International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 12 | Dec - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

DDOS Attacks and Analysis of Different Defense Mechanisms

Chinmayee Mishra, Pullam Bhatla Laxmi Sindhu, Pruthwiraj Mohanty, Ayush Kumar Samrat

Department Of Computer Science

Centurion University, Bhubaneswar, India

ABSTRACT

Denial of Service(DOS) attacks are an immense trouble to internet spots and among the hardest security problems in moment's Internet. Of particular concern- because of their implicit impact- are the Distributed Denial of Service(DDoS) attacks. With little or no advance advising a DDoS attack can fluently exhaust the computing and communication coffers of its victim within a short period of time. This paper presents the problem of DDoS attacks and develops a bracket of DDoS defence systems. Description of each attack and defence system order is provided ,along with the advantages and disadvantages of each approach. The purpose of the study is to organise the existing attack and defence mechanisms to improve knowledge of DDoS attacks and develop more potent defence strategies. In this work, the types of attacks, test characteristics, evaluation techniques are classified and delineated in the review; evaluation methods and test materials used in the methodology of the proposed strategic strategy. Finally, this work provides guidance and possible goals in the struggle to create better events most threat Types of cyber-attacks, or DDoS attacks.

1. INTRODUCTION

Attacks involving denial of service (DOS) pose a serious issue for the Internet. The effects of DOS assaults have been amply. documented in the literature on computer networks. Instead of compromising the service itself, the major goal of the DOS is to interrupt services by attempting to restrict access to a system or service. By focusing on the network's connectivity or bandwidth, these attacks seek to prevent a network from offering standard services. These attacks succeed by bombarding the victim's network or computing power with a steady stream of packets. Attacking Internet resources via Distributed Denial of Service (DDoS) is a relatively easy yet effective technique. DDoS attacks provide the DOS problem a many-to-one dimension that makes avoidance more challenging and the impact proportionally more severe. DDoS streams don't seem to have any traits that might be directly and effectively exploited for their detection. By discussing the issue of DDoS attach and suggesting a taxonomy of the defence methods that might be applied to thwart these attacks, we strive to bring some structure to the DDoS sector in this work. We specify distinctive and significant traits for each defence mechanism. Our goal is to outline the issues currently being experienced so that DDoS attacks can be better understood, and more effective defence strategies can be developed. The biggest security risk to the Internet is the distributed denial of service assault. Even with security safeguards in place, the network is always open to this kind of attack. This research will concentrate on the methods for DDOS attack detection and the subsequent inception of defence mechanisms. Understanding DDOS assaults and identifying security measures are the major goals.

2. DOS ATTACKS

A DOS attack is one that is intended to prevent a computer or network from offering standard services. Only when access to a computer or network resource is purposefully restricted or compromised as the result of malicious action conducted by another user is a DOS attack deemed to have occurred. Although they may not directly or permanently harm data, these attacks may jeopardise the resources' availability. DOS attacks fall into the following categories:

Network Device Level: DOS attacks that take use of software flaws or attempt to deplete the hardware resources of network devices are classified as Network Device Level attacks.

OS Level: DOS attacks at this level take advantage of how operating systems carry out protocols.

Application-based assaults: Many attacks attempt to put a computer or a service out of commission by either exploiting flaws in network apps that are running on the target host or by leveraging such applications to drain the victim's resources.

Data flooding: An attacker may try to exhaust all the network, host, or device's available bandwidth by transmitting tremendous volumes of data, forcing it to process enormous amounts of data.

Attacks based on protocol properties: DOS can survive advantage of certain features of the standard protocol, for example, several attacks benefit from the fact that the IP source addresses can be spoofed.

3. DDOS ATTACKS

3.1 . Definition and strategy of DDoS attacks

A DDoS attack uses multiple computers to launch a coordinated DOS attack against one or more targets. using client/server technology, the author can greatly increase the efficiency of DOS the destruction of several ignorant complicit means computers that act as attack platforms. A DDoS attack is composed of four elements, as illustrated in Figure 1:

- The real attacker.
- The handlers or master compromised hosts, who can control multiple agents.
- Attack demonic agents or zombie hosts responsible for creating packets directed at the intended victim.
- A victim or target host

A DDoS attack can be described as:

Recruitment: The attacker recruits vulnerable agents, which he used to attack.

Compromise: An attacker exploits security holes agents and plant attack codes protecting it detection and deactivation at the same time.

Communication: Agents communicate with the attacker handlers that they are ready.

Attack: The attacker determines the beginning of the attack. Advanced and powerful DDoS tools are available to potential attackers increases the risk a victim of a DOS or DDoS attack. Some the most famous DDoS tools are Trinoo, TFN, Stacheldraht, TFNZK, mstream and Shaft.

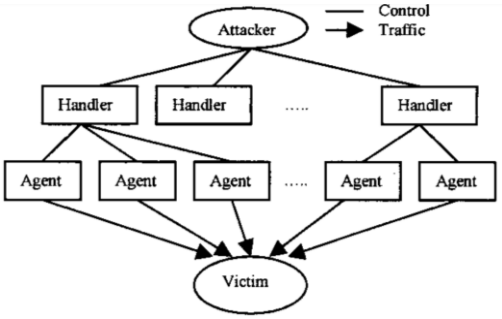

Fig 1 . Architecture of DDoS attacks

3.2. The Most common types of Attacks

SYN flood attack : A SYN attack occurs when a SYN packet hits the system and is initiated by an incomplete connection a request that no longer meets the actual communication requirements resulting in a service failure (DOS). Figure 2 below shows the SYN flood design.

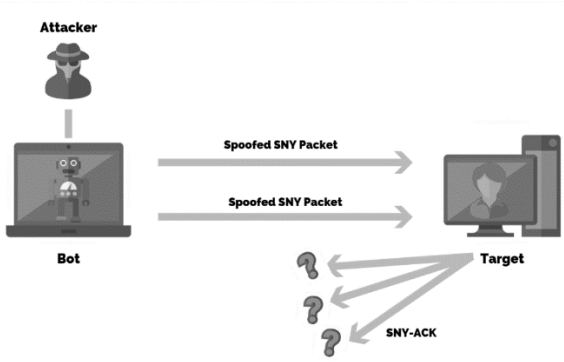

Fig 2. The architecture of SYN Flood Attack

ICMP Flood : An Internet Control Message Protocol (ICMP) flood attack is a common distributed denial of service (DDoS) attack in which malicious actors attempt to flood a server or network device with ICMP ping or echo request packets. ICMP ping is usually used to check the status of the device and its connection. By overwhelming the target device with ICMP flood DDoS attacks, the device loses its ability to respond with the same number of response packets, which consumes too many resources and legally disables the device. The architecture of ICMP attack is illustrated in the below Figure 3

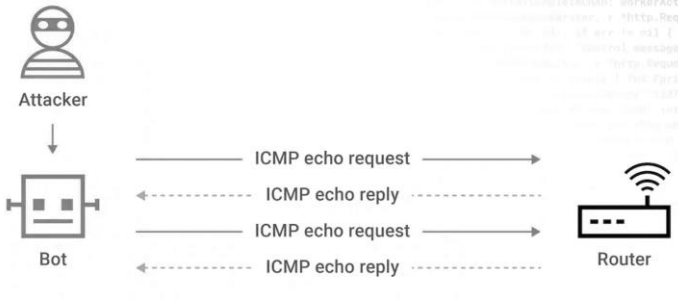

Fig 3. Architecture of ICMP attacks

UDP Flood Attack : UDP flooding is a type of denial-of-service attack in which malicious actors can spoof the source IP address and create User Datagram Protocol (UDP) packets to the target server. If the server cannot find the application associated with the UDP packets, it responds with a "destination unreachable" packet. If the number of UDP packets received and responded to is too large for the server, the system will be overloaded and will not be able to serve requests from legitimate clients and users. The architecture of UDP attack is illustrated in the below Figure 4.

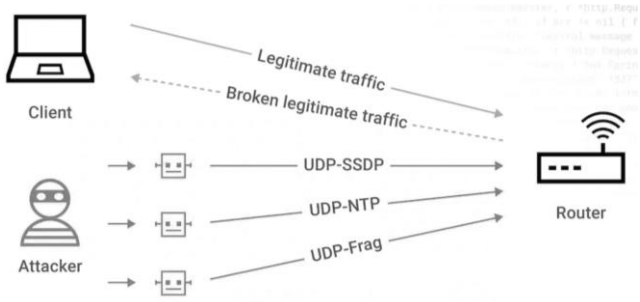

Fig 4. The architecture of UDP Flood Attack

4. DEFENCE MECHANISM

Network-based Defence Mechanisms

Network-based defences are designed to protect network infrastructure against DDoS attacks. These mechanisms include firewalls, intrusion detection/prevention systems, and routers that can filter traffic based on certain criteria. Firewalls are an integral part of network security and can be configured to block traffic from specific IP addresses or ports. Intrusion detection and prevention systems can detect and block malicious traffic, and routers can be configured to limit the number of requests from a single source.

Application-based Defence Mechanisms

Application-specific defences are designed to protect specific applications against DDoS attacks. These mechanisms include load balancers and web application firewalls, which can mitigate DDoS attacks by distributing traffic across multiple servers, filtering malicious traffic, and limiting the number of requests from a single source. Load balancers distribute traffic among multiple servers, which ensures that no server is left with traffic. Web application firewalls can filter malicious traffic based on certain criteria, such as IP addresses or traffic patterns.

Cloud-based defences

Cloud-based defences are a newer approach to DDoS defence that leverages the scalability and flexibility of cloud computing to protect against DDoS attacks. These mechanisms include content delivery networks (CDN) and cloud-based DDoS protection services that can detect and mitigate DDoS attacks in real time. CDNs distribute traffic across multiple servers, ensuring that no single server is overloaded with traffic. Cloud-based DDoS protection services use machine learning algorithms to detect and mitigate DDoS attacks in real time.

Hybrid defence mechanisms

Hybrid defences combine the strengths of web-based, application-based, and cloud-based defences to provide comprehensive DDoS protection. These mechanisms can detect and mitigate DDoS attacks at multiple layers of the network, providing better protection against sophisticated attacks. For example, a hybrid defence mechanism might use a web-based firewall to block traffic from known malicious sources, an application-based load balancer to distribute traffic across multiple servers, and a cloud-based DDoS protection service to detect and mitigate advanced attacks.

5. DDOS ATTACK DEFENCE METHODS

5.1. THE ANALYSIS OF THE DEFENSE METHODS

DDoS attacks face many problems and challenges that are very difficult to solve and understand. Essentially unusual DDoS attacks have no regular and identifiable characteristics.

Shiaeles et al.[1] in an earlier work. A DDoS attack detection point is ready, and limits have been improved as much as possible using atypical assessments of hairy attacks. Evaluation is done as a standard package between arrival times. The problem is divided into two parts, namely DDoS attack detection and identifying the IP of the victim. The location of the attack is determined using very strict thresholds and the IP address of the victim is identified with acceptable allowed requirements that can be quickly identified. the victim's IP address. This in turn requires malware that attacks host computers and uses a skin time as a packet as a necessary measure to detect DDoS attacks.

According to ***Rahul et al. [2]*** use GA to distinguish real users and reduce the distance between VoIP and SIP traffic. The VoIP Flood Guidance Framework (VFD) is used to detect both SIP and TCP flood attacks. In SIP devices using the Hellinger separation fast method. In addition, the methods and techniques of Jacobi Quick The correction uses Guide and Hellinger distance calculation, which is a numerically inconsistent technique as much as possible and find a traffic jam.

Chambers et al [3] provide an advanced NLP neural network program that detects DDOS attacks using only the Internet. network as support. Systematic private networks usually delay the detection of attacks. In this way, a system that uses free information to define the system can better respond to a large-scale attack against various management services. The NLP model is considered a significant percentage of the state of system management in the use of online life. They are looking for two training models for this: a feedforward neural system and an incomplete LDA framework. Both models produced the previous work at a high margin (20% F1 points).

Juneja et al. [4] proposes a multi-agent scheme for source isolation, protection, and monitoring of DDoS attacks. This configuration makes it clear where DDoS attacks are coming from, but some operators need to get the best results. The table shows the analysis of defence technology.

Guang Yao et al. [15] Provided by Passive IP Traceback (PIT), which tracks Scams are based on pathos backscattered messages and public messages available information. The paper illustrates the reasons, collection and path backscatter statistical results. The paper presented two efficient algorithms for implementing PIT in large-scale networks and proved their correctness. This proposed mechanism will certainly not work for everything attacks and can't catch all the rogues, but it can be done say

something about phishing attacks. The table [1] shows the analysis of defence technology.

Ref	Methods	Advantages	Disadvantage
Shiaeles et al.	Real-time ddos attack detection approaches	It has ddos detection capability and identify malicious Ip addresses in real time.	It is inefficient in handling fog computing. Also, difficulty detecting an attack at leave before the attack
Rahul et al	VoIP flood detection system	It is fast and accurate detect ddos attacks.	It is inefficient against fc.
Chambers et al.	The neural language processing model	It is very effective in defence against ddos attacks.	It is limited to certain types of attacks
Juneja et al.	An agent-based framework to counterattack ddos attacks	It can monitor from a distance different type of source ddos attacks.	How much is not yet certain software agents should be used to function optimally.
Guang Yao et al.	ICMP message–based attack source detection	Simple and compatible with existing protocols. It is possible	Authentication is required for the message
		to implement a phased deployment	

Table 1. THE ANALYSIS OF THE DEFENSE METHODS

5.2. HOW TO IMPROVISE AND PREVENT THE DRAWBACKS

Improve accuracy: To avoid over blocking, protection mechanisms should be designed to minimize the number of false positives. This can be done using more sophisticated algorithms that can more accurately distinguish between legitimate and malicious traffic.

Scalability: To deal with large-scale ddos attacks, defences should be designed to be easily scalable. One way to achieve this is to use cloud-based protection solutions that can provide power when needed.

Simplify: Defences should be usable, easy to use and easy to use. This can be achieved by using automated tools that can handle much of the system configuration and management.

Cost: Costs can be reduced by deploying a combination of on-premises and cloud-based defences tailored to an organization's specific needs. This can help ensure the protection of an organization while minimizing costs.

Continuous Update: Defences must be updated regularly to keep up with evolving attack techniques. This can be achieved by staying abreast of new threats and using a combination of human intelligence and machine learning to identify and mitigate new attack methods.

Latency: To minimize latency, defences should be designed to operate as close to the target system as possible, minimizing the impact on system performance.

Comprehensive approach: a comprehensive defence mechanism should be designed to protect

against all types of ddos attacks, including volume attacks, protocol attacks and application-level attacks. This requires a multi-layered approach that includes network and application-level security.

6. Conclusion

The purpose of this article is to understand current security issues and provide a brief overview of available solutions for various security systems and approaches. In addition, the study includes a total of 15 review and research articles. This OSI layer applies to networks, servers, network management, Internet of Things, cloud computing, and all devices that have Internet connection. The report provides a comprehensive and detailed step-by-step overview of the robust methods used to detect and block DDoS attacks. Finally, this article aims to help develop modern and effective defence strategies against DDoS attacks. In addition, the configuration of the DDoS attack component includes updates and endless improvements to deal with new and sophisticated new threats.

7. Reference

1. S. Shiaeles, V. Katos, A. Karakos, and B. Papadopoulos, "Real time DDoS detection using fuzzy estimators," computers & security, vol. 31, pp. 782-790, 2012.
2. A. Rahul, S. Prashanth, S. Kumar, and G. Arun, "Detection of Intruders and Flooding In VoIP Using IDS, Jacobson Fast And Hellinger Distance Algorithms," IOSR Journal of Computer Engineering (IOSRJCE), vol. 2, pp. 30-36, 2012.
3. N. Chambers, B. Fry and J. McMasters, "Detecting Denial-of-Service Attacks from Social Media Text: Applying NLP to Computer Security," In Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers) (Vol. 1, pp. 1626-1635). (2018).
4. D. Juneja, R. Chawla and A. Singh, "An Agent-Based Framework to Counterattack DDoS Attacks," International Journal of Wireless Networks and Communications, vol. 1, p. 193, 2009.
5. K. Igor and A. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms," International Journal of Computing vol. 4, pp. 113-123, 2014.
6. K. Sharma and B. Gupta, "Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defence Mechanisms in Present Era of Smartphone Devices, "International Journal of E-Services and Mobile Applications (IJESMA)," vol. 10, pp. 58-74, 2018.
7. A. Saied, R. Overill and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," Neurocomputing, vol. 172, pp. 385-393, 2016.
8. K. Prasad, A. Reddy, and K. Rao, "DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey," Global Journal of Computer Science and Technology, 2014.
9. N. Z., Bawany, J. A., Shamsi & K. Salah, "DDoS attack detection and mitigation using SDN: methods, practices, and solutions ". Arabian Journal for Science and Engineering, 42(2), 425-441, 2017.
10. J. Ye, Cheng, X., J. Zhu, L. Feng & L. Song, "A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018.
11. Z. Tan, A. Jamdagni, X. He, P. Nanda, & R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis, ". IEEE transactions on parallel and distributed systems, 25(2), 447-456, 2013.
12. J. Gonzalez, M. Anwar and J. Joshi, A trust-based approach against IP-spoofing attacks," In Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on (pp. 63-70). IEEE. (2011, July).

13. A. H. Azizan, S. A. Mostafa, A. Mustapha, C. F. M. Foozy, M. H. Abd Wahab, M. A. Mohammed, and B. A. Khalaf," A Machine Learning Approach for Improving the Performance of Network Intrusion Detection Systems," Annals of Emerging Technologies in Computing (AETiC), 5(5), 2021.
14. N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera, and A. Skarmeta," Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence", Journal of Network and Computer Applications, 173, 102871, 2021.
15. Guang Yao, Jun Bi, Senior Member, Ieee, And Athanasios V. Vasilakos, Senior Member, Ieee "Passive Ip Traceback: Disclosing The Locations Of Ip Spoofers From Path Backscatter" Ieee Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015