Machine Learning Algorithms for 5G Networks Security and the Corresponding Testing Environment

Maksim Iavich[1], Giorgi Iashvili[1], Zhadyra Avkurova[2], Serhii Dorozhynskyi[3], and Andriy Fesenko[4]

[1] *Caucasus University, 1 P. Saakadze str., Tbilisi, 0102, Georgia*
[2] *L.N. Gumilyov Eurasian National University, 2 Satbayev str., Nur-Sultan, 010000, Kazakhstan*
[3] *National Aviation University, 1 Liubomyr Huzar ave, Kyiv, 03058, Ukraine*
[4] *Taras Shevchenko National University of Kyiv, 24 Bohdan Havrylyshyn str., Kyiv, 04116, Ukraine*

Abstract

Wireless networks have been a part of our lives for many years now, they send huge amounts of data every day, and this volume is constantly growing, depending on a number of factors. One of the most important of these is the unprecedented growth of mobile devices and their multimedia applications. Which will automatically be followed by music and video streaming, social networking, video conferencing and more. The telecommunications industry is undergoing a major transformation towards 5G networks to meet existing and expected requirements. As it meets new customer requirements, in particular improved QoS and secure data transfer guarantee, which in turn ensures communication stability and security. The provision of basic services provided by 5G requires new technologies of data storage and processing. With the introduction of these technologies, we will face challenges related to new 5G cybersecurity systems and their operation. Researchers from around the world are involved in the 5G security assessment process. The reviewed materials show that 5G still has security issues. As part of our analysis, we also identified many security issues. Notably, in a 5G security study, the researchers identified weaknesses in the system that allow malicious code to be integrated into the system, Therefore, it is necessary to determine new architectures for 5G and next generation 6G networks in order to set new AI / ML based techniques, that should provide high security level. Even in the absence of a 5G network, it is necessary to check the design of the security function of 5G cellular networks. For this purpose, the paper proposes to test 5G security systems using a simulated 5G library before testing in a real 5G hardware in the lab. Attack datasets are required to validate the system. Below is depicted a design methodology for a modeled 5G lab using 4G sim card raspberry PI modems and a server. Smart IDS (Intrusion Detection System) test results are reviewed. The tests were carried out in the proposed analog laboratory.

Keywords

Cybersecurity, 5G networks, 5G security, QoS, machine learning, IDS.

1. Introduction

The volume of traffic transmitted over Wireless networks is constantly growing, depending on a number of factors. One of the most important of these is the unprecedented growth of mobile devices and their multimedia applications. The telecommunications industry is being transformed towards 5G networks to meet existing and expected requirements. Therefore, the concept of 5G wireless networks is to provide very high data transmission and higher coverage with close proximity of high bandwidth stations. Which results in a much higher quality of service (QoS) and very low latency. The provision of basic services provided by 5G requires new technologies of data storage and processing, definition

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: miavich@cu.edu.ge (M. Iavich); giiashvili@cu.edu.ge (G. Iashvili); zhadyra.avkurova.83@mail.ru (Zh. Avkurova); dorozhun1706@gmail.com (S. Dorozhynskyi); aafesenko88@gmail.com (A. Fesenko)
ORCID: 0000-0002-3109-7971 (M. Iavich); 0000-0002-1855-2669 (G. Iashvili); 0000-0002-0706-6075 (Zh. Avkurova); 0000-0003-0762-5685 (S. Dorozhynskyi); 0000-0001-5154-5324 (A. Fesenko)

of new network architecture and service implementation models. With the introduction of these technologies, we will face challenges related to new 5G cybersecurity systems and their operation.

All critical infrastructure will soon depend on 5G networks, so it is important to create a flawless security system in order to ensure maximum security of the related infrastructure and complete community safety. For example, failures of security in online power systems can be devastating for all the electronic systems on which society depends. Thus, to ensure the security of 5G networks, it is necessary to study and highlight the main problems, as well as analyze potential solutions that can lead to the creation of secure 5G systems. Researchers around the world are actively working on the security of 5G systems. It is also important to compare the security of 4G and 5G systems and analyze their differences [1,2].

Most of the new advances are followed by new challenges, and the same is expected for 5G communications. In addition, 5G is not immune to attacks that have existed during the existence of the Internet. DoS, DDoS, spoofing, application layer attacks, and man-in-the-middle attacks.

2. Overview of 5G Standard Security Issues

The reviewed materials show that 5G still has security issues. As part of our analysis, we also identified many security issues, namely:

1. The 5G network is highly vulnerable to software attacks and has a much larger penetration point, since 5G networks are mainly based on their own logical architecture software configurations. The attack takes place using various security vulnerabilities and bugs that can affect the operation of the 5G network.

2. As 5G networks have much more functionality and increased capabilities, the ability to detect vulnerabilities has also increased, so network equipment, base stations and key network management features can be targeted by hackers.

3. Mobile operators are completely dependent on suppliers, in the case of 5G, this in itself could lead to the emergence of new attack routes.

4. 5G networks will soon be used by almost all IT applications, so attacks on their availability and integrity can cause serious problems.

5. The 5G network will include many devices that can cause various types of attacks, like DoS and DDoS.

6. Network fragmentation can also lead to security problems as attackers may try to force some device to use a segment of the network that was not specifically designed for that it.

Vulnerability in 5G security systems has also been identified, which allows malicious code to be entered into the system and consequently to carry out illegitimate actions.

Therefore, it is necessary to determine new architectures for 5G and next generation 6G networks in order to set new AI / ML based techniques, that should provide high security level and provide adequate protection for mobile subscribers, industry, government.

The researchers proposed to prepare the IDS system using machine learning algorithms. After preparing the IDS, you need to examine it for attacks. Of course, testing this feature in the absence of 5G stations is a daunting task [3-6]. We suggest testing 5G security systems with a simulated 5G lab preparatory to testing real hardware in the lab. A personal attack data set is required to test the system. Researchers suggest using the "NSL KDD" to prepare IDS. In previous works, we suggested using the CICDDoS2019 databases when training IDS. The IDS prepared by them allows to determine the number of attacks on 5G networks. For IDS verification, we offer a laboratory trained using the NSL KDD and CICDDoS2019 data set. During testing, attack samples should be of a similar format.

In the course of our study we had to perform some tests as collect attacks, train and test IDS, so we built a lab, which consists of:

2-layer switch providing the connection between the hosts, 2 access points to test and check whether the IDS module can detect fraud, attacker host, defender server with IPS module, 60 Raspberry PIs to perform attacks and 60 4G SIM card modems [7,8].

The Fig. 1 shows laboratory model:

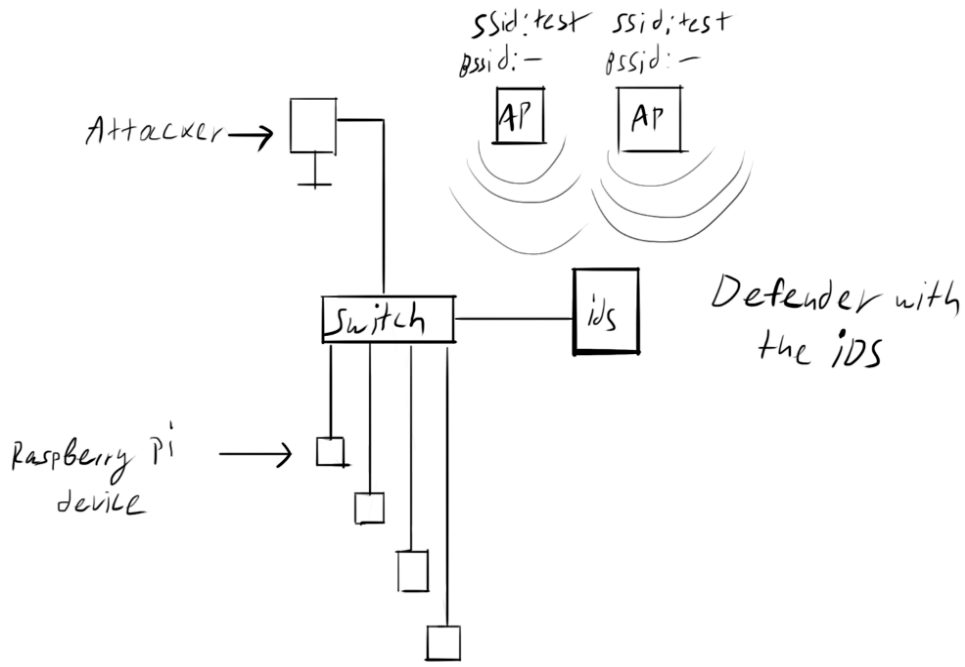

Figure 1: The simplified model of laboratory

Traffic that we receive in “pcap” format is converted to "NSL KDD" and "CICDDoS2019" formats, since IDS can not process this format. To perform conversation this, we use online tools. for this purpose, we suggest to use “Zeek” (also known as “Bro”) IDS along with https://github.com/inigoperona/tcpdump2gureKDDCup99 To convert ‘pcap’ to ‘CICDDoS2019’ format we use the ‘CICFlowMeter’ tool.

In the research process, we used “Oracle VirtualBox,” two virtual “Parrot OS” and two virtual “Ubuntu 20.04,” this way we created the test environment. Everything was placed in one virtual NAT network. In purpose to simulate DoS attacks we used 60 raspberry PIs. As a result, we detected and operated the next attacks.

To ensure that all sent data is transmitted uniformly, we employ the TCP protocol, with it's sequence numbers. Thus, first one sends a number (SYN) and the other side recognizes it, then other side returns an ACK with SYN number that must be recognized by the first party. This is called TCP triple handshake.

What can an attacker do in this case? - Attacker can overload the server by sending a large number of SYN requests to TCP ports. The server send SYN-ACK to each request and waits for the last ACK to finalize the triple handshake, so the server is forced to leave this connection open and wait for the SYN - ACK from the first side. even after closing the connection server immediately receives a new request from attacker. This suggests that we have a lot of connections left open, finally the server memory will be overloaded with SYN connections, leading to the emergence of DoS attack.

hping3 tool was used to perform this attack, which sent a lot of SYN requests to the server.

UDP Datagram Flood Attack

Because of its speed, the UDP protocol is often used in practice, it does not require the so-called three-way handshake and other additional operations. Through this protocol, an attacker can send numerous UDP data diagrams to randomly selected segments of the victim server. As a result of decryption, the server receives NONE, so it returns the "Destination unreachable" package. UDP is a fast protocol, so the server will be overloaded very soon with spam.

To carry out this attack we used the hping3 tool, which sent lots of UDP diagrams to the victim server [9-11].

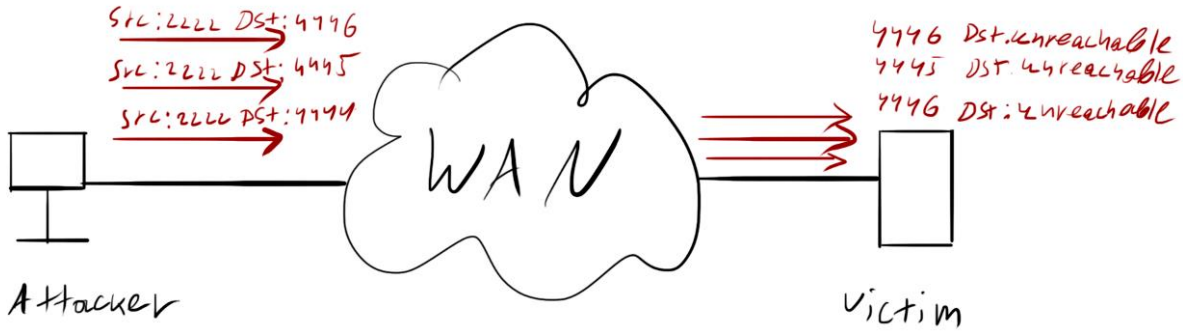

Figure 2: UDP datagram flood attack

We carried out this attack using a generated TCP SYN packet whose source ip / source port matches the destination ip / destination port. As a victim receives a packet, he sends that packet back to himself, rooting to an infinite loop, which results in overflow of system and DoS.

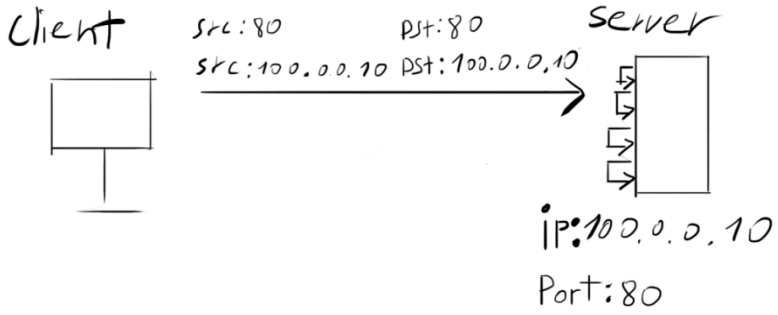

Figure 3: LAND attack

We used the hping3 tool to carry out this attack. We sent packages from the same source to the victim server.

ICMP Flood

To carry out this attack, we send too many ICMP (ping) messages to the server and invoke DoS.

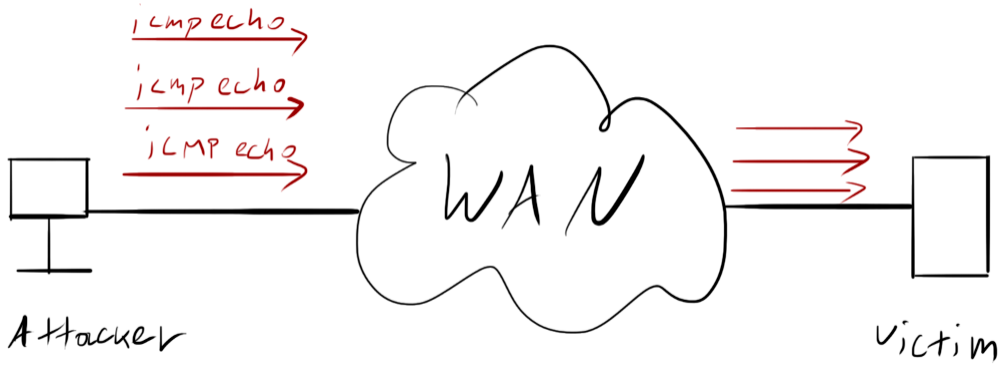

Figure 4: ICMP flood

We used the hping3 tool to carry out this attack. We sent echo requests from the same source to the victim server.

Smurf Attack

Too much ping is sent to the appropriate address to carry out this attack, the IP address of the victim is indicated when sending, which results in overstatement.

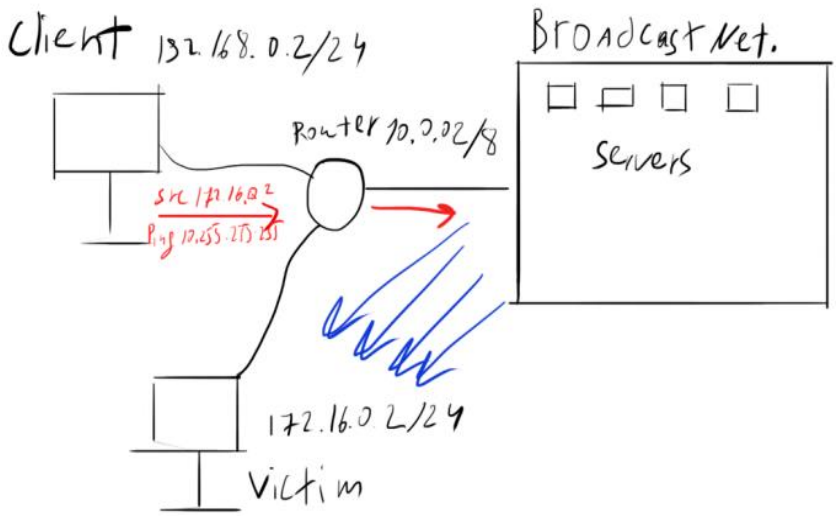

Figure 5: Smurf attack

A large number of pings are sent to the victim resulting in DoS. We used the hping3 tool to carry out this attack. We sent ping request to the target IP, instead of the source IP we indicated victim's IP address and we sent all response ICMP packets to the victim machine.

HTTP Flood Attack

During this attack, a large number of legitimate HTTP requests are sent via botnet, the aim is to waste server resources and caise DoS. We used the TorHammer tool to carry out this attack. Lots of HTTP requests were sent to the victim machine. It is not needed to use any spoofed or fake packets when performing this attack. Here botnet makes very much legitimate HTTP requests, to waste server resources and cause DoS.

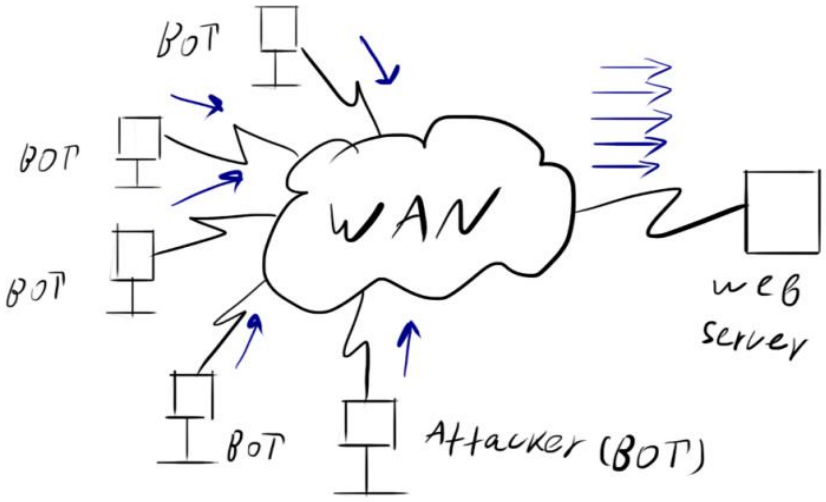

Figure 6: HTTP flood attack

Portmap Attack

Portmapper is used by many Windows and UNIX devices. When using this RPC service, Just like other DoS attacks we use fake IP (victim ip) and requests, we can get a large response that will ultimately be forwarded to the victim machine. To carry out this attack, we used a modified rpcinfom with a fake IP address. we sent all the returned RPCs to the victim machine.

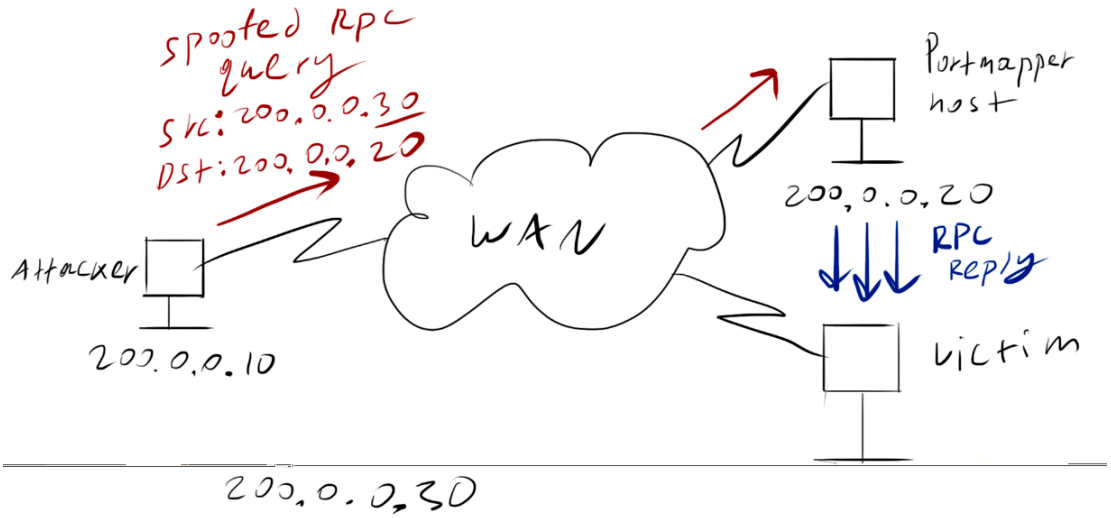

Figure 7: Portmap attack

To carry out this attack, we used the Nmap tool to scan TCP / UDP port on the victim's engine.

Password Brute Forcing

In brute forcing, the password is guessed by choosing simple letters or using dictionary words. During our tests brute force attack was implemented on FTP server. Ncrack tool was used to carry out this attack. FTP server was brute forced over virtualized network. During the testing, the FTP server was accessed through a virtual network

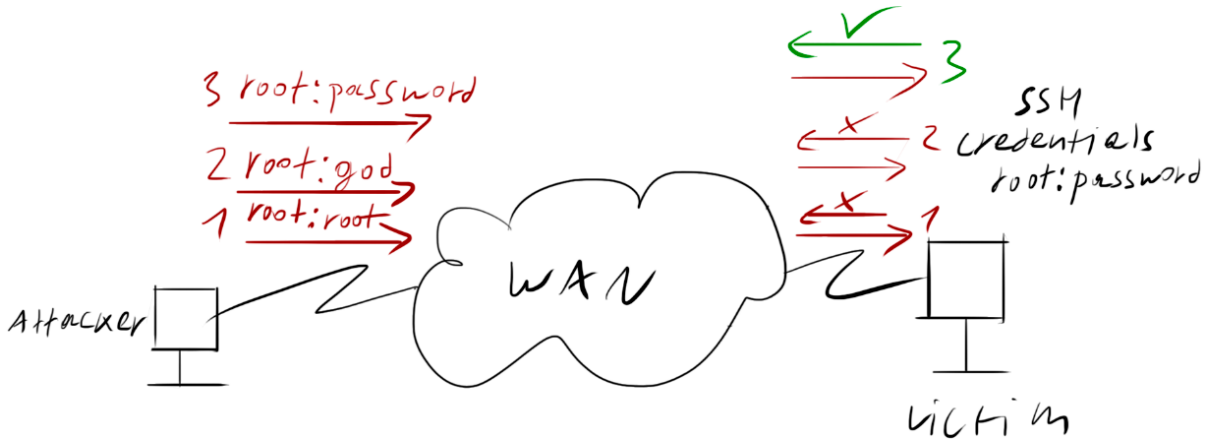

Figure 8: Password brute forcing

SNMP Amplification Attack

SNMP is used to collect and manage information from printers, servers, switches and other similar devices. The attacker sends a large number of requests to SNMP devices using the victim's IP address. The SNMP response size is much larger than the request size. All traffic goes to victim computer, which leads to DoS. To carry out the SNMP amplification attack, we used GetBulk messages, in this way we increased the traffic and forwarded it to the victim's device. We sent fake service configuration request, using the fake source's IP address, to the SNMP device, which returned a response to the victim computer. Due to the specific needs of the project, some "CICDDoS2019" attacks have not been carried out yet (NETBIOS attack).

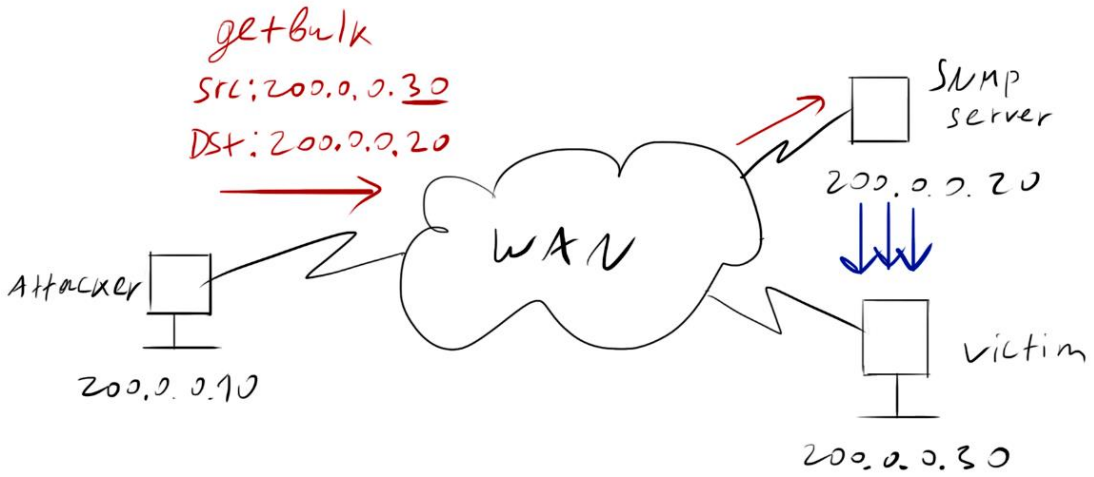

Figure 9: SNMP amplification attack

During IP fragmentation, a large IP packet is split into smaller pieces and sent over the network, then collected at its destination. IP fragmentation is used when the IP size exceeds the maximum transmission unit (MTU) size. When the server receives more data than the limit, it splits the data. The fragmentation mechanism can be used for various attacks:

TCP fragmentation Attack (Teardrop)

These attacks target TCP/IP reassembly mechanisms on a victim machine, preventing them from putting together fragmented packets. Packets overlap and overwhelm victim server, which causes DoS. UDP and ICMP Fragmentation Attack - The attacker sends a larger packet of counterfeits than MTU. The network splits it, but the destination server can no longer get it together as it is fake. This will result in a server overwhelm leading to DoS [12-13].

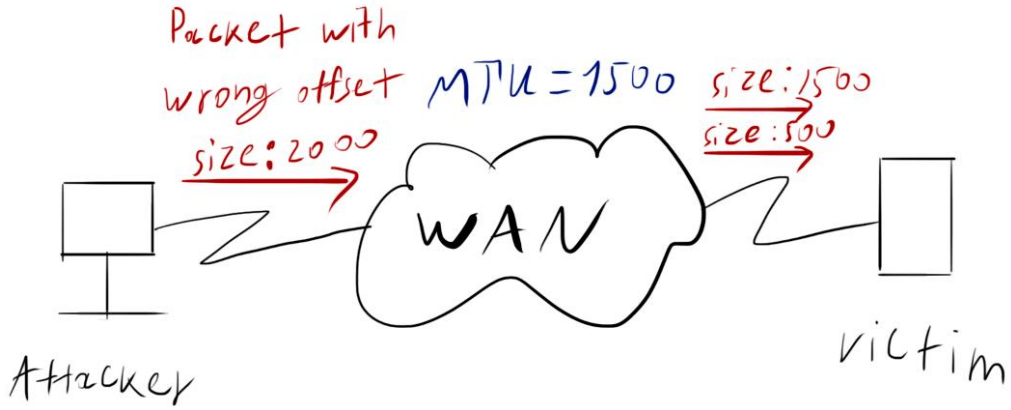

Figure 10: IP fragmentation attack

We used the python "scapy" library to realize this attack.

POD (Ping of Death)

Because of the limit, it is not possible to send a packet larger than 65,535 bytes, so an attacker sends 64,000-bit fragments of the packet. When the victim server assembles them, it receives a very large packet, which can lead to memory overload and DoS.

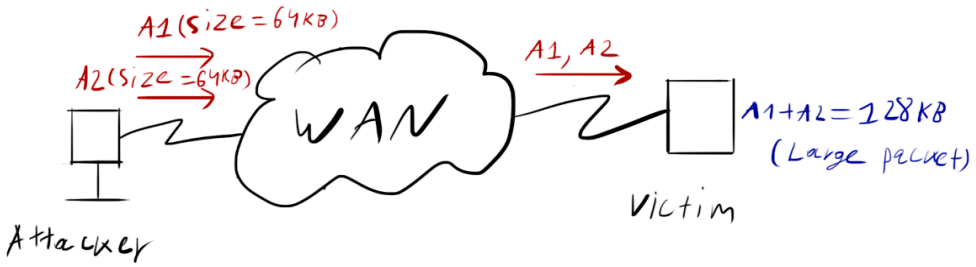

Figure 11: POD attack

To carry out POD attack, we used a special script that sent large segmented packets.

Slowloris Attack

An attack directed to the web service. Attacker sends many incomplete HTTP requests. The victim server opens more and more new connections which causes DoS.

Figure 12: Slowloris attack

We used Nmap script to carry out this attack.

NTP amplification attack

The NTP protocol is used to get exact time on the Internet, some older NTP servers have also monitoring service to count traffic. In this case an attacker can send an order requesting to extract a list of the last 600 hosts associated with the requested NTP server, the source IP has been changed to the victim's IP address. Thus NTP server sends a response to the victim computer, causing memory overload and DoS [14-16].

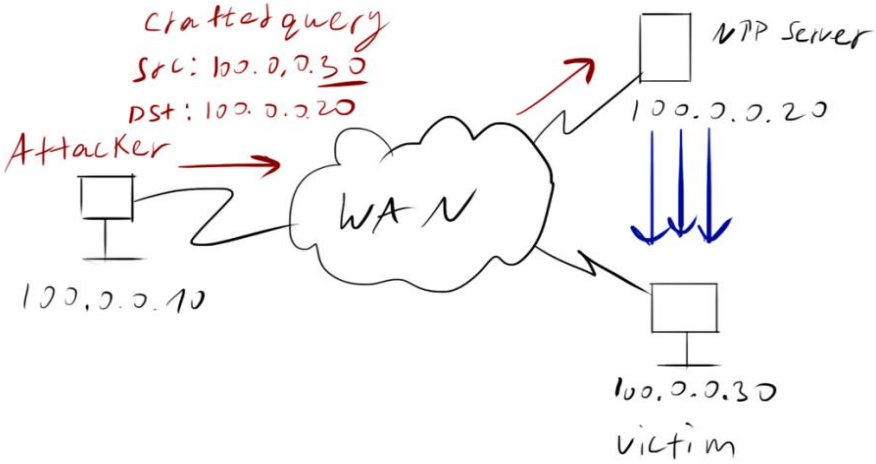

Figure 13: NTP amplification attack

To accomplish this attack, “monlist” requests were sent to the NTP server with a spoofed source IP address [17].

DDoS Attacks

We used our lab to simulate DDoS [18,19]. The attackers were using Ansible software to get orders from the server. The software connects to the host server via SSH and executes orders. To identify attacks, we used IDS module.

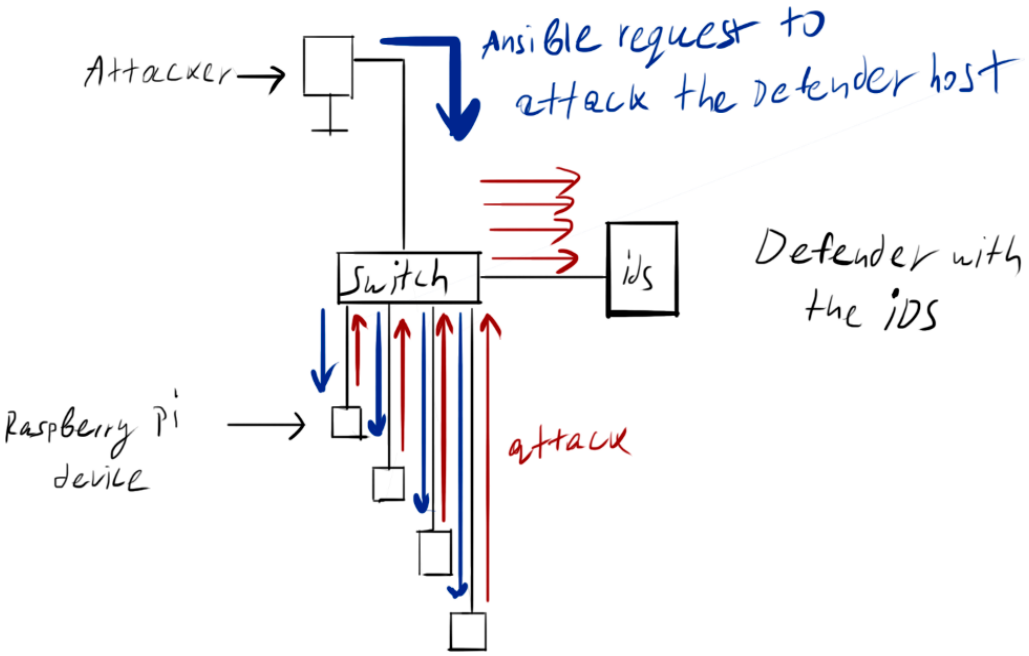

Figure 14: DDoS attacks

3. Experiments and Results

In our laboratory, we installed and tested IDS on a server. We have performed the following types of attacks on this server (Table 1):

- NTP amplification attack and DDoS
- Password brute forcing
- UDP datagram flood attack
- POD (Ping of Death)
- TCP Syn flood attack (Neptune)
- LAND attack
- HTTP flood attack
- Nmap probe
- SNMP amplification attack
- ICMP flood
- Portmap attack
- Smurf attack
- IP fragmentation attack
- Slowloris attack

Up to twenty different types of man in the middle attack were also carried out. Providing 5G protection against these types of attacks is an extremely important issue. We entered this data into our Intrusion Detection System and got the next results [20-22].

Table 1
Results from Intrusion Detection System

Attack type	Number of attacks	Identified attacks
Neptune	100	99
UDP	100	100
LAND	100	98
POD	100	100
ICMP flood	100	98
Smurf	100	82
HTTP flood	100	85
Portmap	100	97
NMAP	100	95
SNMP amplification	100	62
Password brute forcing	100	100
IP fragmentation	100	91
Slowloris	100	51
NTP amplification	100	98
DDoS	800	744
Neptune	100	99
UDP	100	100

The results obtained are a real indication that the IDS we offer can be of great use and can be used as a prototype version of a real IDS system. The detection rate of DOS / DDOS attacks by IDS is very high.

4. Conclusion and Future Plans

The proposed laboratory can test intrusion detection systems prepared using the CICDDoS2019 and NSL KDD datasets. A simulated lab can prepare smart IDS for testing in a 5G environment. The lab includes most of the attacks that pose a threat to the 5G environment. It is noteworthy that through this laboratory we can collect new attack patterns and use them to prepare Intrusion Detection System. On this basis we plan to develop an intrusion prevention system against the describe and integrate it into the 5G architecture. we plan to develop an intrusion prevention system for 5G architecture.

5. References

[1] A. Osseiran et al., "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," in IEEE Communications Magazine, vol. 52, no. 5, pp. 26-35, May 2014, doi: 10.1109/MCOM.2014.6815890.

[2] H. Zhang, et al., "Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges," in IEEE Communications Magazine, vol. 55, no. 8, pp. 138-145, Aug. 2017, doi: 10.1109/MCOM.2017.1600940.

[3] Iavich, M., et al.: "The novel system of attacks detection in 5G." In: Barolli, L., Woungang, I., Enokido, T. (eds.) AINA 2021. LNNS, vol. 226, pp. 580–591. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-75075-6_47

[4] Bocu R., Iavich M., Tabirca S. (2021) "A Real-Time Intrusion Detection System for Software Defined 5G Networks." In: Barolli L., Woungang I., Enokido T. (eds) Advanced Information Networking and Applications. AINA 2021. Lecture Notes in Networks and Systems, vol 227. Springer, Cham. https://doi.org/10.1007/978-3-030-75078-7_44

[5] D. Bega, et al. "A Machine Learning Approach to 5G Infrastructure Market Optimization," in IEEE Transactions on Mobile Computing, vol. 19, no. 3, pp. 498-512, 1 March 2020, doi: 10.1109/TMC.2019.2896950.

[6] M. E. Morocho-Cayamcela, H. Lee and W. Lim, “Machine Learning for 5G/B5G Mobile and Wireless Communications: Potential, Limitations, and Future Directions,” in IEEE Access, vol. 7, pp. 137184-137206, 2019, doi: 10.1109/ACCESS.2019.2942390.
[7] Yu. Danik, R. Hryschuk, S. Gnatyuk, “Synergistic effects of information and cybernetic interaction in civil aviation,” Aviation, Vol. 20, №3, pp. 137-144, 2016.
[8] V. Buriachok, et al., “Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies,” Cybersecurity Providing in Information and Telecommunication Systems (CPITS), pp. 23–32, Jul. 2020.
[9] S. Gnatyuk, “Critical Aviation Information Systems Cybersecurity,” Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks, Vol.47, №3, pp. 308-316, 2016.
[10] I. Ahmad, S. et al., “Security for 5G and Beyond,” in IEEE Communications Surveys & Tutorials, Vol. 21, no. 4, pp. 3682-3722, Fourthquarter 2019, doi: 10.1109/COMST.2019.2916180.
[11] Astapenya, V., Buriachok, V., Sokolov, V., Skladannyi, P., & Ageyev, D. (2021). “Last mile technique for wireless delivery system using an accelerating lens,” Proceedings of 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, pp. 811-814. doi:10.1109/PICST51311.2020.9467886
[12] D. Fang, Y. Qian and R. Q. Hu, “Security for 5G Mobile Wireless Networks,” in IEEE Access, vol. 6, pp. 4850-4874, 2018, doi: 10.1109/ACCESS.2017.2779146.
[13] R. Odarchenko et al, “Improved Method of Routing in UAV Network,” Proceedings of the 2015 IEEE 3rd International Conference on Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), Kyiv, Ukraine, October 13-15, Vol. 1, 2015, pp. 294-297.
[14] J. Cao et al., “A Survey on Security Aspects for 3GPP 5G Networks,” in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 170-195, Firstquarter 2020, doi: 10.1109/COMST.2019.2951818.
[15] Kuznetsov A., Kiian A., Smirnov O. et al, “Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids,” Proceedings of 2019 IEEE 6th International Conference on Energy Smart Systems, ESS 2019, Kyiv, 17 April 2019, pp. 353-358.
[16] M. Zaliskyi, et al., “Method of traffic monitoring for DDoS attacks detection in e-health systems and networks,” CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.
[17] P. Liu, et al., “Mitigating DoS Attacks Against Pseudonymous Authentication Through Puzzle-Based Co-Authentication in 5G-VANET,” in IEEE Access, vol. 6, pp. 20795-20806, 2018, doi: 10.1109/ACCESS.2018.2826518.
[18] Hu Z., et al, “Statistical techniques for detecting cyberattacks on computer networks based on an analysis of abnormal traffic behavior,” International Journal of Computer Network and Information Security, Volume 12, Issue 6, pp. 1-13, 2020.
[19] M. A. Javed and S. khan Niazi, “5G Security Artifacts (DoS / DDoS and Authentication),” 2019 International Conference on Communication Technologies (ComTech), 2019, pp. 127-133, doi: 10.1109/COMTECH.2019.8737800.
[20] Kozlovskyi V., et al., “Applying an adaptive method of the orthogonal laguerre filtration of noise interference to increase the signal/noise ratio,” Eastern-European Journal of Enterprise Technologies, Vol. 2, Issue 9 (104), pp. 14-21, 2020.
[21] Z. Hassan, A. Zaman, M. Shah et al, “Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems,” Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, October 16-18, 2018. Kyiv, Ukraine, pp. 283-288.
[22] E. Kaljic, A. Maric and P. Njemcevic, “DoS attack mitigation in SDN networks using a deeply programmable packet-switching node based on a hybrid FPGA/CPU data plane architecture,” 2019 XXVII International Conference on Information, Communication and Automation Technologies (ICAT), 2019, pp. 1-6, doi: 10.1109/ICAT47117.2019.8938862.