Denial of Service Attacks at the Application and Transport Layer with mitigations

Tomiwa Oladejo
School of Science and Technology
Nottingham Trent University
Nottinham United Kingdom
N0940282@my.ntu.ac.uk

***Abstract*— Distributed denial of service attacks are a method of exploitation used to bypass network security. Using malware infected systems, legitimate users are prevented from gaining access to server resources. As the expands and becomes more essential in today's society, the demand for internet safety continues to grow. This paper delves into the operations of DDoS attacks and how to mitigate it.

I. Introduction

As technology continues to advance, secure safeguarding against cyber-attacks targeted towards communications systems in telematic networks is becoming ever more vital. The OSI (open systems interconnection) model refers to the pathway of information from one data processor to another. Using the model, a set of rules and requirements have been established for the interoperability and flow of data between various software and devices within the infrastructure of a network.

Prior to the introduction of the OSI model in 1984 by the International Organization for Standardization (ISO), fundamental standard protocols to carry out functional design infrastructure and data communication were absent [1]. As a result, the installation and configuring of new equipment within existing and outside networks was a challenging task. Following the integration of the model, network administrators became capable of efficiently designing a network infrastructure with equipment qualified to proficiently communicate with universal networks.

A. The Layers of the OSI Model

The framework of the model consists of seven fundamental layers. Each individual layer is designed to execute a specific function, resulting in a smooth data flow throughout the network. Residing at the top of the model, the application layer (layer 7), the layer and end user are able to interact directly with the software application through the definition of protocols for effective user interaction [2]. Protocols such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) enable software to direct data flow towards the user. Layer 6 is the presentation layer. The role of the layer is to perform data translation on the application data into a network format based on the semantics or syntax accepted by the application [3]. The data is encrypted as it is received and then decrypted once it reaches the receiver's end. Additionally, to reduce the number of bits in exchanged data, the layer can compress data received. The session layer (layer 5) controls the communication session between different computers. Using data synchronization, data can be broken into smaller pieces through the addition of checkpoints into the data stream. Layer 4, known as the transport layer, grants safe message transfer between the sender and receiver through the management of transportation and error checking of packets [2]. The flow of data is regulated as it is divided into smaller segments upon arrival from the above layer. This verifies that data is not sent at higher speeds from devices with a good network connection. All data is then reassembled at the receiver side. The error-checking functionality ensures transmitted data is complete. A request is sent to the system by the layer for the data to be resent if the data is incomplete. Enabling the communication between multiple networks is the role of the network layer (layer 3) [6]. The data segments from the transport layer are divided into network packets. Furthermore, the data is organised into appropriate routes from the sender to the receiver to determine the most secure and efficient path for the packet's transmission. The destination is found using logical addresses, such as Internet Protocol (IP), assigning individual names to devices across the network. The transmission of data between two nodes takes place in the data link layer (layer 2) [6]. These nodes are directly connected, and the data is packaged into frames before being sent to the destination. Within the layer there are two sub-layers; media access control (MAC) and logical link control (LLC). The purpose of the MAC layer is to provide multiplexing and flow control for data transmitted across the network. LLC aids the management of packet retransmission by providing error control to the physical layer and recognizes line protocols.[1]. The Physical layer (layer 1) is responsible for transmitting unstructured data bits across the physical layer of the network. The bits can be either electrical or optical. Network adapters, cabling, network hubs or modems are some examples [3].

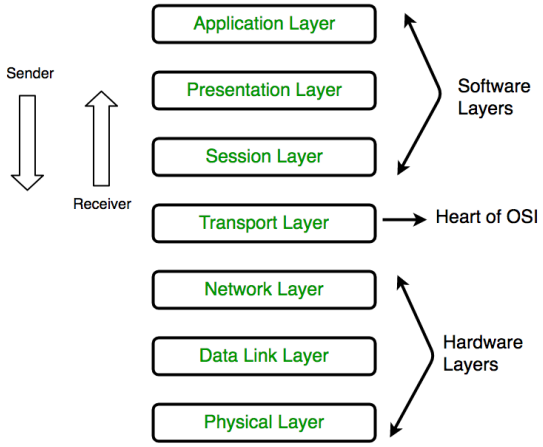

Fig. 1. The 7 OSI layers

B. What threat is there towards the OSI Model?

In order for attackers to disrupt or render the OSI model useless, distributed denial of service attacks (DDoS) attacks are employed. DDoS attacks overload and shut down a machine or network, making it inaccessible to the intended users [4]. To successfully crash the target, a flood of fake traffic is sent to the user using an army of zombie devices called a botnet [5]. Botnets. As a result of the attack, access to the server is prevented or an increase in bounce rate is caused due to the server slowing down.

Throughout this paper the structure and effect of distributed denial of service attacks targeted specifically towards the transport layer. A literature review will be conducted to assess the different forms of attacks used against the application layer and transport layer. There will be a section explaining the methodology approach used when collecting research. The mitigations found to solve the problem will be included to understand how detect threats and secure the availability of operations and services. When looking at the mitigations, it is important to look at the threats to validity and assess potential factors which may have an effect on the found solutions. Lastly, there will be a conclusion assessing the overall findings throughout the paper.

II. Literature Review

A. Literature review process

The initials step taken to conduct the literature review was the comprehension of the key research questions which should be answered through its completion. As a secondary data research method, literature reviews create a remarkable comprehension of the topic. Whilst searching for books, articles and journals concerning the topic, it was important for the sources to be reliable and contain accurate information. In order for an accurate review of the topic to be carried out, a broad collection of literature was accessed. Throughout the literature review, the operation of DDoS attacks used against the application layer and transport layer were broken down and studied in depth.

B. Review of literature

Distributed denial of service (DDoS) attacks target servers, websites or networks with the intention of making them unavailable to the users. DDoS attacks employ a diversity of different techniques to successfully produce an overwhelming force of traffic stemming from multiple sources, causing performance issues [7]. To achieve these attacks, the attacker deploys a network of computers infected with malware known as botnets. Botnets commonly include computers, IoT devices and websites. They can consist of an extremely large quantity of systems, causing the identification of the various sources of the attack to be difficult [8].

The main DDoS attack types used to classify the rest are protocol attacks, application layer attacks and volume-based attacks. Protocol attacks exploit weaknesses residing in network protocols [9]. These are protocols include UDP and TCP/IP and result in the targeted system crashing. Application layer attacks are used to target application such as HTTP-based websites. The application code is exploited, or the server is overloaded with requests, ultimately blocking legitimate users from server access. Volume-based attacks deplete the bandwidth of the server using relentless amounts of traffic. The aftermath of distributed denial of service attacks are inclusive of the obstruction of important services, loss of revenue and, damage to reputations [9].

The duty of the transport layer is to successfully transfer data between applications. A frequent attack used to disrupt the flow of traffic is the SYN flood attack. During this attack, an overwhelming number of SYN packets are sent. In turn, the available ports on the targeted server machine are overloaded, stalling the server's processing capabilities.

The method of the TCP SYN attack is the exploitation of the TCP's three-way handshake mechanism [9]. For a connection to be successfully established, continuous acknowledgements are mandatory from both parties. This is known as the three-way handshake. Paper [10] states at the start of the handshake, a SYN packet is sent from the client to the sever. As a response to the packet, the server, a SYN + ACK packet is sent back to the client [11]. When the SYN + ACK packet is obtained by the client, the ACK packet is sent back, accomplishing the connection through the completion of the handshake. In order for the sever to search and confirm the client's identity, the intermediate states are kept by the server within the memory stacks until a connection is achieved [10]. The exploitation involves flooding the server's memory, ultimately causing the server to deny requests from legitimate users. By intentionally creating a substantial total of incomplete connections, the attacker is able to flood the server's memory. Incomplete connections are made by spoofing the source with non-existing IP addresses, using the spoofed IP addresses to send the SYN packets. After the packets are acquired, the server attempts to send SYN + ACK packets to the client. However, the as the IP is non-existent, the ACK packets are never sent back [10]. The server continues to wait to receive the ACK packets, resulting in the ports becoming overloaded and blocking legitimate users from access. Machines using real IP addresses are also capable of this attack. During these cases the SYN + ACK message is disregarded, creating the same effect.

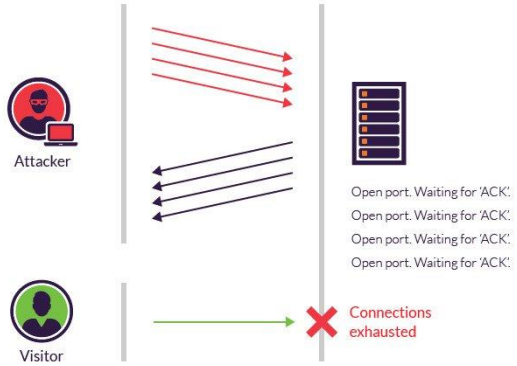

Fig. 2. TCP SYN attack

Paper [12] states scenario of a TCP PUSH + ACK attack, manipulated botnet agents are used to send a sizeable amount of TCP packets. The PUSH and ACK bits of the header are also set to "1", coercing the target into clearing its memory stack and send the client its acceptance [12]. The constant flood of these messages drains the CPU processing power, resulting in a system overload. As the system is inoperable, connections are unable to be established with legitimate users [10].

UDP flood attacks occur on the transport layer. During this attack, the target server is flooded with a large number of UDP packets [11]. As a result of the flooding, the server resources are depleted, preventing responses to legitimate requests. Services that depend on VoIP, UDP and DNS are the most vulnerable to this attack [10].

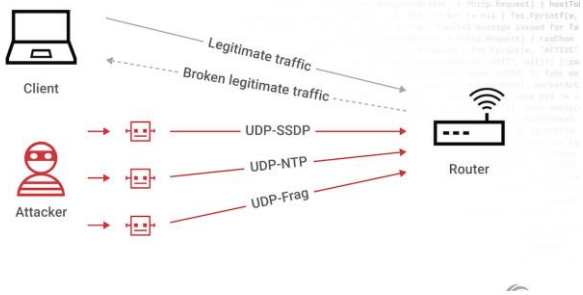

Fig. 3. UDP flood

HTTP flood attacks exploit the application layer using resource depletion [12]. According to [9] HTTP protocol is exploited through the HTTP GET and HTTP POST requests. The requests are manipulated whilst communicating to a server. For the attack to be executed, a TCP connection to a valid IP address is necessary [10]. The IP addresses of the botnets are used to successfully create these connections. The attacker then carries out a HTTP GET request for a large file to be downloaded. The botnets are employed to dispatch a high number of requests [13]. As a response to the requests, the server is obligated to read the file from the back-end storage and store the file into working memory. Additionally, it must break the file down into numerous packets so it can be sent. The process results in the CPU processing power and memory becoming overloaded, flooding the systems resources [10]. Legitimate users would be unable to receive a response from the server due to extreme the traffic. By resolving the link attached to the response and following the links, the attacker make the generated traffic appear as regular traffic. The utilization of this method is capable of achieving a higher probability of bypassing detection.

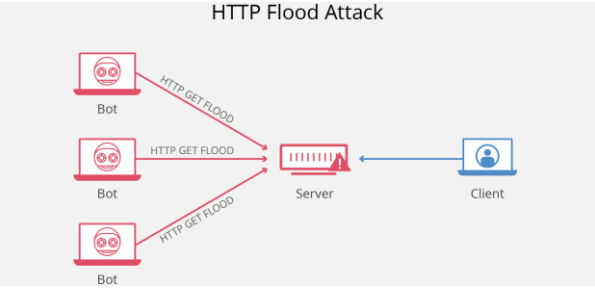

Fig. 4. HTTP flood

The application protocol SIP is vulnerable to exploitation through a SIP flood. This protocol is adopted in voice over IP (VOIP) call setup. Similar to the HTTP flood, this attack takes advantage of resource depletion by flooding the target with request and call messages. The SIP call control messages consist of SIP NOTIFY, SIP INFO and SIP RE-INVITE [9]. The different request messages are SIP REQUEST and SIPINVITE. Using these messages, the attack aims to flood the SIP registration server (SIP REGISTRAR) or the proxy server in order to deplete the network bandwidth, CPU and memory with botnets [9]. As the SIP registrar server is responsible for accepting all REGISTRAR requests, it has to respond to the multitude of requests being received from the botnets [10]. Moreover, the parameters of the user agents and the addresses are required to be documented. The immense influx of requests causes legitimate users to be denied access to the server.

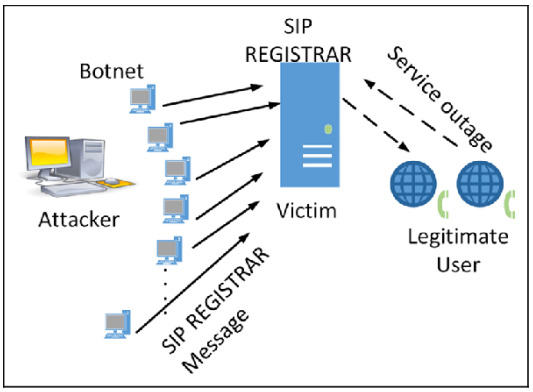

Fig. 5. SIP flood

Slowloris employs a different method to the other flood attack. The DDoS method uses a single machine to shut down the victim [9]. To begin the attack a partial HTTP request is sent. The header information is sent afterwards routinely so the sockets remain open [14]. This action results in the consumption of the sockets, causing legitimate clients to be declined by the server.

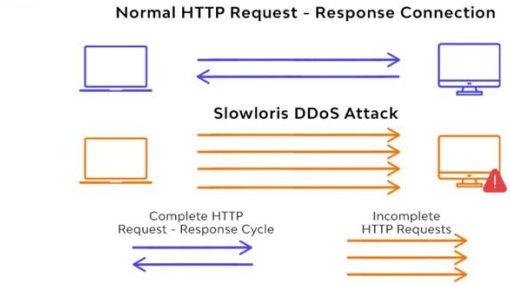

Fig. 6. Slowloris attack

A slow read attack establishes a connection using a valid HTTP request [15]. However, to prolong the request the attacker intentionally reads the response extremely slowly. After a number of requests such as that, the server becomes inaccessible to legitimate users.

R.U.D.Y. (R-U-DEAD-YET?) is another slow request attack which uses the submission form fields of websites for exploitation. During this attack, multiple parallel HTTP POST connections are opened [10]. The information is submitted within a 1-byte sized packet at an extremely slow rate. Due to the tremendously slow rate of submission, the connection continues to stay open. Consequently, the server is overloaded and crashes [9].

III. METHODOLOGY

In order to gather research on the topic, a literature review-based methodology was adopted. This methodology involves reading through, analyzing and sorting literature, leading to the identification of the essential attributes of the materials. As the literature review was being carried out, relevant material was selected by filtering out papers which did not meet any of the question's criteria. The secondary data research method made a number of perspectives relating to the topic accessible, providing a clearer understanding of the answers to the research questions. As there is a wide range of data already available, the breadth and depth of the topic can be delved into, assisting the research paper. Libraries such as IEEE, google scholar, science direct, ResearchGate, IJERT

and hindawi were used as they are viewed as reliable sources. To locate different aspects of topic information within these resources, various search strings were applied. These search variations caused deeper subject knowledge to be accessible. Correspondingly, this led to the chosen research questions established from the beginning to be answered in addition to a solid conclusion.

IV. Defence Mechanisms

After reviewing the effects which distributed denial of service attacks have on the network, the prevention methods and mitigation techniques proposed by a few authors were looked into.

In resource [11] Ingress/egress filtering is a filtering technique used to prevent traffic containing a spoofed IP address from entering the network. Ingress filtering filters malicious traffic on the pathway to a local network. Whereas egress filtering discards the traffic leaving the network. A sufficient number of DDoS attacks utilizing spoofed IP addresses are preventable with the employment of this filtering technique. According to RFC 2267, ingress filtering gives permission for the entry of traffic into the network if it matches a predefined range of domain prefix of the network. As a result, if the attacker uses a spoofed IP address which mismatches the prefix, it is discarded in the routers. An understanding of the expected range of IP addresses for a port determines the methods effectiveness [10]. The complex topologies applied in various networks can cause difficulty in this area when attempting to gather information of the IP ranges. However, if the spoofed IPs are in the valid address range, the attacker is able to bypass the routers defences. In the scenario where valid IP addresses of botnets are being used as the source IP, the technique ceases to be impactful.

Another defence mechanism is TCP SYN cookies [16]. Crafted SYN-ACKs are used to respond to TCP SYN requests without the creation of a new TCB (contains information about the connection state) for the connection. Only after the client responds to the crafted response, a TCB is created. The backlog queue can also be increased.

A mitigation against the HTTP flood is the web application firewall. The firewall aids web applications by filtering and monitoring the HTTP traffic being transmitted between the internet and web application. Polices are a set of rules used by the firewall. These are beneficial as policy modifications, such as rate limiting, can be administered in a short period of time. Due to this feature, response speeds to different attack vectors are swifter.

When it comes to DDoS attack, rate limiting and/or filtering is a highly practical approach. System's decipher which technique to incorporate in accordance to the results received from the detection mechanisms. In the situation malicious and legitimate traffic are not differentiable between or large false negatives are produced, rate limiting is the better option. Filtering is more suitable if the attack flow is distinguishable, as the malicious traffic can then be filtered.

Limiting the response rate of ICMP packets is applicable as a mitigation towards UDP floods [10]. However, a drawback of this method is legitimate packets can potentially be caught in the course of filtering. When the flood reaches the point of saturating the state table of the server's firewall, any server level mitigation's will not be adequate enough.

As slowloris is a bandwidth flooding attack, it aims to congest the resource. Congesting policing mechanisms can be implemented for the reduction or elimination of the attacks effect. Example mechanisms where the policing is utilized are NetFence and Re-feedback [17]. Restrictions for a minimum transfer speed allowed and rate limiting incoming requests are also effective.

MANAnets reverse firewall filters the outgoing packets leaving a network. This method guards against packet flooding attacks deriving from within a network, making it potent against DDoS attacks that originated from within a network. The firewall causes the rate at which the packets are transmitted for the transmitter engine (the attacker) to be limited. However, during runtime the configuration is not dynamically changeable. Additionally, the administrator's presence is mandatory as the reverse firewall is not automatic.

Implementation of rate limiting in addition to observations are suitable methods as mitigation against slow HTTP attacks. Limiting the rate of incoming data and denying HTTP connections without support are examples of effective measures. Another protective step is the limitation of the messages body or header length.

Paper [9] proposes the use of Path Identifiers (PIDs) as interdomain routing objects, so they can be employed as a prevention technique against flooding attacks. This method is a deterministic approach which stamps packets with an identifier depending on its travelled path [10]. The same identifiers are assigned to packets which travel the same path. As a result, packets sent by the hacker can be filtered once they are identified. However, as it operates within a small sized identification field there is the possibility of false-negative and false-positive results [10].

V. Threats to validity

When looking at the research conducted, it is important to evaluate the factors which may affect how accurate and effective the research could be.

When the selection of the data is being taking place, there may have been biases surrounding the selection of the research material. These may have been formed during the selection of material as a means to portray certain information, causing the incorrect classification of publication and inaccurate data. As the filter process is manual, the researcher holds all authority over which data is deemed suitable for the research. Consequently, this can result in failure to accurately cover the scope of the topic. This leads to another threat of incomplete research.

Furthermore, as others attempt to carry out the same study, they may utilize different methods. Varying research methods can lead to different results. For example, if someone was to conduct primary research supposed to the method of secondary data applied in this paper, the outcome would be dissimilar.

Lastly, the appliance of different online libraries is an additional threat to validity. A non-identical pool of sources can result in a different set of data being discovered. This could create an inconsistency across the board if a comparison was to be made.

VI. Conclusion

To conclude, throughout this research paper different types of DDoS attacks used to penetrate layer 7 and layer 4 of the

OSI model have been studied in depth. Distributed denial of service attacks poses a threat to the internet's reliability and security with no one solution to prevent them from occurring across the board. With each attack, whether it is an application layer attack, volumetric attack or protocol attack, a different form of defense is required. Consequences of being a victim to a DDoS attack include a negative impact on the future of companies as it has been displayed there are security flaws and an economic loss to the victim as services are inaccessible during the attack. However, there are a number of methods and techniques available as defense mechanisms. This paper is important as there is a growing need for higher level of security across the network. In the future new attacks may surface in attempt to terrorize the internet. With the ever-rising use of networks, it is vital for the appropriate security measures to be put in place to mitigate these inbound threats.

REFERENCES

[1] Kanade, V. (2022). What Is The OSI Model? Definition, Layers, and Importance |. [online] Spiceworks. Available at: https://www.spiceworks.com/tech/networking/articles/what-is-osi-model/ [Accessed 20 Mar. 2023]. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Forcepoint (2018). What is the OSI Model? [online] Forcepoint. Available at: https://www.forcepoint.com/cyber-edu/osi-model#:~:text=The%20OSI%20Model%20(Open%20Systems [Accessed 20 Mar. 2023]. K. Elissa, "Title of paper if known," unpublished.

[3] S, D.E.L. (2021). Common TCP/IP OSI layer attacks. [online] Medium. Available at: https://systemweakness.com/common-tcp-ip-osi-layer-attacks-51e4b9f99fb1 [Accessed 20 Mar. 2023].

[4] Globaldots, A. (2018). DDos Quick Start Guide. [online] GlobalDots. Available at: https://www.globaldots.com/resources/blog/ddos-quick-start-guide/#:~:text=Transport%20Layer%20(4) [Accessed 20 Mar. 2023].

[5] Sucuri. (n.d.). What is a DDoS Attack? Types & Best Prevention Methods. [online] Available at: https://sucuri.net/guides/what-is-a-ddos-attack/#:~:text=Introduction [Accessed 20 Mar. 2023].

[6] Imperva (2021). What is OSI Model | 7 Layers Explained | Imperva. [online] Learning Center. Available at: https://www.imperva.com/learn/application-security/osi-model/ [Accessed 21 Mar. 2023].

[7] Reena, Singh, Y. and Chaudhary, S. (2018). A Defense Strategy for DDoS flooding Attacks. *International Journal of Engineering Research & Technology*, [online] 3(10). doi:https://doi.org/10.17577/IJERTCONV3IS10111.

[8] Manavi, M.T. (2018). Defense mechanisms against Distributed Denial of Service attacks : A survey. *Computers & Electrical Engineering*, 72, pp.26–38. doi:https://doi.org/10.1016/j.compeleceng.2018.09.001.

[9] Cheema, A., Tariq, M., Hafiz, A., Khan, M.M., Ahmad, F. and Anwar, M. (2022). Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review. *Security and Communication Networks*, 2022, pp.1–15. doi:https://doi.org/10.1155/2022/8379532.

[10] Mahjabin, T., Xiao, Y., Sun, G. and Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, [online] 13(12), p.155014771774146. doi:https://doi.org/10.1177/1550147717741463.

[11] kumarasamy, S. (2011). Distributed Denial of Service (DDOS) Attacks Detection Mechanism. *International Journal of Computer Science, Engineering and Information Technology*, 1(5), pp.39–49. doi:https://doi.org/10.5121/ijcseit.2011.1504.

[12] Gaurav, A., Gupta, B.B., Alhalabi, W., Visvizi, A. and Asiri, Y. (2022). A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques. *International Journal of Intelligent Systems*, 37(12), pp.11407–11431. doi:https://doi.org/10.1002/int.23048.

[13] Verma, A. (2016). *A Survey on HTTP Flooding Attack Detection and Mitigating Methodologies*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/309385762_A_Survey_on_HTTP_Flooding_Attack_Detection_and_Mitigating_Methodologies [Accessed 23 Mar. 2023].

[14] Sabri, S. (2021). *Slowloris DoS Attack Based Simulation*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/349328456_Slowloris_DoS_Attack_Based_Simulation [Accessed 23 Mar. 2023].

[15] Park, J., Iwai, K., Tanaka, H. and Kurokawa, T. (2014). *Analysis of Slow Read DoS attack*. [online] IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/6979803 [Accessed 23 Mar. 2023].

[16] Islam, M.N.U., Fahmin, A., Hossain, Md.S. and Atiquzzaman, M. (2020). Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques. *Wireless Personal Communications*, 116(3), pp.1993–2021. doi:https://doi.org/10.1007/s11277-020-07776-3.

[17] Liu, X. (2010). https://www.researchgate.net/publication/46582342_NetFence_Preventing_Internet_Denial_of_Service_from_Inside_Out.

[18] HTTP Flood DDoS Attack | Cloudflare. (n.d.). *Cloudflare*. [online] Available at: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/ [Accessed 27 Mar. 2023].

[19] GeeksForGeeks (2019). *Layers of OSI Model - GeeksforGeeks*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/layers-of-osi-model/ [Accessed 27 Mar. 2023].

[20]