DDOS ATTACK DETECTION USING SNORT

Tanushree Gorai
20BCE1269
SCOPE
VIT Chennai

Poulami Bera
20BCE1305
SCOPE
VIT Chennai

ABSTRACT

The increasing prevalence of Distributed Denial of Service (DDoS) attacks is a major concern for organizations that rely on internet services. These attacks disrupt the availability of online services and cause significant financial losses. Therefore, detecting DDoS attacks in real-time is crucial for mitigating their impact. As the world is adapting and quickly moving with advanced development in technology and communication, the risks of such attacks is a serious problem to be addressed and solved by the security engineers and cybersecurity architects. DDoS attack detection also faces many disadvantages like false positives, overhead and scalability. In this paper we will try to detect DDoS attacks through simple visualization techniques by analysing and understanding the network data traffic. The network traffic data will be generated manually using snort for easy understanding of the concept of DDoS attacks. The performance metrics of the attack detection model can be detection rate, false positive rate, robustness, and response time. Our proposed future work is intended to provide researchers in this field with a comprehensive understanding of DDoS attack detection using visualization of the network data.

KEYWORDS – DDoS attacks, Snort, Visualization

INTRODUCTION

Distributed Denial of Service (DDoS) attacks have become a major concern for organizations of all sizes, as they can cause severe damage to businesses, leading to downtime, data theft, and financial loss. DDoS attacks can overwhelm a server, network, or website with a flood of traffic, making it inaccessible to legitimate users. Therefore, detecting and mitigating DDoS attacks has become a critical need for organizations to maintain the availability and security of their services. Traditional DDoS detection methods, such as signature-based detection and rule-based detection, are no longer effective against sophisticated attacks that use advanced techniques like encryption, low-and-slow attacks, and application-layer attacks. To overcome these challenges, researchers and security practitioners are exploring new approaches to DDoS attack detection, including machine learning, deep learning, and visualization techniques. DDoS or Distributed Denial of Service is a type of cyber-attack where a large number of compromised devices, also known as a botnet, flood a target website or server with traffic, rendering it inaccessible to legitimate users. The aim of a DDoS attack is to disrupt the availability of a website or server, causing inconvenience or financial loss to the target.

The whole world is now moving towards being digital technology. Every person has a laptop and an internet connection. All devices are now connected over a network, not only laptop but phones and home appliances etc. are all connected over a network. The threat of attacks and hacking the systems have also increased. The vast number of users and different types of devices, communication, social media contribute to the complex network data flow around the world which makes the network data more complex to analyse and determine the attackers on the network. To detect the network attackers, administrators usually collect huge amount of complex network data to study, analyse and understand the streamline and situation of the network. But to understand and interpret a huge dimension of data is difficult.

Visualization plays an important role here to help administrators understand and interpret the data efficiently. Visualization is the process of creating visual representations of data or information. In the context of cybersecurity, visualization can be a powerful tool for detecting DDoS attacks. Visualization tools can help by providing a graphical representation of network traffic patterns. By visualizing the traffic flow, spikes or unusual patterns can be detected which might indicate a DDoS attack.

In this paper, we will try to understand network data flow using snort in Linux. We will setup the systems using Virtual Machine, Kali Linux and try to record the ping requests from one system to the other and log the pings in a readable file. We also intend to use hping3 to create a dynamic network data model and understand the network flow deeply. Hping3 is a command-line tool that allows to transmit customized packets of data over a network to test for things like network connectivity, network latency, and firewall configurations. Hping3 will be used to detect the attacks by sending packets of data to the targeted system and monitoring the response time. After collecting a sample of network data, we will visualize the network data to interpret and determine the attackers in the network.

LITERATURE SURVEY

In this section, we will present the surveys we carried out on the papers related to DDoS attack detection. This section will help us understand the previous works executed on the topic and will help us gain insight about different interpretations of different experiments and project.

The ever-growing fast technology has now brought a huge amount of data on Internet. This gives rise to new threats and opportunities for attackers to intrude. DDoS attacks are performed easily by using the weaknesses of networks and by generating requests for services for software.

Real time detection and mitigation of DDoS attacks is difficult but holds a vital role to prevent attacks and enhance security of systems. This paper addresses the prediction of application layer DDoS attacks in real-time with different machine learning models. Two machine learning approaches Random Forest (RF) and Multilayer Perceptron (MLP) are utilized in this paper. They were able to use the big data approach, to detect an attack in real-time in a few milliseconds **[1]**. The network administrators work on large volume of traffic data to monitor the DDoS attack. The information visualization method is then introduced comprehend the information behind the multi-dimensional data efficiently. In this work, they surveyed the literature from 2004 to 2017 concerning network security visualization. They have classified these methods and given the advantages and shortcomings of each kind of method **[2]**.

This paper presents methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. The algorithms used are entropy and chi square. In result, they were able to determine that the network is under attack and deploy accurate filtering rules **[3]**. The article aims to address the growing concern of Distributed Denial of Service (DDoS) attacks in cloud computing environments. As more and more organizations rely on cloud computing for their critical infrastructure, the potential impact of DDoS attacks on the cloud becomes increasingly significant. The article describes an intrusion detection system (IDS) that is designed to detect and prevent DDoS attacks in cloud computing environments. The proposed IDS employs a combination of network traffic analysis and machine learning techniques to identify anomalous traffic patterns that may indicate a DDoS attack. The authors evaluate the performance of their IDS using a dataset of real-world traffic, and they report promising results in terms of accuracy and efficiency **[4]**. With advancing technology in telecommunication and internet, a security architecture is proposed for 5G mobile networks that includes a DDoS attack detection system. The proposed architecture is intended to protect 5G networks from various types of attacks, including DDoS attacks, which are becoming increasingly common. The authors suggest a Modified-DDoSNet, a system for detecting DDoS attacks in the SDN environment. A model based on Deep Learning (DL) techniques will be implemented, combining a Recurrent Neural Network (RNN) with an Autoencoder **[5]**. Even mathematics can be applied to detect DDoS attacks in the network. Effects of multivariate correlation analysis on the DDoS detection and proposes an example, a covariance analysis model for detecting SYN flooding attacks. The covariance model verifies the effectiveness of multivariate correlation analysis for DDoS detection to some extent. Some open issues still exist in this model for further research **[6]**. A DDoS attack is a serious global threat that results in the crashing of multiple servers, the blocking of network traffic, and a significant reduction in speed due to an overwhelming number of TCP and UDP flooding SYN attacks. This paper examines the various technologies, such as Machine Learning, Deep Learning, Blockchain, and Cybersecurity, that researchers have implemented to combat DDoS attacks **[7]**. Visualizing the data makes it easier to interpret and understand complex data of the systems. While there are numerous systems to visualize events that occur in the network, most of them are too complex to perceive, and require several visualization modes. The authors propose a framework that can represent different types of attacks and their relationships to each other. They also suggest a visualization tool that can display the state of an attacked network and the paths of the attacks through the network. The authors argue that such visualizations can help security experts to identify patterns in attacks and develop more effective countermeasures **[8]**. A three-stage approach that involves data preprocessing, feature extraction, and visualization. The visualization of network data can display the real-time status of the network and identifies potential DDoS attacks. The authors argue that this system can provide security analysts with a more intuitive understanding of the network and enable them to respond more quickly to attacks **[9]**. A visual analytics model for detecting intrusion in a flood attack. The proposed model uses a combination of statistical analysis, data mining, and visualization techniques to identify anomalies in network traffic that indicate a flood attack **[10]**. Network defenders require an interactive visualization system to monitor and manage real time complex data and determine any anomalies or attacks in the Network. A light-weight traffic visualization system (TVis) can be used for detecting distributed denial of service (DDoS) attacks. The proposed system uses a combination of data visualization and machine learning techniques to detect anomalous network traffic patterns. The model uses undirected graph to analyse the network data and utilizes mapping to determine intruders with a high-rate of detection of DDoS attacks **[11]**. An artificial neural network method contains self-organizing mapping facilities efficient to complete and visualize high-dimensional data topology representation, applicable in a number of applications such as network intrusion detection. Some numerical experiments demonstrate that the key performance in DoS attack detection including the detection rate, the false positive rate, and the training time is greatly enhanced **[12]**. There are several types of attacks the attackers use to breach into the systems. Therefore, it is important to prepare a system in a such a way which is able to detect any kind of attack. identification of DoS attacks by grouping similar attack patterns based on their characteristics can help cover various kinds of attacks for the system to detect. K-means algorithm can be implemented to cluster the traffic into several groups. Then the results are visualized using graphs and charts to show the distribution of traffic and the identified clusters **[13]**. It is very important to develop effective and efficient automated cyberattack detection and visualization techniques due to the growing number of cyberattacks and their impact on various sectors. Combination of automated detection and visualization techniques can enhance the ability of cybersecurity experts to identify and respond to cyberattacks quickly and effectively **[14]**. The authors used a dataset of network traffic to evaluate the performance of the proposed model. The results show that the proposed model can effectively identify and classify intrusion patterns in flood attacks and provide a clear and intuitive visual representation of the analysed data. The authors suggest future research directions, including the exploration of different visualization techniques and the development of more advanced machine learning algorithms to improve the accuracy and efficiency of intrusion detection systems **[15]**. A combination or hybrid models can help in efficiently to detect and classify attacks in a network. For example, A proposal of combining Random Forest algorithm with feature selection techniques to improve the accuracy and efficiency of the detection process. The results show that the proposed approach can effectively detect and classify different types of DoS attacks, including UDP flood, HTTP flood, and SYN flood attacks **[16]**. Traditional signature-based approaches are no longer effective against the ever-increasing number and complexity of DoS attacks. Machine learning algorithms can be used to train a neural network to detect and classify DoS attacks based on the characteristics of network traffic **[17]**. A framework that combines network visualization with expert knowledge to detect and analyse network security breaches caused by complex attacks. The proposed approach can be used in conjunction with existing intrusion detection and prevention systems to enhance their capabilities in detecting and mitigating complex attacks **[18]**. Collaborative based systems are also useful in efficiently processing data and applying algorithms for accurate results. Collaborative defence system is effective in detecting and mitigating the attack, with a significant reduction in the number of attack packets reaching the target. Blockchain-based collaborative defence, including improved security management, faster response times, and reduced costs **[19]**. Analysing the traffic flow data can help identify patterns and anomalies associated with DDoS attacks. The authors use spline functions to model the traffic flow, and develop an algorithm to detect deviations from the expected behavior. They also use the spline functions to predict future traffic flow, allowing for early detection of potential DDoS attacks. The potential advantages are scalability and applicability to a range of network topologies and attack scenarios **[20]**.

PROPOSED SYSTEM ARCHITECTURE

The tools used for DDoS attack simulation are snort, hping3 and scapy module in python. The victim machine uses snort to detect packets that are sent by the hacker by configuring existing and local rules in order to match the packets that might be sent as an attack. The hacker uses hping3 command, which is an efficient ‘ping’ command to send multiple packets to a victim system by knowing its ip address. The rules configured in this project detects packets sent by hackers if more than 100 packets are sent to the victim machine within 1 second. This kind of an attack is called a DoS attack as it uses up the resources of the machine and prevents it from responding to its original work.

The scapy library is used in the python code to visualize the number of packets sent from the particular ip of the hacker and the reply or acknowledgement sent by the victim machine. This is useful to compute the statistics of the number, type and origin of the packets that are sent as an attack towards the system.

MODULE DESCRIPTION

<u>Snort</u>

1) Rules

The rules for detecting packets as per user requirements is mentioned in the local.rules file and that file is included in the snort configuration document. The local.rules file allows custom rules to be included in the original configuration document.

To detect more than 100 icmp packets that are sent within 1 second from any external ip address and any port to any port in the victim ip address, and to log the captured packet detail, the following rule is mentioned.

alert icmp any any → $HOME_NET any (msg:“Possible ICMP flood Attack”; threshold: type both, track by_src, count 100, second 1; sid:100001;)

2) Start snort

This command starts Snort for detecting network traffic.

```
snort -A console -q -c /etc/snort/snort_test.conf -l /var/log/snort
```

-A console ensures that alerts are displayed in the console
-q keeps the warnings and other irrelevant outputs in quiet mode.
-c is followed by the path to the snort configuration file
-l specifies the directory in which the detected packet information should be logged.

3) Accessing Log File

The log files are present in /var/log/snort directory. To open a log file in human readable format and write it into a visualizable format (here we use .pcap files), we use the tcpdump command.

```
tcpdump -r <log_file_name> -w <visualizing_file_name.pcap>
```

-r specifies the log file to be read
-w denotes the file in which it must be written.

hping3

hping3 command is used to send efficient ping to specific ip addresses with various options of manipulating the type, number, interval and many other features of the packets that are sent.

To send 500 icmp packets to the victim ip address within 1 second, we use

```
hping3 -c 500 -i u10 -1 <victim_ip_address>
```

-c specifies the count of packets
-i u10 mentions that the packets should be sent in an interval of 10 microseconds
-1 shows that icmp packets need to be sent

Visualisation

Scapy

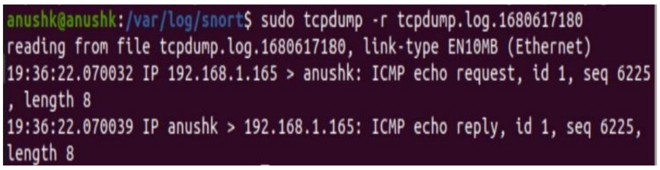
Using scapy library in python helps us to visualize the log files that are generated in snort when it captures packets sent from an attacker. These log files are converted to .pcap format using tcpdump command in order to make this visualization process simpler. The code then uses matplotlib library to plot the graphs of the captured packet as specified by the us

IMPLEMENTATION AND RESULTS

Dataset

The dataset used in this project is generated in real time while the packets are sent from any source ip address to the victim address. The log files created during this process is used as a dataset for the visualisation and interpretation.

The log files are converted to human readable format and python libraries are used in visualizing and interpreting this data.



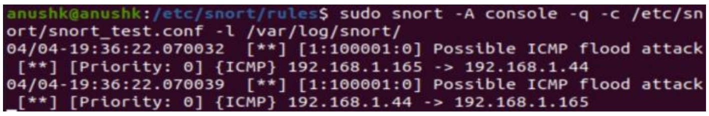
```
anushk@anushk:/var/log/snort$ sudo tcpdump -r tcpdump.log.1680617180
reading from file tcpdump.log.1680617180, link-type EN10MB (Ethernet)
19:36:22.070032 IP 192.168.1.165 > anushk: ICMP echo request, id 1, seq 6225
, length 8
19:36:22.070039 IP anushk > 192.168.1.165: ICMP echo reply, id 1, seq 6225,
length 8
```

Working of Project

Step 1: - Start snort in console mode with snort. conf file and instruction to log in var/log/snort/folder

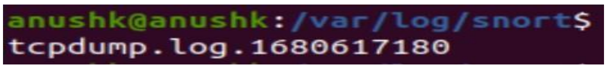
Step 2: - Send packets from attack machine using hping3

Step 3: - Observe the alerts posted by snort while receiving the packets

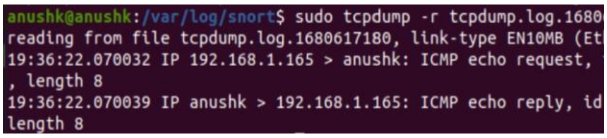


```
anushk@anushk:/etc/snort/rules$ sudo snort -A console -q -c /etc/sn
ort/snort_test.conf -l /var/log/snort/
04/04-19:36:22.070032  [**] [1:100001:0] Possible ICMP flood attack
 [**] [Priority: 0] {ICMP} 192.168.1.165 -> 192.168.1.44
04/04-19:36:22.070039  [**] [1:100001:0] Possible ICMP flood attack
 [**] [Priority: 0] {ICMP} 192.168.1.44 -> 192.168.1.165
```

Step 4: - Check for log file

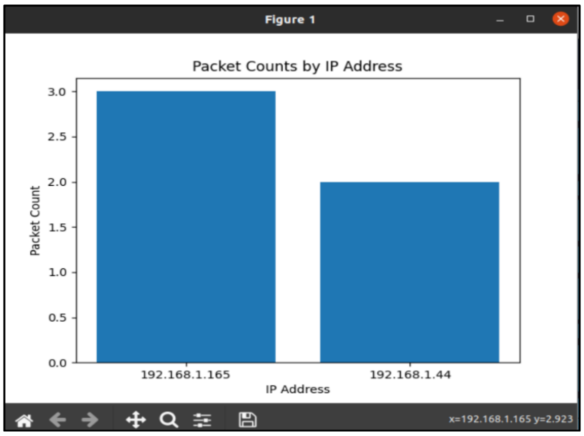


```
anushk@anushk:/var/log/snort$
tcpdump.log.1680617180
```



```
anushk@anushk:/var/log/snort$ sudo tcpdump -r tcpdump.log.1680
reading from file tcpdump.log.1680617180, link-type EN10MB (Et
19:36:22.070032 IP 192.168.1.165 > anushk: ICMP echo request,
, length 8
19:36:22.070039 IP anushk > 192.168.1.165: ICMP echo reply, id
length 8
```

Step 5: - Visualization



Results – visualization and final interpretation

The packets have been sent from the attack machine using hping3 and detected in the victim machine using snort successfully. The log files are collected from snort automatically and the details of the packet sent are visualized.

The visualization shows the number of packets sent from any attacker and the number f response/acknowledgement sent by the victim machine. This is done only when more than 100 packets are sent from a single IP address within a second.

The victim machine is now enabled to detect ddos attacks that are attempted by any malicious user and can detect it immediately, thereby safeguarding resources in the machine.

CONCLUSION AND FUTURE WORKS

In conclusion, the project on DDoS attack detection using Snort and Hping3 has shown that it is possible to effectively detect and mitigate DDoS attacks. The system utilizes Snort, a popular open-source network intrusion detection system, to monitor network traffic and identify potential DDoS attacks. Hping3 is used to simulate a DDoS attack and test the effectiveness of the system in detecting and mitigating the attack.

The project has highlighted the importance of having reliable and efficient solutions in place to counter DDoS attacks. With the increasing frequency and sophistication of these attacks, it is essential to have robust defense mechanisms that can quickly detect and mitigate them.
Future work for this project could involve enhancing the system's performance by implementing machine learning algorithms to improve the accuracy of attack detection and mitigation.

Additionally, exploring the use of other open-source tools and technologies to improve the system's overall effectiveness would be beneficial.. In summary, this project provides a solid foundation for continued research and development in the field of DDoS attack detection and mitigation. With the ongoing evolution of DDoS attacks, it is crucial to have effective and reliable defense mechanisms in place to safeguard networks and systems.

REFERENCES

[1] Awan, M.J.; Farooq, U.; Babar, H.M.A.; Yasin, A.; Nobanee, H.; Hussain, M.; Hakeem, O.; Zain, A.M. Real-Time DDoS Attack Detection System Using Big Data Approach. Sustainability 2021, 13, 10743. https://doi.org/10.3390/su131910743

[2] C. Wu, S. Sheng and X. Dong, "Research on Visualization Systems for DDoS Attack Detection," 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, 2018, pp. 2986-2991, doi: 10.1109/SMC.2018.00507.

[3] L. Feinstein, D. Schnackenberg, R. Balupari and D. Kindred, "Statistical approaches to DDoS attack detection and response," Proceedings DARPA Information Survivability Conference and Exposition, Washington, DC, USA, 2003, pp. 303-314 vol.1, doi: 10.1109/DISCEX.2003.1194894.

[4] N. Kumar and S. Sharma, "Study of intrusion detection system for DDoS attacks in cloud computing," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, India, 2013, pp. 1-5, doi: 10.1109/WOCN.2013.6616255.

https://ieeexplore.ieee.org/document/6616255

[5] J. Gojic and D. Radakovic, "Proposal of security architecture in 5G mobile network with DDoS attack detection," 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Split / Bol, Croatia, 2022, pp. 1-5, doi: 10.23919/SpliTech55088.2022.9854338.

https://ieeexplore.ieee.org/document/9854338

[6] Shuyuan Jin and D. S. Yeung, "A covariance analysis model for DDoS attack detection," 2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577), Paris, France, 2004, pp. 1882-1886 Vol.4, doi: 10.1109/ICC.2004.1312847.

[7] I. Varalakshmi, M. Thenmozhi and R. Sasi, "Detection of Distributed Denial of Service Attack in an Internet of Things Environment -A Review," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526378.

[8] A. Yelizarov and D. Gamayunov, "Visualization of complex attacks and state of attacked network," 2009 6th International Workshop on Visualization for Cyber Security, Atlantic City, NJ, USA, 2009, pp. 1-9, doi: 10.1109/VIZSEC.2009.5375527.

[9] C. Wu, S. Sheng and X. Dong, "Research on Visualization Systems for DDoS Attack Detection," 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, 2018, pp. 2986-2991, doi: 10.1109/SMC.2018.00507.

[10] J. Zhang and M. L. Huang, "Visual Analytics Model for Intrusion Detection in Flood Attack," 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 2013, pp. 277-284,doi: 10.1109/TrustCom.2013.38.

[11] A. Kalwar, M. H. Bhuyan, D. K. Bhattacharyya, Y. Kadobayashi, E. Elmroth and J. K. Kalita, "TVis: A Light-weight Traffic Visualization System for DDoS Detection," 2019 14th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP), Chiang Mai, Thailand, 2019, pp. 1-6, doi: 10.1109/iSAI-NLP48611.2019.9068666.

[12] X. Qu et al., "Statistics-Enhanced Direct Batch Growth Self-Organizing Mapping for Efficient DoS Attack Detection," in IEEE Access, vol. 7, pp. 78434-78441, 2019, doi: 10.1109/ACCESS.2019.2922737.

[13] N. A. Putri, D. Stiawan, A. Heryanto, T. W. Septian, L. Siregar and R. Budiarto, "Denial of service attack visualization with clustering using K-means algorithm," 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), Palembang, Indonesia, 2017, pp. 177-183, doi: 10.1109/ICECOS.2017.8167129.

[14] F. Alhaidari et al., "A study on Automated Cyberattacks Detection and Visualization," 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, 2022, pp. 715-722, doi: 10.1109/CICN56167.2022.10008351

[15] J. Zhang and M. L. Huang, " Intrusion Detection in Flood Attack using Visual Analytics Model," 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 2013, pp. 277-284, doi: 10.1109/TrustCom.2013.38.

[16] P. J. Shinde and M. Chatterjee, "A Novel Approach for Classification and Detection of DOS Attacks," 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 2018, pp. 1-6, doi: 10.1109/ICSCET.2018.853734

[17] S. Wankhede and D. Kshirsagar, "DoS Attack Detection Using Machine Learning and Neural Network," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697702.

[18] A. Yelizarov and D. Gamayunov, "Determining State of attacked network of complex attacks using visualization ," 2009 6th International Workshop on Visualization for Cyber Security, Atlantic City, NJ, USA, 2009, pp. 1-9, doi: 10.1109/VIZSEC.2009.5375527.

[19] C. Killer, B. Rodrigues and B. Stiller, "Security Management and Visualization in a Blockchain-based Collaborative Defense," 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 108-111, doi: 10.1109/BLOC.2019.8751272.

[20] S. Kivalov and I. Strelkovskaya, "Detection and prediction of DDoS cyber attacks using spline functions," 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2022, pp. 710-713, doi: 10.1109/TCSET55632.2022.9766940.