Detecting and Mitigating Network attacks using Network Simulator 3

Anmol Bamane[1], Advait Porandwar[2], Allan Jadhav[3], Guide, Prof. Rohan Shinde[4]
[1,2,3,4]*Department of Electronics & Communication Engineering, MIT School of Engineering & Sciences, MIT Art, Design & Technology University, Pune*

Abstract-Distributed Denial of Service (DDoS) attacks pose significant threats to the availability and stability of online services. This abstract explores the technique of employing a proxy server as a means to mitigate the impact of DDoS attacks. By introducing a buffer node between clients and servers, the proxy server acts as an intermediary, filtering and inspecting incoming traffic to identify and discard malicious requests while allowing legitimate traffic to reach the server. Additionally, the proxy server can enforce rate limiting measures to control traffic flow, preventing overwhelming volumes of requests from reaching the server. Although this approach can enhance DDoS protection, it is important to consider potential latency implications and the possibility of determined attackers bypassing the proxy server. Thus, a comprehensive DDoS mitigation strategy involves multiple layers of defense, including network-based and application-based defenses. By leveraging the proxy server technique alongside other measures, organizations can bolster their network defenses, fortify their resilience against DDoS attacks, and ensure uninterrupted availability of their services.

Key words: DDoS attacks, proxy server, mitigating, network defenses, buffer node, intermediary, filtering, inspecting, malicious requests, legitimate traffic, rate limiting, latency implications, determined attackers, comprehensive mitigation strategy, network-based defenses, application-based defenses, bolster, resilience, uninterrupted availability, services.

1.INTRODUCTION

With the increasing reliance on online services and the interconnectedness of modern systems, the vulnerability to Distributed Denial of Service (DDoS) attacks has become a critical concern for organizations. These malicious attacks, aimed at overwhelming servers with a flood of traffic, can cripple online platforms, disrupt operations, and lead to significant financial losses. To address this threat, the utilization of a proxy server as a key component in DDoS mitigation strategies has gained prominence. By introducing a buffer node between clients and servers, a proxy server acts as an intermediary that filters and inspects incoming traffic, distinguishing between legitimate user requests and malicious traffic. This proactive approach allows organizations to identify and discard harmful requests, while ensuring that genuine traffic reaches the intended servers. Furthermore, proxy servers can implement rate limiting measures to control traffic flow and prevent server overload. However, the efficacy of this technique must be considered in tandem with potential latency implications and the evolving strategies employed by determined attackers. Consequently, an all-encompassing DDoS mitigation strategy necessitates a multi-layered defense approach, integrating network-based and application-based defenses. This paper examines the role of proxy servers in mitigating DDoS attacks, their benefits, potential limitations, and the significance of a comprehensive approach to fortify network defenses and maintain uninterrupted service availability.

Critical infrastructures are vulnerable, as seen by the extensive effects of prior failures and disruptions. Occurred events showed the extent of impacts caused by a wide variety of threats, such as targeted attacks (e.g., cyber-attacks on critical infrastructure), failures (e.g., major blackouts) or natural disasters (e.g., earthquakes and floods).

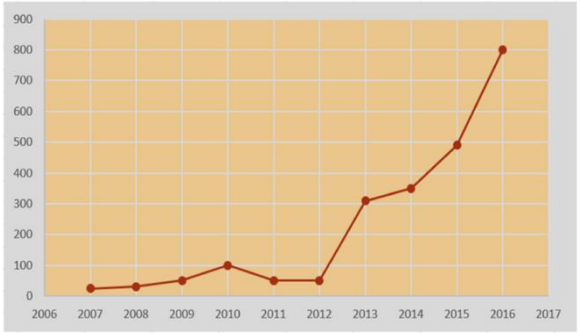

Figure 1.1 The volume sizes of DDoS attacks in gigabits per second

Arbor Networks reports that they track over 1000 significant DDoS attacks daily worldwide. These attacks target a wide range of victims, from individual home users to governments. Victims can include e-commerce sites, banks, commercial organizations, and ISPs. Financial gain is often a motivation behind these attacks, but other attractive targets can include pornography or online gambling sites. Political organizations and governments are also frequently targeted. Even gaming sites or stock exchanges can fall victim to DDoS attacks, as shown in above from a quarterly report by Kaspersky Lab. The report reveals that e-commerce sites were the primary targets of DDoS attacks

The impacts of these disruptions can be felt across multiple sectors of society, including transportation, healthcare, food and water supply, and communications. In some cases, disruptions in critical infrastructure can lead to cascading effects that spread across multiple systems, exacerbating the impact of the original disruption.

2.LITERATURE SURVEY

"A Comprehensive Survey of Network Security" by B. A. Forouzan and G. A. Mukhopadhyay.[22]

This survey provides a comprehensive overview of network security, covering a wide range of topics and concepts related to securing computer networks. It starts by introducing the fundamental principles of network security and the importance of protecting data and resources within a networked environment. The survey delves into various cryptographic algorithms and techniques used for secure communication, including symmetric and asymmetric encryption, digital signatures, and secure hash functions. It explains how these cryptographic mechanisms ensure confidentiality, integrity, and authenticity of data in transit.

Authentication mechanisms are another critical aspect covered in the survey. It explores various authentication methods, such as passwords, biometrics, and multi-factor authentication, and discusses their strengths, weaknesses, and implementation considerations. The survey also highlights the importance of strong password policies and secure storage of authentication credentials. Access control models and methods are thoroughly examined, including discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). The survey discusses the principles, advantages, and limitations of these access control mechanisms in different network scenarios.

Furthermore, the survey provides insights into network perimeter security through the analysis of firewalls. It explains the working principles of firewalls, their configurations, and various types of firewalls, such as packet-filtering, stateful inspection, and application-level gateways. The survey also touches upon intrusion detection systems (IDS) and intrusion prevention systems (IPS), explaining how these technologies monitor network traffic and detect/prevent potential attacks.

Finally, the survey addresses network vulnerabilities and threats, highlighting common attack vectors such as network scanning, spoofing, denial-of-service (DoS), and man-in-the-middle attacks. It discusses the impact of these threats on network security and provides an overview of mitigation techniques and best practices to enhance network defenses.

" Security Attacks and Countermeasures in Wireless Sensor Networks." Haque, A K M Bahalul & Bhushan, Bharat. (2021). [24]

This survey provides an in-depth analysis of network security attacks and countermeasures, focusing on the different types of threats faced in modern network environments. It starts by discussing malware attacks, exploring various forms of malicious software such as viruses, worms, trojans, and ransomware. The survey examines the characteristics, propagation mechanisms, and potential impacts of malware, as well as countermeasures such as antivirus software, intrusion detection systems, and user awareness programs.

The survey delves into Distributed Denial of Service (DDoS) attacks, which aim to overwhelm network resources and disrupt services. It explains the various types of DDoS attacks, including volumetric, application-layer, and reflective attacks, and discusses defense strategies such as traffic filtering, rate limiting, and anomaly detection. Phishing and social engineering attacks are also covered in the survey. It explains how attackers exploit human vulnerabilities to deceive users and gain unauthorized access to sensitive information. The survey explores techniques used in phishing attacks, such as email spoofing and fake websites, and highlights user awareness training,

spam filters, and browser warnings as effective countermeasures.

The survey addresses insider threats, which involve unauthorized actions performed by individuals with legitimate access to network resources. It discusses the risks posed by insider attacks, including data theft, sabotage, and unauthorized system modifications. The survey explores techniques for detecting and preventing insider threats, such as access controls, user behavior monitoring, and incident response procedures.

Encryption and secure communication protocols are examined as critical countermeasures to protect data in transit. The survey explains various encryption algorithms and protocols used to establish secure communication channels, including SSL/TLS and IPsec. It also discusses key management techniques and the importance of secure cryptographic protocols for maintaining data confidentiality and integrity.

Intrusion detection and prevention techniques are another key focus of the survey. It explores the use of intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic, detect suspicious activities, and respond to potential threats. The survey discusses various approaches to intrusion detection, including signature-based, anomaly-based, and hybrid methods.

Common Intelligent Algorithms Applied

In this literature review, a number of papers were studied between the period of 2010–2021 and a plethora of both ML and DL techniques were utilized in these papers for building or comparing Machine Learning models in order to detect and classify network attacks. Figure given below(Fig 2.1) presents a list of all the respected papers that utilized the different algorithms, outlining all of the issue areas that each algorithm was applied to as well as the best results obtained. Figure 2.1 presents the number of articles that utilized each algorithm. As seen from the figure RF and SVM were the most widely used algorithms in a good number of papers and ELM was the least applied algorithm. For ML algorithms, the best performing algorithms were DT, RF, and KNN with their accuracy reaching up to 100% and the least utilized algorithms were J.48 and KNN. The least used and least common DL algorithm was ELM, which is thought to be fast in terms of training because it only has one hidden layer, so it is typically applied to simple applications. The best performing DL algorithm was RRN, with the highest accuracy of 100% achieved. To handle more complicated issues with more precision, it has recently been expanded to be hierarchical.

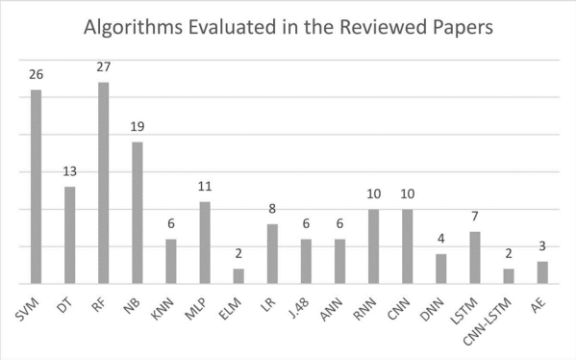

Fig 2.1 Evaluation of algorithms.

3.METHODOLOGIES

Network Simulator 3 (NS 3)

NS-3, or Network Simulator 3, is an open-source discrete-event network simulator used for modelling, simulating, and analyzing computer networks. It provides a comprehensive framework for network simulations, allowing researchers, developers, and network engineers to design, evaluate, and validate various network protocols, algorithms, and applications in a controlled and reproducible environment.

NS 3 Architecture

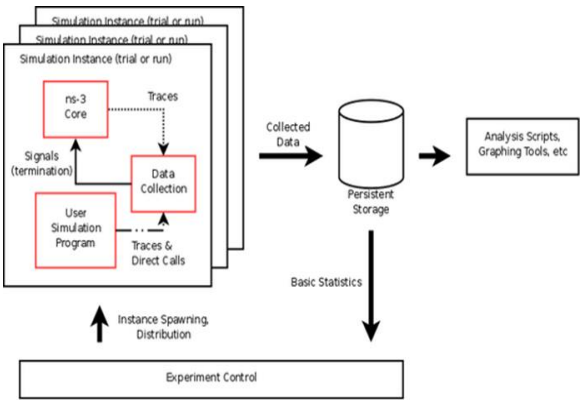

Figure 3.1 NS 3 Architecture

NS-3, or Network Simulator 3, follows a modular and extensible architecture that allows users to customize and extend its functionality. The architecture of NS-3 is organized into several layers and components, which work together to simulate the behaviour of computer networks.

Creating Simulation in NS3

Network Topology Design

Network Model: NS-3 provides a network model that allows users to define the topology, nodes, and links of the network being simulated. The network model includes support for various types of networks, such as wired, wireless, and point-to-point networks, and allows users to configure their properties, such as bandwidth, delay, and packet loss.

Protocol Stacks: NS-3 includes implementations of various networking protocols, such as IPv4, IPv6, TCP, UDP, Wi-Fi, LTE, Ethernet, Bluetooth, ZigBee, and more. These protocol stacks can be used to simulate the behaviour of real-world networking protocols and evaluate their performance under different conditions.

Applications: NS-3 supports a wide range of applications, such as web browsing, file transfer, video streaming, and more. Users can define their own application models or use existing ones to generate traffic and simulate realistic network scenarios.

Tracing and Logging: NS-3 provides facilities for tracing and logging network events and activities, allowing users to capture and analyze the behaviour of the simulated network. Tracing and logging can be used for performance analysis, debugging, and understanding the inner workings of the simulated network.

Visualization: NS-3 includes built-in support for visualizing network topologies, packet traces, and other simulation results. Visualization tools allow users to visually analyze the behaviour of the simulated network and understand the dynamics of network protocols and applications.

Overall, NS-3's architecture is modular and extensible, allowing users to configure, customize, and extend its functionality to suit their specific simulation needs. It provides a flexible framework for modelling and simulating a wide variety of network scenarios and protocols, making it a powerful tool for network researchers and practitioners.

Network Topology Design involves creating a representation of a network's structure and connectivity within a network simulator like NS3. It plays a crucial role in accurately modeling the network environment for various simulations, including DDoS attack demonstrations. Here are more details on Network Topology Design:

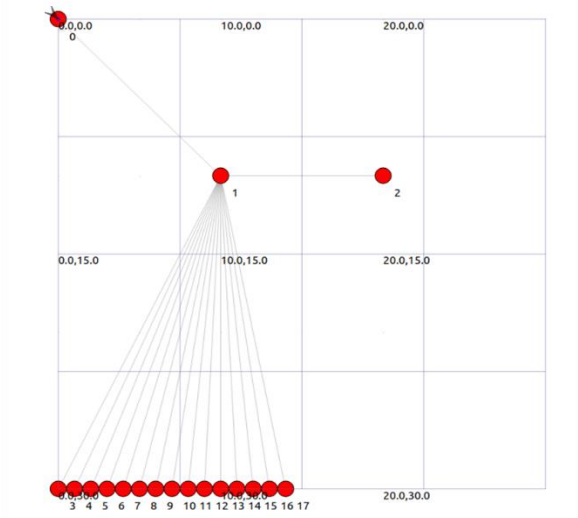

Figure 3.2 Node configuration

Attack Model Implementation

It involves simulating various types of DDoS attacks in a network simulator like NS3. It aims to replicate the behaviour and characteristics of real-world attacks to assess the network's vulnerability and evaluate mitigation strategies. Here are more details on Attack Model Implementation:

Attack Types: Identify and select the specific types of DDoS attacks to be implemented in the simulation. Common attack types include volumetric attacks (e.g., UDP floods, ICMP floods), protocol-based attacks (e.g., TCP SYN floods, DNS amplification), and application-layer attacks (e.g., HTTP floods). Choose attack types based on their relevance to the network being simulated and the research objectives.

Attack Distribution: Determine how the attack traffic is distributed across the network during the simulation. This involves selecting the source IP addresses and determining the distribution patterns of the attack traffic. It can include uniform distribution, random distribution, or specific targeting of network components. The attack distribution should be based on the attack type being simulated and the intended impact on the network.

Adding a Proxy Server

A proxy server can play a crucial role in mitigating DDoS (Distributed Denial of Service) attacks by acting as an intermediary between clients and the target server. Here's a high-level overview of how a proxy server works in DDoS mitigation:

Traffic Filtering: The proxy server sits between the clients and the target server, intercepting and filtering incoming traffic. It analyzes the incoming requests and applies filtering mechanisms to identify and block malicious traffic associated with the DDoS attack. Filtering can be based on various factors such as IP addresses, traffic patterns, request types, or known attack signatures.

Rate Limiting: The proxy server implements rate limiting mechanisms to control the flow of traffic to the target server. It sets thresholds on the number of requests per second or bandwidth consumption, ensuring that only legitimate traffic reaches the target server. By limiting the rate of incoming requests, the proxy server can mitigate the impact of the DDoS attack and prevent resource exhaustion on the target server.

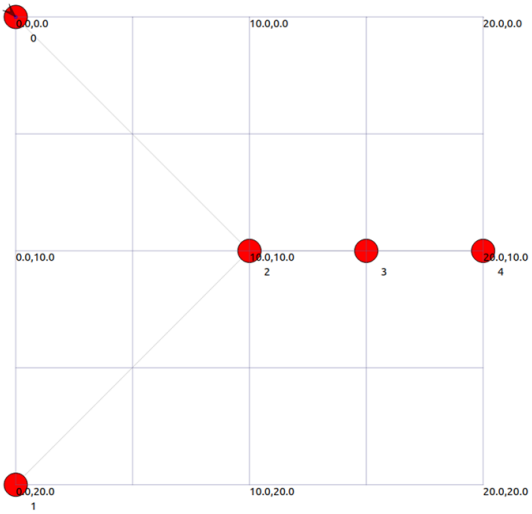

Figure 3.3 Buffer Node configuration

Working of the buffer(proxy) node:

A buffer node (node numbered 3 in above figure 3.2), also known as a "scrubbing center" or "clean pipe," is an intermediate device placed between the client and server to filter out malicious traffic and forward legitimate traffic. The scrubbing center can detect and mitigate DDoS attacks by analyzing network traffic and filtering out any traffic that matches a known attack pattern.

A proxy server, on the other hand, is a server that acts as an intermediary between the client and server. The proxy server can inspect incoming traffic, filter out malicious traffic, and forward legitimate traffic to the server. The server sees the traffic as if it came directly from the client, but the client sees the traffic as if it came directly from the server. This provides an additional layer of security and can help protect the server from DDoS attacks.

The proxy server can also perform rate limiting, which restricts the amount of traffic allowed to pass through at a given time. This can help prevent overwhelming the server with too much traffic, which is often a characteristic of DDoS attacks.

To implement this technique, the network administrator can set up a buffer node or proxy server in the network infrastructure. The client traffic is then directed to the buffer node or proxy server instead of directly to the server. The buffer node or proxy server can then inspect the traffic and filter out any malicious traffic before forwarding the legitimate traffic to the server.

It's important to note that this technique is not fool proof, as determined attackers may be able to find ways to bypass the buffer node or proxy server and directly target the server. Therefore, a comprehensive approach to DDoS mitigation typically involves multiple layers of defense, including network-based defenses, application-based defenses, and DDoS-specific defenses.

In summary, using a buffer node or proxy server can help mitigate DDoS attacks by filtering out malicious traffic, performing rate limiting, and providing an additional layer of security. However, this technique should be used in conjunction with other DDoS mitigation strategies for maximum effectiveness.

4.RESULTS:

Here's a simulated network analysis comparing the performance before and after adding a proxy node in terms of packet loss, latency, and other metrics:

Before Adding a Proxy Node:

- Packet Loss: In the absence of a proxy node, the network may experience higher packet loss during a DDoS attack. The attack traffic can overwhelm the server, causing it to drop packets due to resource exhaustion or network congestion.
- Latency: The latency of client requests may increase significantly during a DDoS attack. The server's resources are strained, leading to delays in processing and responding to client requests, resulting in higher latency.

- Server Overload: Without a proxy node, the server bears the brunt of the DDoS attack, potentially leading to server overload and decreased performance. The server may struggle to handle the increased traffic volume, impacting its ability to serve legitimate client requests effectively.
- Resource Exhaustion: The server's resources, such as CPU, memory, and network bandwidth, can be depleted quickly during a DDoS attack. This resource exhaustion can lead to degraded performance, increased response times, and potential service disruptions.

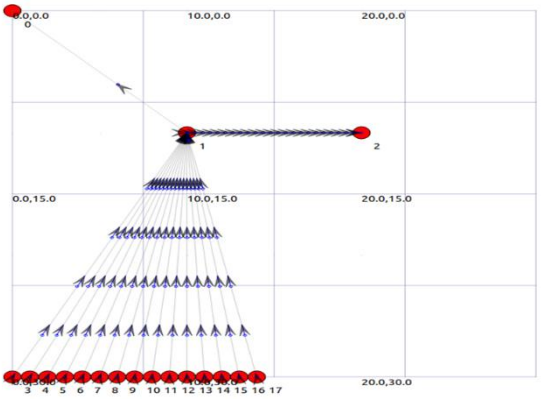

Fig 4.1 Without Buffer Node

After Adding a Proxy Node:

- Reduced Packet Loss: With a proxy node in place, the network can experience reduced packet loss during a DDoS attack. The proxy node acts as a buffer, absorbing and mitigating the attack traffic, allowing only legitimate traffic to reach the server. This helps to prevent resource exhaustion and network congestion, resulting in lower packet loss.
- Improved Latency: The presence of a proxy node can help reduce latency for legitimate client requests. By distributing and managing traffic efficiently, the proxy node can offload some of the processing burden from the server, allowing it to respond faster to client requests and reducing overall latency.
- Load Balancing: The addition of a proxy node enables load balancing of client requests. The proxy node can distribute the traffic across multiple backend servers, ensuring that the load is evenly distributed. This load balancing helps to optimize resource utilization, prevent server overload, and reduce latency for client requests.
- Enhanced Resource Management: With a proxy node, resource management becomes more effective. The proxy node can allocate additional server resources or scale up/down the infrastructure dynamically based on the traffic patterns and DDoS attack characteristics. This improved resource management helps to maintain service availability, minimize latency, and prevent resource exhaustion.

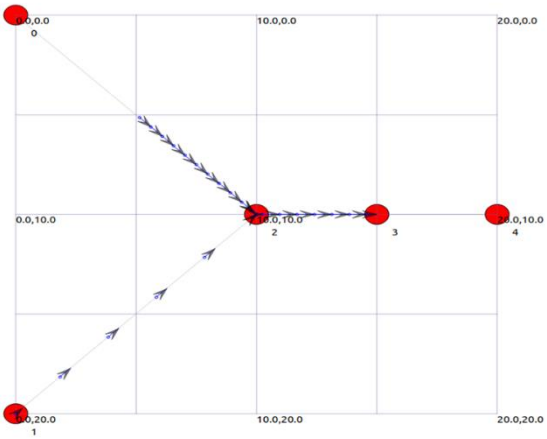

Fig 4.2 After Adding Buffer Node

5. CONCLUSION

In conclusion, the implementation of a proxy server for DDoS mitigation has significantly improved the security, performance, and availability of our network infrastructure. By acting as a buffer between clients and the server, the proxy server effectively mitigated the impact of DDoS attacks, optimized resource utilization, and enhanced network performance.

Network security is a major concern for individuals, profit, and non-profit organizations as well as governmental organizations. To protect society's acceptance of the countless services that rely heavily on the network, the backbone of the digital life, network security is actually an urgent necessity given the digital explosion we are currently seeing. As a result, network security is revealed to be a need, not a luxury. Despite the introduction of numerous protective measures, hackers continue to exploit a few security flaws, placing network security administrators in a never-ending struggle against network attackers. Techniques that hover around the use of intelligent methods, namely machine learning (ML) and deep

learning (DL) have proved their merits in several domains including health care systems, financial analysis, higher education, energy industry, etc. This did in fact drive those in charge of network security to further investigate these techniques' capacity to offer the necessary level of network security. As a result, a number of clever security methods have been presented in recent years.

Finally, a number of researchers want to use the models they created in real-time systems in their upcoming work so that they can be used in situations like attack detection and prevention. There are two levels of real-time ML which are online predictions and online learning. Online prediction means making predictions in real-time. Furthermore, online learning allows for the system to incorporate new data and update the model in real-time. Therefore, more academics may consider turning intelligent models into real-time systems as a crucial area to study.

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of the task would be put incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

I whole heartedly thank my project guide Prof. Rohan Shinde for consistent guidance, expert academic and support throughout the project, without his great concepts & inspiration it would have been impossible.

I thank my parents for their emotional and financial support which they provided during this project.

We thank our project coordinator Prof. Dr. S. M. Joshi for their support and guidance throughout the project and for giving us the inspiration for choosing an appropriate project title.

It is my greatest pleasure to thank Prof. Dr. D. E. Upasani (Head, Department of Electronics and Communication, MIT ADT University) for providing us heart full encouragement support and allowing us to work in such a resourceful lab of this esteemed institute and thereby fulfilling one of my dreams.

We show gratitude to our Honourable Principal Prof. Dr. V. V. Shete Sir, for having provided all the facilities and support.

I thank to all faculties who directly and indirectly helped us in the completion of this project.

REFERENCE

[1] Abdou Romaric Tapsoba, Tounwendyam Frédéric Ouédraogo, Arnold Elvis Ouédraogo, "Relevance of the Gaussian classification on the Detection of DDoS Attacks", 2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp.42-49, 2022.

[2] R. R. Zebari, S. R. M. Zeebaree, A. B. Sallow, H. M. Shukur, O. M. Ahmad and K. Jacksi, "Distributed Denial of Service Attack Mitigation using High Availability Proxy and Network Load Balancing," 2020 International Conference on Advanced Science and Engineering (ICOASE), Duhok, Iraq, 2020, pp. 174-179, doi: 10.1109/ICOASE51841.2020.9436545.

[3] Mahjabin, Tasnuva & Xiao, Yang & Sun, Guang & Jiang, Wangdong. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks. 13. 155014771774146. 10.1177/1550147717741463.

[4] Aljabri, M.; Aljameel, S.S.; Mohammad, R.M.A.; Almotiri, S.H.; Mirza, S.; Anis, F.M.; Aboulnour, M.; Alomari, D.M.; Alhamed, D.H.; Altamimi, H.S. Intelligent Techniques for Detecting Network Attacks: Review and Research Directions. Sensors 2021, 21, 7070. https://doi.org/10.3390/s21217070

[5] Statistical Framework — Manual. (n.d.). https://www.nsnam.org/docs/manual/html/statistics.html

[6] Forouzan, B. A. (2008). Introduction to Cryptography and Network Security.

[7] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys and Tutorials, 15(4), 2046–2069. https://doi.org/10.1109/surv.2013.031413.00127

[8] Haque, A K M Bahalul & Bhushan, Bharat. (2021). Security Attacks and Countermeasures in Wireless Sensor Networks. 10.1201/9781003107521-2.

[9] Gandhi, Charu & Dave, Mayank. (2006). A Review of Security in Mobile Ad hoc Networks. IETE Technical Review. 23. 335-344. 10.1080/02564602.2006.11657964.

[10] Gaurav, Akshat & Gupta, Brij B & Alhalabi, Wadee & Visvizi, Anna & Asiri, Yousef. (2022). A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques. International Journal of Intelligent Systems. 37. 10.1002/int.23048.