to their target networks and drop all received SYN/ACK packets.

The steps mentioned above are required to exploit the vulnerability of 5G NR mmWave at the transport layer of the TCP/IP model. Without registering itself to the radio network, malicious UEs cannot participate in data exchange. So, our approach makes sure that the malicious UE appears normal and gets it registered with a gNB to carry out a SYN flood attack. The procedure shows that illegitimate UE can register itself in the 5G NR mmWave and carry out SYN flood attacks.

The algorithm for the registration of attacking UE with gNB and the SYN flood attack in 5G NR mmWave is as follows:

Proc_Core_Network
{// at the core network
Set Flag_s: =False;
    Send(*attachment_data*);
    WaitforEvent();
if (Flag_s: == False)
{
    if(*attachment_reply* & valid)
    Set Flag: = True;
}}

Proc_Attack_UE
{// at the malicious UE
WaitforEvent();
if (*attachment_data* & valid)
        Send (*attachment_reply*);
WaitforEvent();
if(*NRPSS* / *NRSSS* & valid)
        Send(*Measurement_Report*);
WaitforEvent();
if(*RRC_connection-reconfiguration_setup* & valid)
   Send(*RRC_connection-reconfiguration_Reply*);
WaitforEvent();
if(*Addition_Request_acknowledge*)
{
        while(1)
        {
        Send(*Spoofed_SYN*);
        if(*SYN/ACK*)
                Drop *SYN/ACK*;
}}}

Proc_gNB
{// at gNB
Set Flag: =False;
WaitforEvent();
if(Flag:== True)
        Send(*NRPSS*);Send(*NRSSS*);
WaitforEvent();

```
if(Measurement_Report & valid){
        Set Flag_s=True;
    Send(RRC_connection-reconfiguration_setup);}
WaitforEvent();
if(RRC_connection-reconfiguration_Reply){
        Set Flag_s: =True;
        Send(Addition_Request_acknowledge );
WaitforEvent();
Send_to_destination UE();
WaitforEvent();
if(SYN/ACK )
        Send_to_Source UE(SYN/ACK);
}}
```

We used the fact that after receiving an initial SYN packet, the machine (server) will react with few SYN/ACK packets and wait for the final step of the handshake procedure to produce denial-of-service. The functions are as under: [*Figure 3*]

1. We bombarded the targeted wired node (server) with many SYN packets, many of which had faked IP (logical) addresses.
2. The wired node (server) then answers each new connection request and opens a port to accept the response.
3. Malicious UEs continued to transmit SYN packets when the wired node (server) waited for the last acknowledgement packet. But it never arrives. With the help of the SYN packet, the UEs can utilise all the available ports in the wired node (server). Because of which the server becomes unable to do its function correctly.

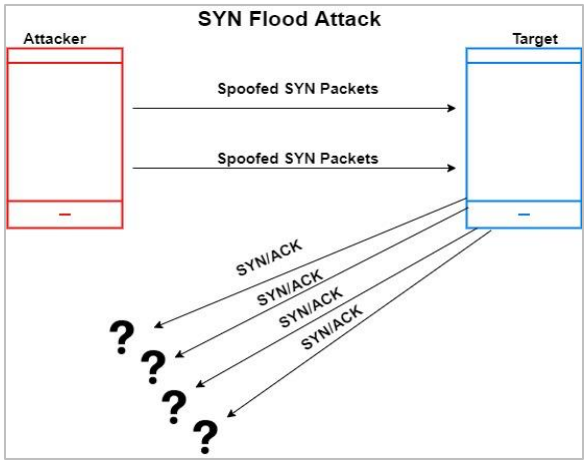

Figure 3 SYN flood attack in 5G NR mmWave

We used this approach with simulation because it helps to correctly predict the behaviour of all the components of 5G mmWave network. It helps to explore the pitfalls of the underlying protocols and examine its effect. Now, once the design and implementation are done, we implemented the following scenarios. The critical parameters of the creation of simulation test-bed are as follows:

Once we created the test-bed, we prepared simulation environment as shown in *Table 1*, *Table 2*, *Table 3* and *Table 4*. Note that in *Figure 4*, there are no attack nodes/UEs available. We first simulated the environment with zero attack nodes with round robin scheduler and proportional fair schedulers.

After we took the observation for no attack node, one SYN flood attack node was introduced. We took observations for the scenario with round robin and proportional fair algorithm, respectively.

Table 1 Application properties

Parameter	Value
Application method	Unicast
Application type	Constant Bit Rate (CBR)
Packet size	1460 Bytes & Constant
Inter arrival time	486 Micro. Sec. & Constant
Source ID	For App1 to App10, UE_7 to UE_16 respectively
Destination ID	Wired Node 4

One SYN flood attack node was introduced after taking observation for no attack node. We took observations for the scenario with round robin and proportional fair algorithm, respectively

Figure 5 shows the one attack-node simulation setup. Now, observations were recorded again and again for two, three and four attack nodes with round robin and proportional fair, respectively.

Figure 6 shows the simulation snapshot with four numbers of attack nodes. Due to space constraints, we didn't put the figure for simulation with two, three, and four attack nodes. *Figures 7*, 8 and 9 clearly indicate the collected observations for vital networking criteria like delay, throughput and jitter.

Table 2 Devices tools used for simulation

	Simulation framework 0	Simulation framework1	Simulation framework 2	Simulation framework 3	Simulation framework 4
No.s of UEs	10	10	10	10	10
No.s of gNBs	1	1	1	1	1
No.s of EPCs	1	1	1	1	1
No.s of routers	1	1	1	1	1
Malicious nodes	0	1	2	3	4

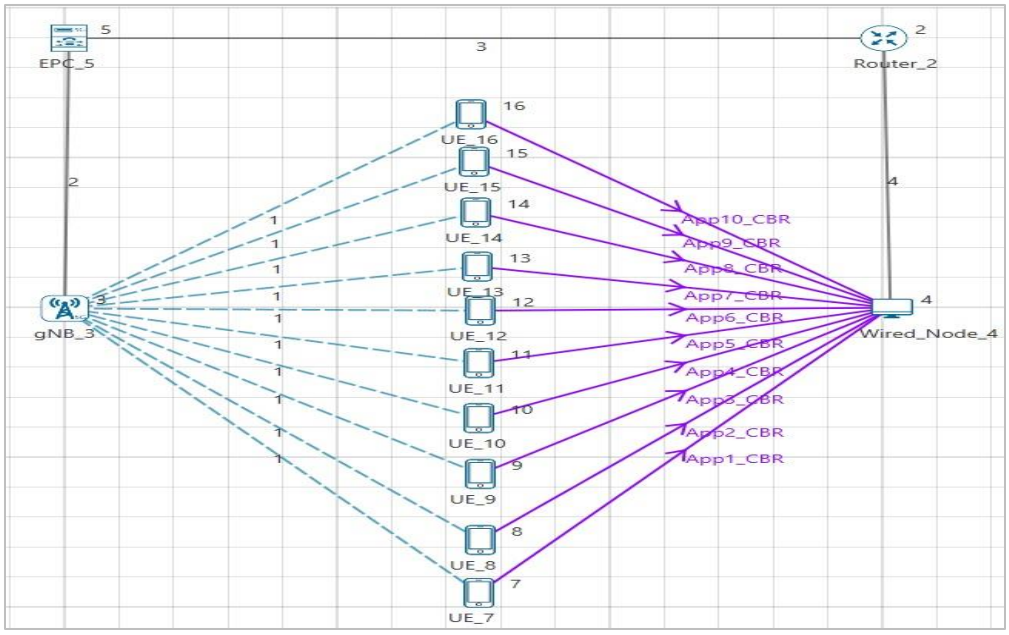

Figure 4 Simulation scenario with no attack node

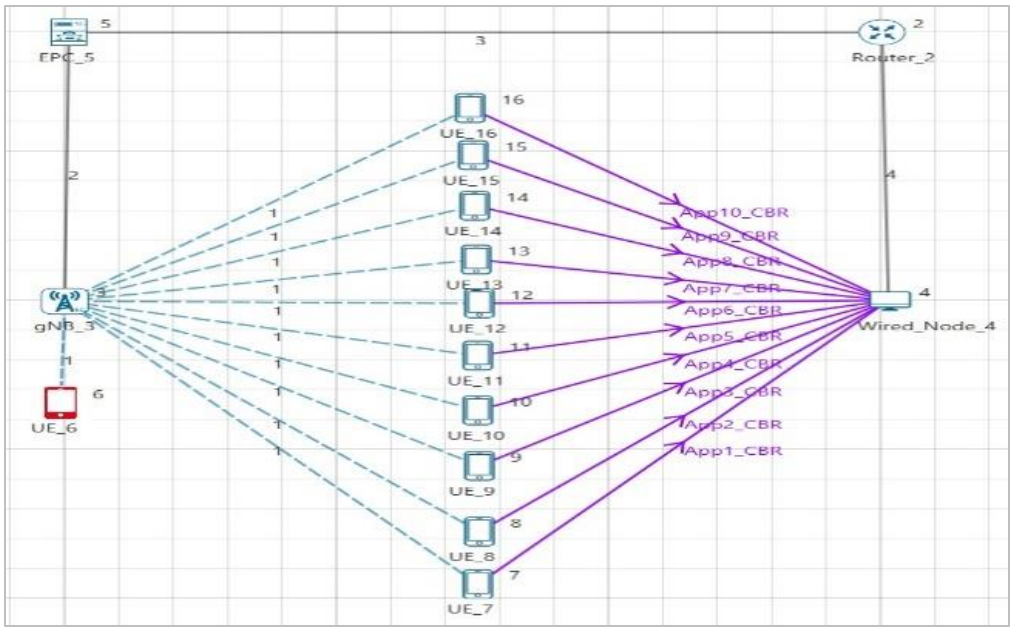

Figure 5 Simulation scenario with 1 attack node

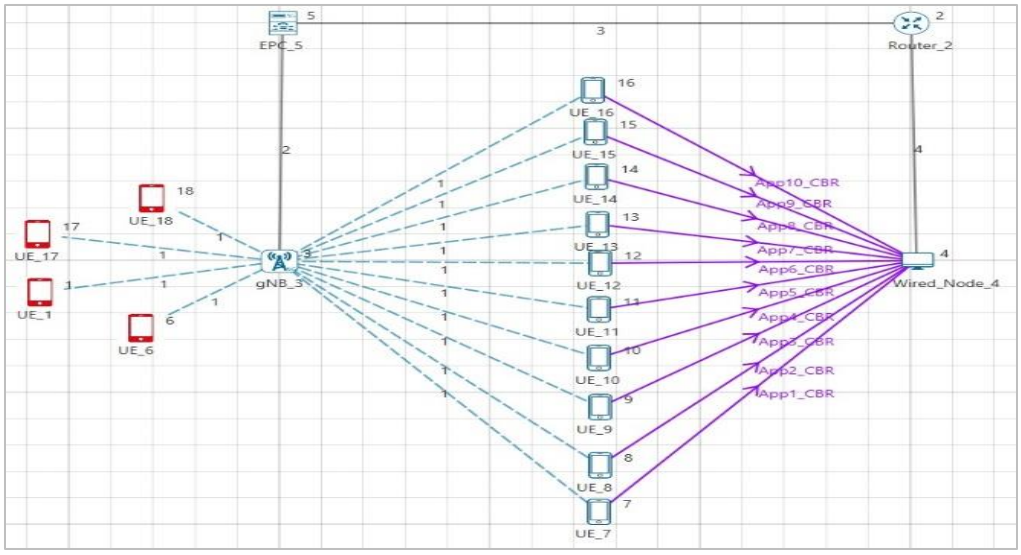

Figure 6 Simulation scenario with four attack nodes

Table 3 Wired link properties

Link Type	Speed
Down-link speed	5000 Mbps
Up-link Speed	5000 Mbps

Table 4 Scheduler properties

	Simulation framework 0	Simulation framework 1	Simulation framework 2	Simulation framework 3	Simulation framework 4
Scheduler	1. Round Robin				
	2. Proportional Fair				

Delay of the network is calculated using Equation 1.

$$\lambda_{nodal} = \lambda_{proc} + \lambda_{queue} + \lambda_{trans} + \lambda_{prop} \quad (1)$$

where

- λ_{nodal} = Nodal Delay
- λ_{proc} = Processing Delay
- λ_{prop} = Propagation Delay
- λ_{queue} = Queuing Delay
- λ_{trans} = Transmission Delay

Equation 2 is used to calculate the throughput of the network. Third Generation Partnership Project Technical Specification (3GPPTS) 38.306 standard is the basis of the calculation. For calculation of throughput, number of carriers mode of 5G network, frequency range, modulation type, number of MIMO layers, bandwidth etc., is essential.

$$data\ rate\ (in\ Mbps) = 10^{-6} \sum_{j=1}^{J} \left(V_{Layers}^{(j)} \cdot Q_m^{(j)} \cdot f^{(j)} \cdot R_{max} \cdot \frac{N_{PRB}^{BW(j),\mu} \cdot 12}{T_s^{\mu}} \cdot (1 - OH^{(f)}) \right) \quad (2)$$

Jitter is defined as the variation in the packet delay. Equation 3 and Equation 4 are the formulae used for the calculation of jitter.

Jitter for any packet = |End to end delay of current packet -End to end delay of the previous packet| (3)

Jitter for the entire application= Total packet jitter of all successful packets / (Total number of successfully received packets - 1) (4)

Overhead transmitted is calculated by adding all the overhead transmitted in each link of the network.

4. Results

After implementing the test-bed of the simulation, we used the proportional fair algorithm to determine the throughput with 0,1,2,3 and 4 attack nodes. As mentioned in *Table 2*, the simulation frameworks differ in the number of attack nodes. Simulation framework 0 contains zero attack nodes, and simulation framework 1 consist of one number of attack nodes. Simulation framework 2, 3 and 4 consists of 2, 3 and 4 numbers of malicious nodes, respectively. The network's average throughputs with proportional fair MAC scheduler under various attack nodes are shown in *Table 5*. Similarly, *Table 6* and

Table 7 shows the average jitter and the average delay for different simulation frameworks.

Table 5 Average throughput of the network for various simulation frameworks with proportional fair MAC Scheduler

	Simulation framework 0 / 0 Attack node	**Simulation framework 1 / 1 Attack node**	**Simulation framework 2 / 2 Attack node**	**Simulation framework 3 / 3 Attack node**	**Simulation framework 4 / 4 Attack node**
Average throughput (Mbps)	2.098312	2.049139	1.58521	1.467242	1.306992

Table 6 Average jitter of the network for various simulation frameworks with Proportional Fair MAC Scheduler

	Simulation framework 0 / 0 Attack node	**Simulation framework 1 / 1 Attack node**	**Simulation framework 2 / 2 Attack node**	**Simulation framework 3 / 3 Attack node**	**Simulation framework 4 / 4 Attack node**
Average jitter (Micro. Sec)	5231.707	5366.34	6884.995	7447.556	8379.415

Table 7 Average delay of the network for various simulation frameworks with proportional fair MAC Scheduler

	Simulation framework 0 / 0 Attack node	**Simulation framework 1 / 1 Attack node**	**Simulation framework 2 / 2 Attack node**	**Simulation framework 3 / 3 Attack node**	**Simulation framework 4 / 4 Attack node**
Average delays (Micro. Sec)	2142647	2175939	2180534	2234770	2240051

We have measured observations of throughputs, jitters and delays for the applications running in the UEs. *Figures 7, 8, & 9* depict the impact of the various SYN flood attack nodes on applications' throughput, jitter, and delay, respectively, compared to a zero-attack scenario. The *Figure 7, Figure 8 and Figure 9* show the comparisons of throughput, jitter and delay in various simulation frameworks.

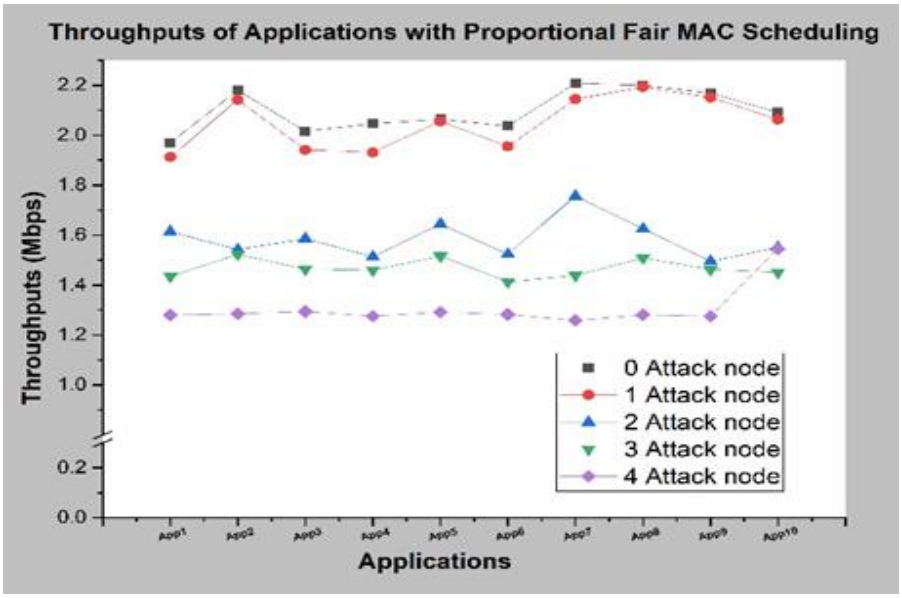

Figure 7 Throughputs of applications with proportional fair Scheduler (with attack nodes)

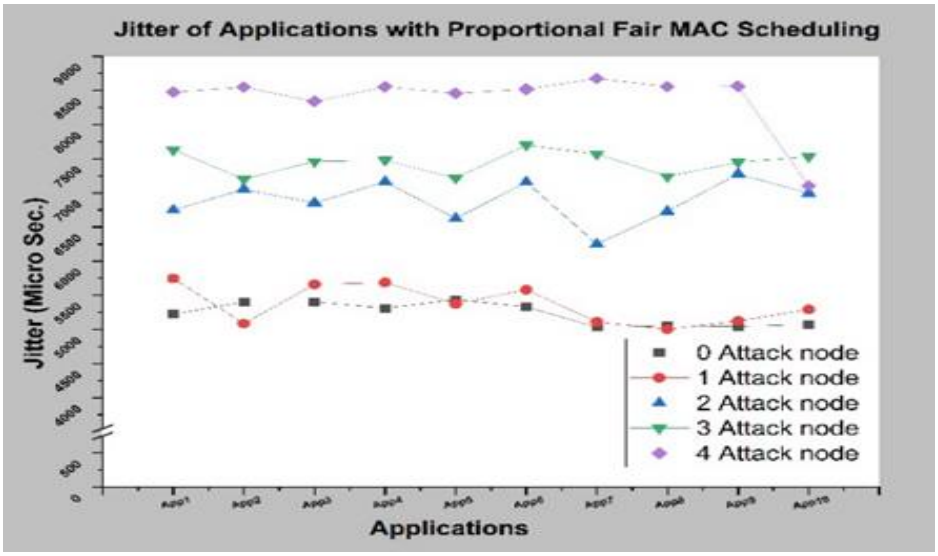

Figure 8 Jitter of applications with proportional fair Scheduler (with attack nodes)

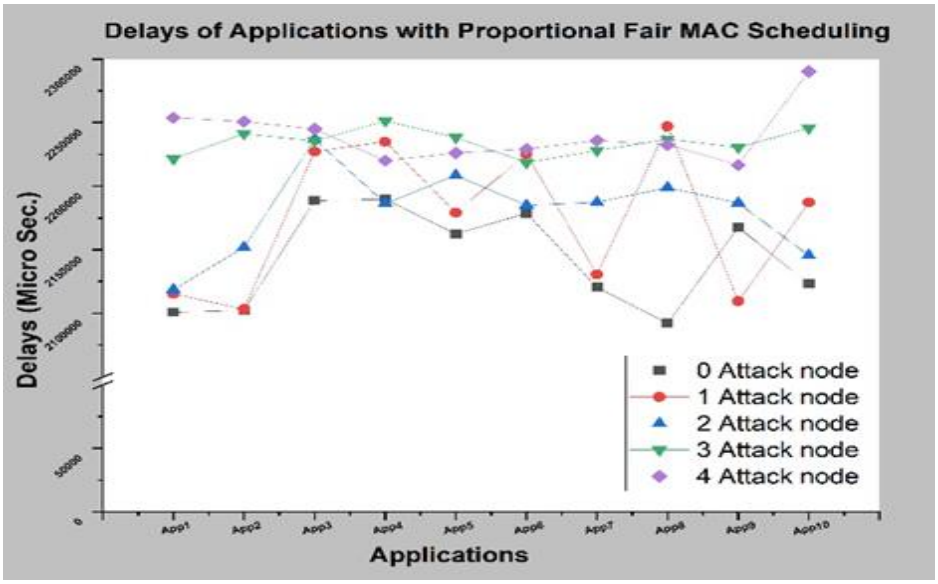

Figure 9 Delays of applications with proportional fair Scheduler (with attack nodes)

The same procedure for round robin scheduler for all the simulation frameworks were performed after recording all the required observations for proportional fair scheduler for all the simulation frameworks. *Table 8* shows the average throughput for various simulation frameworks with round robin MAC scheduler. *Table 9* and *Table 10* depict the jitter and the delay for various simulation frameworks with the round robin MAC Scheduler.

Table 8 Average throughput of the network for various simulation frameworks with round-robin MAC Scheduler

	Simulation framework 0 / 0 Attack node	**Simulation framework 1 / 1 Attack node**	**Simulation framework 2 / 2 Attack node**	**Simulation framework 3 / 3 Attack node**	**Simulation framework 4 / 4 Attack node**
Average throughput (Mbps)	2.098312	2.049139	1.618848	1.467242	1.309094

Table 9 Average jitter of the network for various simulation frameworks with round-robin MAC Scheduler

	Simulation framework 0 / 0 Attack node	Simulation framework 1 / 1 Attack node	Simulation framework 2 / 2 Attack node	Simulation framework 3 / 3 Attack node	Simulation framework 4 / 4 Attack node
Average jitter (Micro. Sec)	5199.707	5366.34	6740.653	7447.556	8333.227

Table 10 Average delay of the network for various simulation frameworks with round-robin MAC Scheduler

	Simulation framework 0 / 0 Attack node	Simulation framework 1 / 1 Attack node	Simulation framework 2 / 2 Attack node	Simulation framework 3 / 3 Attack node	Simulation framework 4 / 4 Attack node
Average delays (Micro. Sec)	2156647	2190939	2227517	2234770	2245411

Figure 10, *Figure 11* and *Figure 12* show the throughput, the jitter and the delay of the applications of UEs in simulation framework 0 (0 attack nodes), simulation framework 1 (1 attack nodes), simulation framework 2 (2 attack nodes), simulation framework 3 (3 attack nodes) and simulation framework 4 (4 attack nodes) for round robin MAC scheduler respectively. *Figure 13*, *Figure 14* and *Figure 15* show the average throughput, the average jitter and the average delay of the network for numbers of attack nodes for proportional fair MAC scheduler, respectively. Similarly, *Figure 16*, *Figure 17* and *Figure 18* show the average throughput, the average jitter and the average delay of the network for numbers of attack nodes for the round robin MAC scheduler.

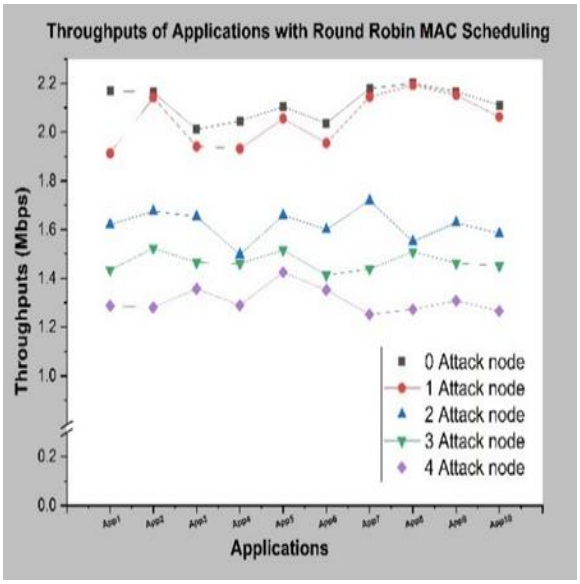

Figure 10 Throughput of applications with round robin scheduler (with attack nodes)

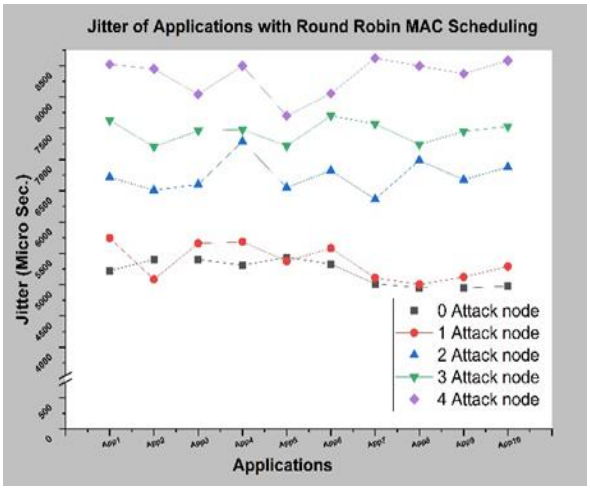

Figure 11 Jitters of applications with round robin scheduler (with attack nodes)

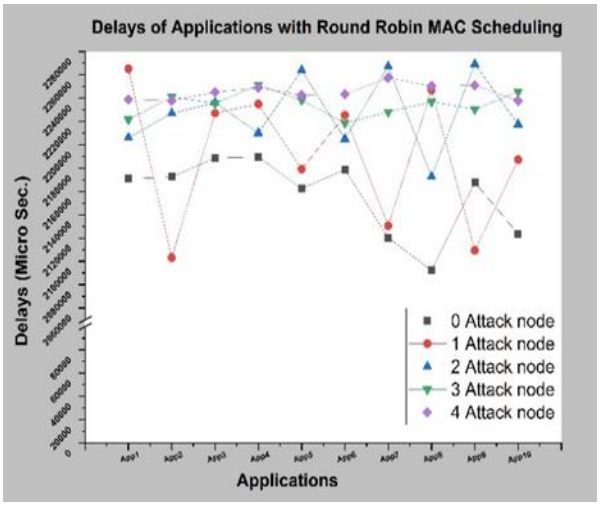

Figure 12 Delays of applications with round robin scheduler (with attack nodes)

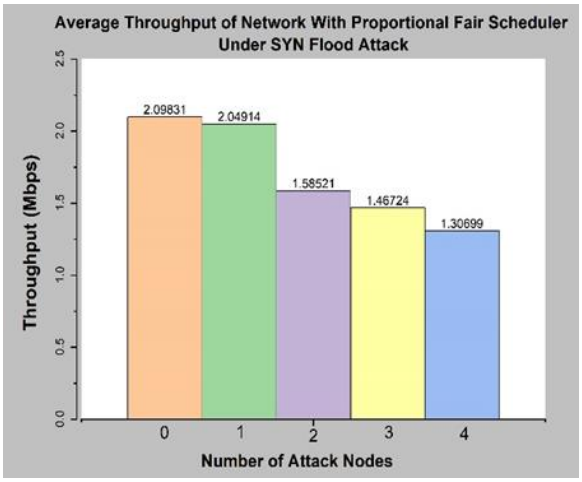

Figure 13 Average throughput of network with proportional fair scheduler (with attack nodes)

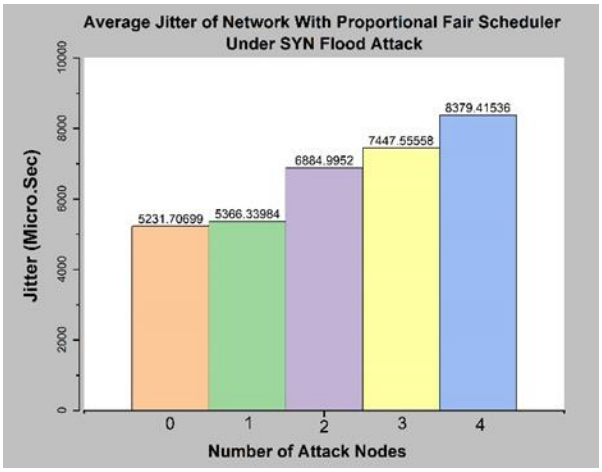

Figure 14 Average jitter of network with proportional fair scheduler (with attack nodes)

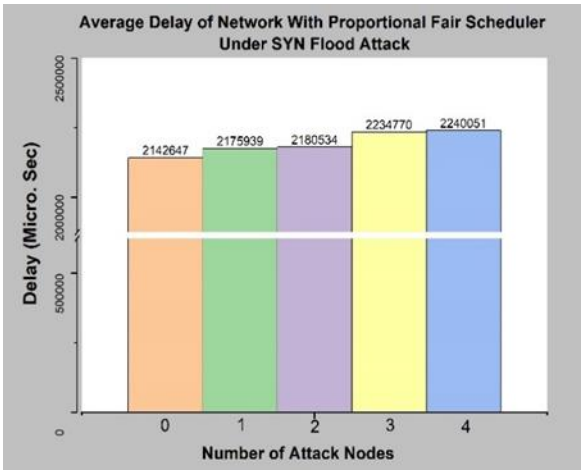

Figure 15 Average delay of Applications with proportional fair scheduler (with attack nodes)

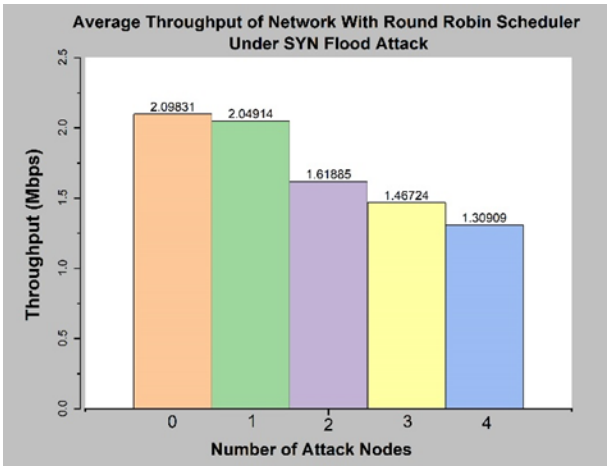

Figure 16 Average throughput of network with round robin scheduler (with attack nodes)

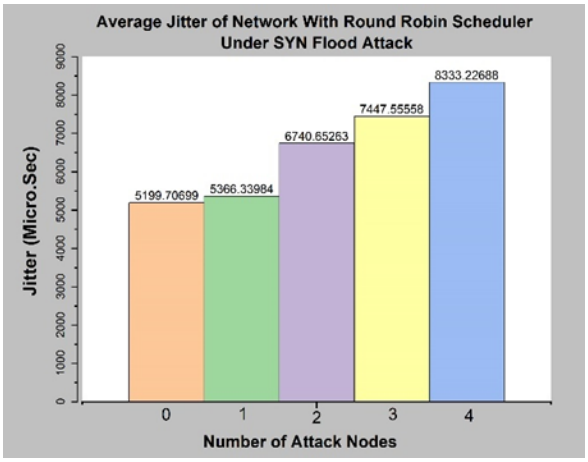

Figure 17 Average jitter of network with round robin scheduler (with attack nodes)

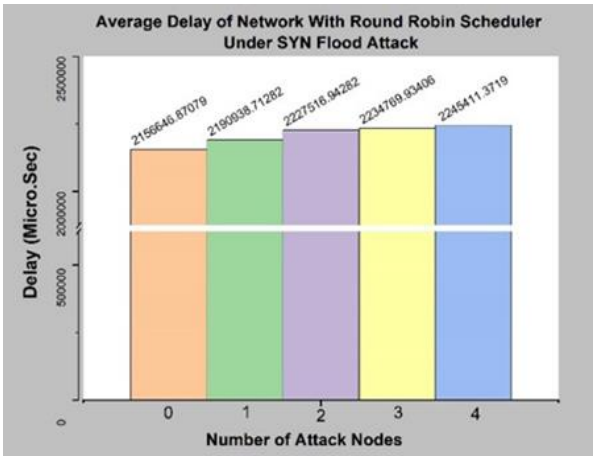

Figure 18 Average delay of network with round robin scheduler (with attack nodes)

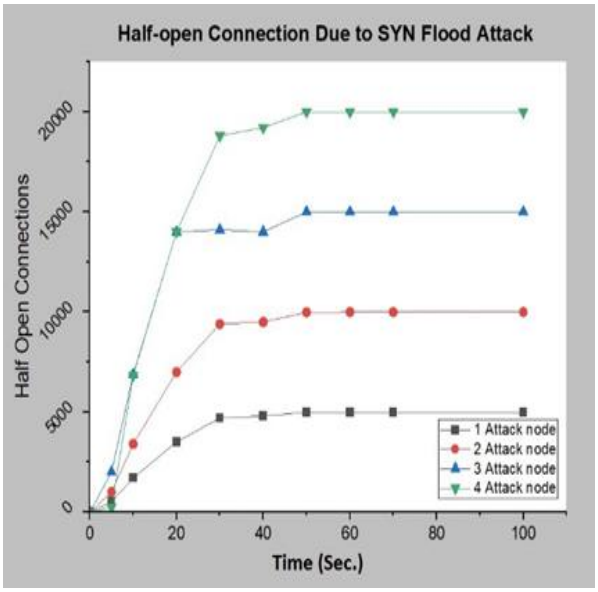

Figure 19 Number of half-open connection in attack scenarios

We also measure a few additional performance parameters. *Figure 19* shows the number of half-open connections created due to the SYN flood attack. *Figure 20* and *Figure 21* show the overhead transmitted in the network with proportional fair and round robin MAC scheduler.

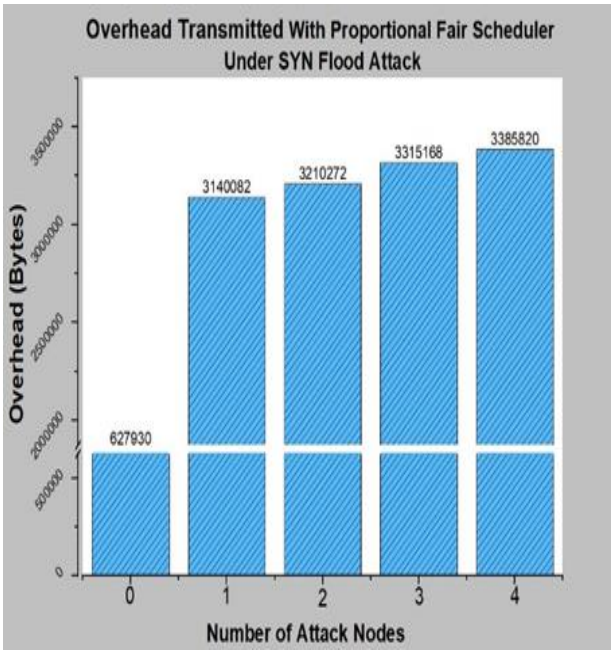

Figure 20 Overhead transmitted in the network with proportional fair scheduler (with attack nodes)

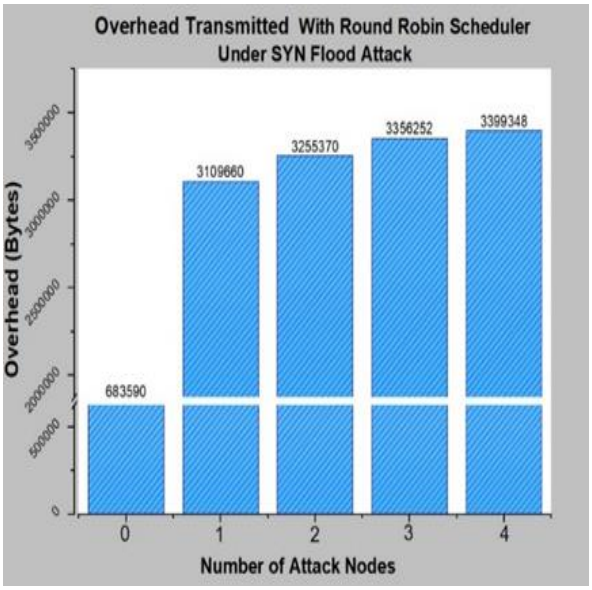

Figure 21 Overhead transmitted in the network with round robin scheduler (with attack nodes)

5. Discussions

Table 1 presents the application properties. The mentioned properties are identical for all five simulation frameworks. UE_7 to UE_16 are the genuine UEs. Each of the UEs has one constant bit rate (CBR) application running on it. App1, App2 etc., are the application running on the UEs.

Table 2 shows the devices or equipment used in the simulation. The devices are UEs, gNBs, EPC, routers and malicious nodes/UEs. We used the same set of devices in all the simulation frameworks except the malicious nodes/UEs. Different simulation frameworks use different numbers of attack nodes. Similarly, *Table 3* shows the downlink speed and uplink speed of the network. Table 4 shows that round robin and proportional fair schedulers are alternately used in different simulation frameworks.

Table 5 shows the average throughput of the network for various simulation frameworks with the proportional fair MAC scheduler. Each simulation framework consists of a different number of attack nodes. We can observe that the simulation framework 0 having no attack nodes has the maximum average throughput. The average throughput decreases as the number of attack nodes increases. That is, simulation framework 4, having four attack nodes, has the minimum average throughput.

Throughput significantly affects the QoS in the network. Higher throughput will increase the QoS. A reduction in throughput will affect the audio and video quality. Also, the reduced throughput will affect the performance of time-sensitive applications. For example, self-driving will not detect obstacles in real-time if throughput is lower than expected. SYN flood attack reduces the throughput of the network. This reduced throughput will result in the collision of self-driving cars.

Tables 6 and *Table 7* show the average jitter and network delay for various simulation frameworks with proportional fair MAC scheduler, respectively. The average jitters and delays have increased substantially due to the increasing attack nodes in simulation frameworks 0 to 4. *Figure 7* shows the throughputs of the applications with proportional fair MAC scheduling algorithms in various simulation frameworks. Simulation frameworks 0 contains no attack nodes. Similarly, simulation frameworks 1, simulation frameworks 2, simulation frameworks 3 and simulation frameworks 4 includes one, two, three and four number of attack nodes, respectively. Each simulation framework consists of 10 numbers of UEs, and each UEs has one application running on top of it. *Figure 7* elaborately shows the throughput of each application under different simulation frameworks. It is visible in the figure that application throughput deteriorates as the number of attack nodes increases. *Figure 8* and *Figure 9* depicts the jitter and delays of the applications with proportional fair MAC scheduling algorithms in various simulation frameworks. The jitter and delays are lowest in simulation frameworks 0. The jitter and delay keep on increasing noticeably from simulation frameworks 1 to simulation frameworks 4. In other words, jitter and delay increase as the number of attack nodes increases. *Table 8* shows the average throughput of the network for various simulation frameworks with round robin MAC scheduler. Each simulation framework consists of a different number of attack nodes. We can overserve that the simulation framework 0 having no attack nodes has the maximum average throughput. The average throughput decreases as the number of attack nodes increases. The simulation framework 0 has no attack nodes and maximum throughput, and simulation framework 4 has four attack nodes with the least average throughput. Jitter is a significant parameter for measuring network performance. It is the variation in time delay when a signal is transmitted and received over a network connection. The increased jitter will negatively impact the performance of the voice and video service. The attacking UEs flood the target network with SYN packets. The ports in the serving device will be overwhelmed by SYN packets creating half-open connections. The half-open connections increase the service time of requests by genuine UEs. Therefore, there will be variations in time delay. Because of this, the UEs in the network will not get the required QoS from the serving device. *Table 9* and *Table 10* show the average jitter and network delay for various simulation frameworks with a round robin MAC scheduler. We can observe that the attack nodes have adverse effects on the performance of the network. As the number of attack nodes increases, the average jitter and average delay also increase. *Figure 10, Figure 11* and *Figure 12* represent the effects of attack nodes on throughput, jitter and delay in various simulation frameworks with round robin MAC scheduler, respectively. Simulation frameworks 0 to 4 were decreasing throughput for the applications and increasing jitter and delay. The network's performance with round robin MAC scheduler deteriorates with the increase of attack nodes. Similarly, network delay also plays a vital role in maintaining QoS in the network. Increased network delay means increased waiting for requests made. Responses or replies from the service provider become useless if the responses or replies arrive lately. This is true for all time-sensitive applications. A SYN flood attack increases the delay in the network. It happens because the service provider is overwhelmed by incoming SYN packets. The SYN packets open a half-open connection resulting in many half-open connections due to numerous SYN packets. Thus, the service provider fails to cater for the requests made by the UEs immediately, resulting in an increased delay in the network and performance deterioration.

Figure 13 is the graphical representation of *Table 5*. It shows the average throughput of the network for various simulation frameworks with a proportional fair MAC scheduler. Similarly, *Figure 14* and *Figure 15* is the graphical representation of *Table 6* and *Table 7* respectively. It is visible from the figures that the attack nodes degrade the performance of the network. Both average jitter and average delay increase as the number of attack increases. In other words, the performance of the network decline from simulation framework 0 to simulation framework 4.

Similarly, *Figure 16, Figure 17* and *Figure 18* are the graphical representation of *Table 8, Table 9* and *Table 10*, respectively. As expected, average throughput is maximum when there is no attack. But the average throughput drops with the increase of attack nodes. Hence, simulation framework 4, having 4 number of

attack nodes, has the least average throughput. The average jitter and the average delay of the network were also affected by the attack nodes. The attack nodes increased the average jitter and the average delay. Because of this, simulation framework 0 has the minimum average jitter and average delay. Simulation framework 4 has the maximum average jitter and the average delay as anticipated.

The SYN flood attack has a devastating effect on the overhead transmission of packets. The attack has increased the traffic volume considerably because of which overall traffic volume has increased. *Figure 20* and *Figure 21* show the comparisons of overhead transmission due to attack nodes in the network with proportional fair and round robin MAC scheduler, respectively. *Table 11* compares the SYN flood attack with various types of attacks [44] in the 5G network in terms of percentage traffic volume. 3.091 percent of total network traffic is overhead traffic when there is no intrusion with proportional fair MAC scheduler. Similarly, 3.024 percent of total network traffic is overhead traffic when there is no intrusion with the round robin MAC schedule. We observe that traffic created by the SYN flood attack is more significant in volume than most mentioned attacks. Complete list of abbreviations is shown in *Appendix I.*

Table 11 Comparison of SYN flood attack with various types of attacks in terms of percentage traffic volume

S. No.	Attack type	Percentage of traffic volume
1	SYN flood attacks with proportional fair MAC scheduler	6.703 %
2	SYN flood attacks with round robin MAC scheduler	6.756 %
3	Infiltration attacks	5.892 %
4	Slowloris DoS attacks	0.340 %
5	GoldenEye DoS attacks	1.510 %
6	SQL injection attacks	0.003 %
7	BruteForce-XSS attacks	0.008 %
8	BruteForce-web attacks	0.022 %
9	SlowHTTPTest DoS attacks	5.090 %

The critical assessments from the study are as follows:

1. There are vulnerabilities in a 5G NR mmWave network that can be exploited. We exploited one such vulnerability to create a SYN flood attack. The 5G NR mmWave network is vulnerable because it keeps the connection open when a SYN packet arrives at UEs. Bombardment of SYN packets to any UEs will create numerous connections open without actually sending any data. Thus, the attack will overwhelm the resources to deprive genuine connection of services.
2. The throughput of the applications running on UEs, with either proportional fair MAC scheduling or round robin MAC scheduling, is negatively affected. The throughput of the applications decreases as the number of attack nodes increases.
3. The jitter and the delay of applications are adversely affected by the SYN flood attack. The severe SYN flood attack causes an increase in the jitter and the delay of applications.
4. The average throughput of the network decreases as a result of the SYN flood attack. If the application running on UEs is an audio call, the clarity may get affected, or the call may drop.
5. The average jitter and average delay of the network increase because of the SYN flood attack. As a result, the quality of service deteriorates. If the application running on UEs is media content, the user may face a media buffering problem.

Limitations:

There are a few limitations of our study. The following aspects may constrain the performance of the attacking UEs or nodes:

1. The attacking UE can easily deteriorate the network's performance. But, if the attacking node wants to attack any particular UE, it must be aware of the target node's network. Therefore, the attacking node must be mindful of the neighbourhood of the target UE.
2. Continuous sending packets (SYN) cause high battery power consumption. Thus, the attack's longevity depends on the power source (battery) of the attacking UE.

6. Conclusion and future work

This document demonstrated the implementation of a specific type of DoS attack known as a SYN flood attack in 5G NR mmWave. The attack takes advantage of a 5G NR mmWave vulnerability to exhaust the resources and deny authentic nodes/UEs access to network services. A study on the impact of the SYN flood attack on the performance of MAC scheduling algorithms such as round robin and proportional fair is presented. The network's performance has worsened

using either the round robin MAC scheduler or the proportional fair MAC scheduler. In scenarios with both round robin and proportional fair MAC schedulers, we observed that adding one to four SYN flood attack nodes decreased the average network throughput by 2.34 per cent to 37.7 per cent. The insertion of one to four SYN flood attack nodes in scenarios with both round robin and proportional fair MAC schedulers increased average network delays by 1.55 to 4.5 per cent and average jitter by 2.57 per cent to nearly 60 per cent. In the future, we will investigate the network's performance with other MAC schedulers under the SYN flood attack. We also intend to develop a machine-learning-based intrusion detection system to detect SYN flood attacks in the 5G NR mmWave network with large numbers of UEs.

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Tu GH, Li CY, Peng C, Li Y, Lu S. New security threats caused by IMS-based SMS service in 4G LTE networks. In proceedings of the ACM SIGSAC conference on computer and communications security 2016 (pp. 1118-30).
[2] Tu GH, Li CY, Peng C, Lu S. How voice call technology poses security threats in 4g LTE networks. In conference on communications and network security 2015 (pp. 442-50). IEEE.
[3] Tu GH, Li Y, Peng C, Li CY, Raza MT, Tseng HY, et al. New threats to SMS-assisted mobile internet services from 4G LTE: lessons learnt from distributed mobile-initiated attacks towards facebook and other services. arXiv preprint arXiv:1510.08531. 2015.
[4] Bhattarai S, Wei S, Rook S, Yu W, Erbacher RF, Cam H. On simulation studies of jamming threats against LTE networks. In international conference on computing, networking and communications 2015 (pp. 99-103). IEEE.
[5] Li W, Wang N, Jiao L, Zeng K. Physical layer spoofing attack detection in MmWave massive MIMO 5G networks. IEEE Access. 2021; 9:60419-32.
[6] Sánchez JD, Urquiza-aguiar L, Paredes MC, Osorio DP. Survey on physical layer security for 5G wireless networks. Annals of Telecommunications. 2021; 76(3):155-74.
[7] Grover K, Lim A, Yang Q. Jamming and anti–jamming techniques in wireless networks: a survey. International Journal of Ad Hoc and Ubiquitous Computing. 2014; 17(4):197-215.
[8] Shi Y, Sagduyu YE, Erpek T, Davaslioglu K, Lu Z, Li JH. Adversarial deep learning for cognitive radio security: jamming attack and defense strategies. In international conference on communications workshops 2018(pp. 1-6). IEEE.
[9] Erpek T, Sagduyu YE, Shi Y. Deep learning for launching and mitigating wireless jamming attacks. IEEE Transactions on Cognitive Communications and Networking. 2018; 5(1):2-14.
[10] Szegedy C, Zaremba W, Sutskever I, Bruna J, Erhan D, Goodfellow I, et al. Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199. 2013.
[11] Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. 2014.
[12] Sadeghi M, Larsson EG. Adversarial attacks on deep-learning based radio signal classification. IEEE Wireless Communications Letters. 2018; 8(1):213-6.
[13] Kokalj-filipovic S, Miller R, Morman J. Targeted adversarial examples against RF deep classifiers. In proceedings of the ACM workshop on wireless security and machine learning 2019 (pp. 6-11).
[14] Kokalj-filipovic S, Miller R, Vanhoy G. Adversarial examples in RF deep learning: Detection and physical robustness. In global conference on signal and information processing 2019 (pp. 1-5). IEEE.
[15] Flowers B, Buehrer RM, Headley WC. Evaluating adversarial evasion attacks in the context of wireless communications. IEEE Transactions on Information Forensics and Security. 2019; 15:1102-13.
[16] Lin Y, Zhao H, Tu Y, Mao S, Dou Z. Threats of adversarial attacks in DNN-based modulation recognition. In INFOCOM conference on computer communications 2020 (pp. 2469-78). IEEE.
[17] Kim B, Sagduyu YE, Davaslioglu K, Erpek T, Ulukus S. Over-the-air adversarial attacks on deep learning based modulation classifier over wireless channels. In annual conference on information sciences and systems 2020 (pp. 1-6). IEEE.
[18] Kim B, Sagduyu YE, Davaslioglu K, Erpek T, Ulukus S. Channel-aware adversarial attacks against deep learning-based wireless signal classifiers. arXiv preprint arXiv:2005.05321. 2020.
[19] Hameed MZ, György A, Gündüz D. Communication without interception: defense against modulation detection. In global conference on signal and information processing 2019 (pp. 1-5). IEEE.
[20] Hameed MZ, György A, Gündüz D. The best defense is a good offense: adversarial attacks to avoid modulation detection. IEEE Transactions on Information Forensics and Security. 2020; 16:1074-87.
[21] Kim B, Sagduyu YE, Davaslioglu K, Erpek T, Ulukus S. How to make 5G communications" invisible": adversarial machine learning for wireless privacy. In Asilomar conference on signals, systems, and computers 2020 (pp. 763-7). IEEE.
[22] Kim B, Sagduyu YE, Erpek T, Davaslioglu K, Ulukus S. Adversarial attacks with multiple antennas against deep learning-based modulation classifiers. In globecom workshops 2020 (pp. 1-6). IEEE.
[23] Kim B, Sagduyu YE, Erpek T, Davaslioglu K, Ulukus S. Channel effects on surrogate models of adversarial attacks against wireless signal classifiers. In ICC

international conference on communications 2021 (pp. 1-6). IEEE.
[24] Sagduyu YE, Shi Y, Erpek T. IoT network security from the perspective of adversarial deep learning. In annual international conference on sensing, communication, and networking 2019 (pp. 1-9). IEEE.
[25] Adesina D, Hsieh CC, Sagduyu YE, Qian L. Adversarial machine learning in wireless communications using RF data: a review. arXiv preprint arXiv:2012.14392. 2020.
[26] Shi Y, Erpek T, Sagduyu YE, Li JH. Spectrum data poisoning with adversarial deep learning. In MILCOM military communications conference 2018(pp. 407-12). IEEE.
[27] Sagduyu Y, Shi Y, Erpek T. Adversarial deep learning for over-the-air spectrum poisoning attacks. IEEE Transactions on Mobile Computing. 2019; 20(2):306-19.
[28] Luo Z, Zhao S, Lu Z, Xu J, Sagduyu Y. When attackers meet AI: learning-empowered attacks in cooperative spectrum sensing. IEEE Transactions on Mobile Computing. 2020.
[29] Luo Z, Zhao S, Lu Z, Sagduyu YE, Xu J. Adversarial machine learning based partial-model attack in IoT. In proceedings of the ACM workshop on wireless security and machine learning 2020 (pp. 13-8).
[30] Shi Y, Davaslioglu K, Sagduyu YE. Over-the-air membership inference attacks as privacy threats for deep learning-based wireless signal classifiers. In proceedings of the ACM workshop on wireless security and machine learning 2020 (pp. 61-6).
[31] Davaslioglu K, Sagduyu YE. Trojan attacks on wireless signal classification with adversarial machine learning. In international symposium on dynamic spectrum access networks 2019 (pp. 1-6). IEEE.
[32] Gupta V, Krishnamurthy S, Faloutsos M. Denial of service attacks at the MAC layer in wireless ad hoc networks. In MILCOM 2002(pp. 1118-23). IEEE.
[33] Kyasanur P, Vaidya NH. Detection and handling of MAC layer misbehavior in wireless networks. In DSN 2003 (pp. 173-82).
[34] Bayraktaroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B. Performance of IEEE 802.11 under jamming. Mobile Networks and Applications. 2013; 18(5):678-96.
[35] Li M, Koutsopoulos I, Poovendran R. Optimal jamming attacks and network defense policies in wireless sensor networks. In INFOCOM international conference on computer communications 2007 (pp. 1307-15). IEEE.
[36] Xu W, Trappe W, Zhang Y, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. In proceedings of the ACM international symposium on mobile ad hoc networking and computing 2005 (pp. 46-57).
[37] Zander J. Jamming in slotted ALOHA multihop packet radio networks. IEEE Transactions on Communications. 1991; 39(10):1525-31.
[38] Theodorakopoulos G, Baras JS. Game theoretic modeling of malicious users in collaborative networks. IEEE Journal on Selected Areas in Communications. 2008; 26(7):1317-27.
[39] Sagduyu YE, Berry RA, Ephremides A. Jamming games in wireless networks with incomplete information. IEEE Communications Magazine. 2011; 49(8):112-8.
[40] Sadeghi M, Larsson EG. Physical adversarial attacks against end-to-end autoencoder communication systems. IEEE Communications Letters. 2019; 23(5):847-50.
[41] Manoj BR, Sadeghi M, Larsson EG. Adversarial attacks on deep learning based power allocation in a massive mimo network. arXiv preprint arXiv:2101.12090. 2021.
[42] Zhong C, Wang F, Gursoy MC, Velipasalar S. Adversarial jamming attacks on deep reinforcement learning based dynamic multichannel access. In wireless communications and networking conference 2020 (pp. 1-6). IEEE.
[43] Wang F, Zhong C, Gursoy MC, Velipasalar S. Defense strategies against adversarial jamming attacks via deep reinforcement learning. In annual conference on information sciences and systems 2020 (pp. 1-6). IEEE.
[44] Lam J, Abbas R. Machine learning based anomaly detection for 5g networks. arXiv preprint arXiv:2003.03474. 2020.

Bhargabjyoti Saikia has completed his B.Tech in ECE from the Biju Patnaik University of Technology, Odisha, in 2009 and his M. Tech degree in IT NERIST, Arunachal Pradesh, in 2012. He achieved his Ph.D degree in wireless communication from ECE, NEHU, Meghalaya, in 2020. His research interests are in Wireless Communication and Information Theory. Currently, he is working as a senior assistant professor at the Department of ECE, DUIET, Dibrugarh University.
Email: bhargab.2008@gmail.com

Sudipta Majumder completed his B.Tech in CSE NERIST in 2009. He has done his M.Tech degree in IT and PhD degree in Network Security from the Department of Electronics and Communication Engineering. His research interest is Peer to Peer Networks, Wireless Networks and Network Security. Currently, he is working as a senior assistant professor at CSE department, DUIET, Dibrugarh University. He is also a life member of the Computer Society of India (CSI).
Email: sudipta2020@dibru.ac.in

Appendix I

S.No.	Abbreviation	Description
1	3G	Third-Generation
2	4G	Fourth-Generation Mobile Network
3	5G	Fifth Generation Mobile Network
4	5G NR mmWave	Fifth-Generation New Radio Millimeter Wave
5	3GPPTS	Third Generation Partnership Project Technical Specification
6	ACK	Acknowledgement
7	CBR	Constant Bit Rate
8	DL	Deep Learning
9	DN	Deep Neural
10	DoS	Denial of Service
11	EPC	Evolved Packet Core
13	Gbps	Gigabits per second
14	gNB	Next-generation Node B
15	LTE	Long Term Evolution
16	MAC	Media Access Control
17	Mbps	Megabits per second
18	MME	Mobility Management Entity
19	NG	New Generation
20	NR	New Radio
21	NRPSS	New Radio Physical Layer-Specific
22	NRSSS	New Radio Secondary Synchronisation Signals
23	PGW	Packet Gateway
24	QoS	Quality of Service
25	RRC	Radio Resource Control
26	SMS	Short Message Service
27	SSBs	Synchronisation Signal Blocks
28	SYN	Synchronize
29	SWG	Secure Web Gateway
30	TCP/IP	Transmission Control Protocol/ Internet Protocol
31	UE	User Equipment
32	V2I	Vehicle-to-Infrastructure
33	V2V	Vehicle-to-Vehicle