International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review of Defense Mechanisms against Distributed Denial-of-Service (DDoS) Attacks on the Application Layer, as well as Machine Learning (ML)-based Mechanisms to Defend Against DDoS Attacks

Dharmesh Dhangar [1], Dr. Vikram Agrawal[2]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: DoS attacks at the application layer are made possible by flaws in the implementation or design of protocols. In contrast to volumetric DoS attacks, these assaults are covert and aim at a particular program that is currently running on the victim. Numerous attacks on commonly used protocols at the application level have been discovered in recent years. In this paper, we provide a structured and thorough review of current application-level DoS risks and ways to mitigate them. Existing attacks and defenses are broken down into distinct groups, detailed in-depth, and contrasted using significant indicators of performance. The paper ends with suggestions for additional research.

***Keywords*:** *Distributed Denial-of-service attacks; Intrusion detection systems; Firewalls*

1. Introduction

For the past two decades, network managers have been concerned about denial-of-service (DoS) assaults and their version, Distributed Denial-of-Service (DDoS) attacks. These attacks are designed to deplete resources (memory, CPU cycles, and network bandwidth) and make them inaccessible to legitimate users, therefore breaching one of the most important aspects of cyber security: availability. From the malicious client's standpoint, launching a DoS attack often takes less bandwidth, and so can be established with a small number of devices. A DDoS attack, on the other hand, necessitates flooding the victim with packets. A DDoS attack can be launched in two ways by a rogue client. The malicious client transmits a flood of packets using faked IP addresses in the first technique (e.g., amplification/reflection attacks [1]). In the second approach, the malicious client takes control of a large number of bots that have been infected with malware and instructs them to overwhelm the victim with packets. Attacks are carried out for a variety of reasons by hacking groups. These might range from simple acknowledgment in underground communities to financial incentives offered by businesses to carry out these attacks against possible market competitors. DDoS assaults target network equipment and infrastructure in order to disrupt its victims' connectivity. These attacks have been well-known in the community for some time, and various surveys have been released to address them [2].

DDoS (Distributed Denial of Service) assaults are a type of collaborative attack in which attackers attempt to compromise internet security by disrupting services. In this attack, the attacker takes advantage of compromised systems to deny legitimate users access to server resources and to launch a series of attacks against the target. This research looked at DDoS assault defensive mechanisms that are useful on the internet. The mechanisms were divided into two layers: the network/transport layer and the application layer. The network/transport layer 6 is then broken down into four categories: source-based, network-based, destination-based, and hybrid. Destination-based and hybrid mechanisms are the two types of application layer methods. We looked at key advancements in each of the above-mentioned classes and identified new obstacles. This research report offers a comparison of the above-mentioned categorizations of processes based on features of detection, defense, and responses.

[1]*Ph.D. Research Scholar, Department of CE/IT Engineering, Gujarat Technological University, Ahmedabad, Gujarat,India.*
ORCID ID: 0009-0002-0354-2377
[2]*Assistant Professor, Department of Computer Engineering, Bhailalbhai & Bhikhabhai Institute of Technology, Anand, Gujarat,India.*
ORCID ID: 0000-0001-9408-4919
* *Corresponding Author Email: [1]dharmesh.dhangar94@gmail..com*

General Architecture of DDoS Attack [3]**:**

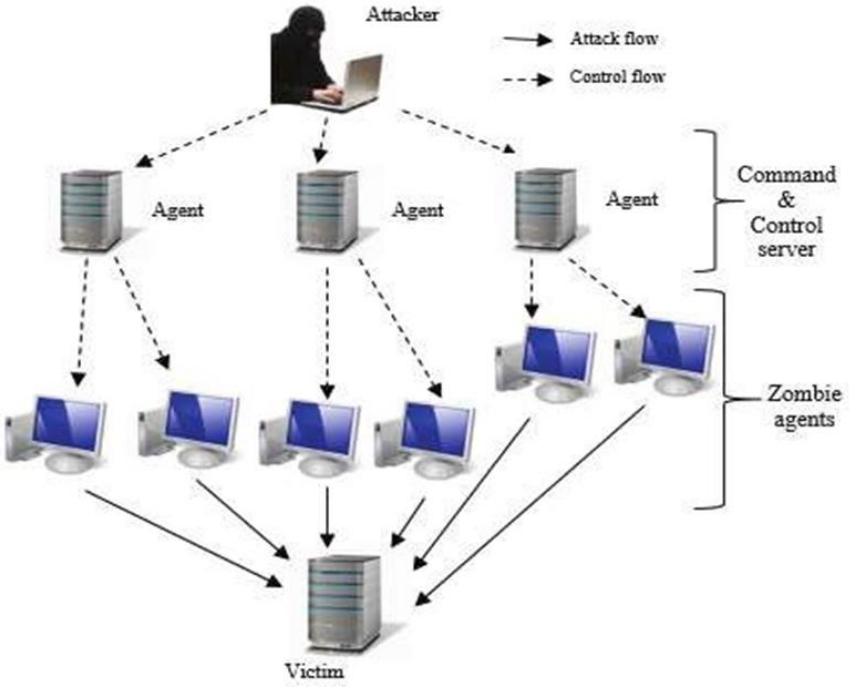

Fig. 1. The general architecture of DDoS attack [3]

1.1 Types of DDoS Attacks:

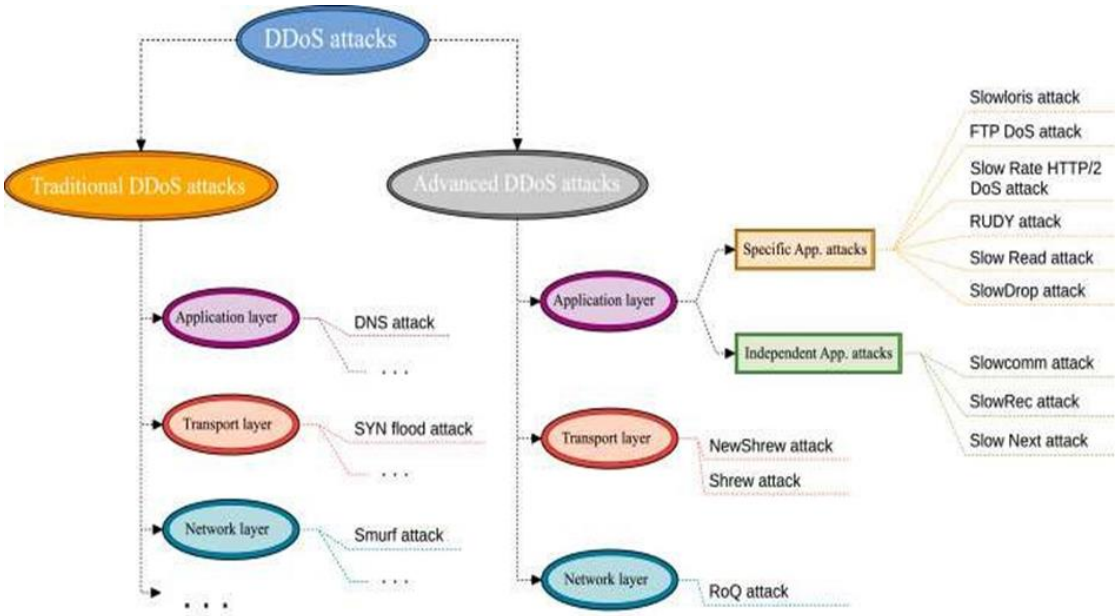

Fig. 2. Classification of DDoS Attacks [4]

2. Classification of defense mechanisms against DDoS attack

The mechanisms against DDoS attacks are classified into two layer-based groups 1. Network/transport layer & 2. Application layer.

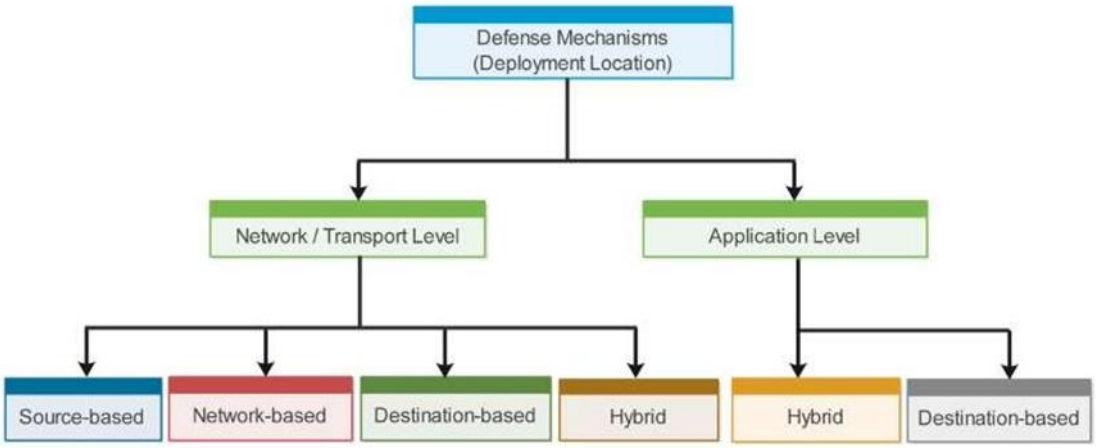

Fig. 3: Classification of defense mechanisms against DDoS attack based on layers and location [2]

2.1 Network/transport layer attacks

Flooding and amplification attacks fall under the network/transport layer category.

Flooding Attack: A flooding attack occurs when an attacker uses bots to send a large amount of traffic to a victim system, causing the system's bandwidth to be exhausted. UDP, ICMP, and SYN flooding attacks are examples of this type of assault [3].

Amplification attack: In this assault, attackers or bots take use of routers' broadcast IP address features to magnify and reflect the attack before sending messages to the broadcast IP address. This approach transmits the message to every IP address in the broadcast address range, consuming all available bandwidth. Attacks like Smurf and Fraggle are examples of amplification [1].

2.2 Application layer attacks

HTTP flood: Because port 80 (Hypertext Transfer Protocol or HTTP) is still usable for firewalls, attackers use this weakness to infiltrate HTTP. As a result of the attacker's flood of HTTP requests, the victim servers' resources are depleted [5].

SIP flood: Voice over IP (VOIP) telephony is a unique concept that has increased in popularity due to its low cost and convenience. The Session Initiation Protocol (SIP) standard was created to facilitate VOIP, and SIP proxy servers accept and process VOIP customers' call setup requests via the internet. Attackers employ request packets to infiltrate the SIP proxy server and flood, spoofing source IP addresses, because VOIP call establishment is based on request packets.

2.2.1 Destination based DDoS defense Mechanisms on the Application layer

Akbar et al. [6] have suggested a low-rate, multiple-trait DDoS detection technique based on Hellinger distance (HD). ISPs should utilize a cluster of servers because there are millions of customers and connections on the VOIP network.

Jun et al. [7] suggested an entropy-based detection approach to ensure proper traffic transmission while avoiding aberrant traffic floods. Entropy is a metric used in detection that is calculated based on packet information over a period of time.

Because the CAPTCHA [8]method faces difficulties, Bhuyan M and Kashyap H presented a technique in which each server connection is rated based on statistical analysis, and the attack is identified based on the score[8].

Ranjan et al. [9] developed a suspicion allocation system for detecting anomalies in session arrival, session request arrivals, and session workload profiles in the application layer. The suggested method assigns a session to a continuous measure of suspicion, which is updated after each request.

2.1.1 Hybrid DDoS defense Mechanisms on the Application layer

Overview of hybrid mechanisms:

These methods work in tandem with the Client/Server to detect and respond to assaults in a distributed manner [3].

Yu et al.[10] presented a flow correlation coefficient as a similarity metric between suspicious flows as part of a detection method. The correlation coefficient is effective since DDoS assault flows are considerably more comparable than Flash crowd.

Yan and colleagues [11] suggested a game-theoretic framework for evaluating and defending DDoS attacks. The suggested framework can mimic complicated levels of strategic thought on the part of both the attacker and the defense, and it allows for a wide range of legitimate traffic distributions to be chosen.

To deal with DDoS session flooding assaults, Yu et al.[12] suggested a Trust Management Helmet (TMH) technique that employs trust management. Short-term trust, long-term trust, negative trust, and misuse trust, which is used to

measure overall confidence, are the four user trust elements examined to form the link.

Table 1 The destination-based (server-side) techniques

Authors	Methodology	Type of Defense	Pros	Cons
Jun et al. [7]	Attack detection by entropy.	Detection	Guaranteeing normal traffic transmission and filtering Suspicious traffic.	Lack of comparison and accurate study of the proposed method with other detection methods, based on the quality of service Factors.
Liu and Chang [6]	Using customer properties and scheduling requests to defend against attacks.	Response and Protection	provided For legitimate Users. • Resource waste. time and accuracy in detection.	Efficient service defense on scheduling Policies. Preventing Proper response
Ranjan et al.[9]	Defense against attacks by allocating suspicion metric and using this metric in scheduler for deciding about providing service for the request.	Detection and Mitigation	• Improving efficiency and • response time of the victim.	• Not considering the limitation for simultaneous customers

Akbar et al. [5]	Detection the scheme implemented in SIP load balancer using leading open source VOIP sip server, namely Kamailio.	Detection and Mitigation	• Good Detection rate against DDos attack	• Efficiency of Load Balancer is less due to fewer DDoS attack Scenarios

2.1.2 Hybrid DDoS defense Mechanisms on the Application layer

Overview of hybrid mechanisms:

These methods work in tandem with the Client/Server to detect and respond to assaults in a distributed manner [3].

Yu et al.[10] presented a flow correlation coefficient as a similarity metric between suspicious flows as part of a detection method. The correlation coefficient is effective since DDoS assault flows are considerably more comparable than Flash crowd.

Yan and colleagues [11] suggested a game-theoretic framework for evaluating and defending DDoS attacks. The suggested framework can mimic complicated levels of strategic thought on the part of both the attacker and the defense, and it allows for a wide range of legitimate traffic distributions to be chosen.

To deal with DDoS session flooding assaults, Yu et al.[12] suggested a Trust Management Helmet (TMH) technique that employs trust management. Short-term trust, long-term trust, negative trust, and misuse trust, which is used to measure overall confidence, are the four user trust elements examined to form the link.

Table 2 Hybrid mechanisms

Authors	**Methodology**	**Type of Defense**	**Pros**	**Cons**
Yu et al. [10]	Using flow correlation coefficient to discriminate attack from Flash Crowd.	Detection	•Efficiency against unknown attacks. •Surveying the proposed method based on actual data. •Efficiency versus current Botnets size.	•Not surveying computational complexity. •Storage space to record information. •Dependence of analysis on assumptions. • Severe efficiency drop in Botnet big organization.
Yan et al. [11]	A game-theoretic framework is used to detect DDoS attacks	Detection	• able to model complex levels of the attacker	Complex to Implement the mechanism in different infrastructures.

Yu et al. [12]	Trust Management Helmet (TMH) method is used to cope with DDoS session flooding attacks	Detection	• TMH is lightweight, independent to the service details, adaptive to the server's resource consumption	• Limited to Session flooding attack only
Tang et al.[13]	Detecting and monitoring attacks based on meta-data and preventing attacks by rate limiting rules.	Detection and Prevention	• Achieving monitoring speed of 9 Gbps for server protection. • Detection efficiency.	• CPU • computational • cost. • Memory storage Space. • Dependence of Rule capacity restriction on the accuracy of using IP address mass.

3. Machine Learning-based DDoS Mitigation Techniques

The signature-based detection system is a labor-intensive process that takes many hours to test, develop, and deploy the signature, as well as create a new signature for unknown assaults. As a result, a system that is less reliant on humans becomes necessary. Anomaly-based IDS built from Machine Learning languages provide a solution to this problem, allowing for the incorporation of a framework that can learn from data and predict unknown statistics from learned data.

3.1 ML Techniques Using Naive Bayes

The Secret Nave Bayes (HNB) model delivers more dependable findings than the Standard Nave Bayes model, according to Kanagalakshmi. R et al. [13]. Because of the closely connected dynamic characteristics and comprehensive network Data stream capabilities, the Hidden Naive Bayes (HNB) technique could predict intrusion problems such as DOS attacks.

To detect attack rates, Jasreena Kaur Bains et al.[14] recommended using a hierarchical layered technique. Between each attack type on the smaller NSL KDD dataset, the system used a Naive Bayes classifier with a K2 learning approach. Each layer is taught to recognize a specific assault type using the research approach. The output of one layer is shifted to another layer to increase the detecting rate.

3.2 ML Techniques Based on Support Vector Machines (SVM)

Using the supervised approach of learning, SVM does classification and regression. An SVM algorithm generates a design that forecasts that the new model will tend to fall into one of two categories based on a set of training instances, each designated as the process is separated into two categories.

Vipin Das and colleagues (Vipin Das and colleagues) (Vipin Das and colleagues) (Vipin Das and colleagues)[15]. To classify DOS attacks, researchers used RST and SVM (supporting vector machines). Initially, network packets were acquired, and RST processed the data right away. The SVM model will be taught and tested using the RST feature sets that have been chosen. The findings are then evaluated using PCA, which demonstrates that RST and SMV are capable of doing so, and that the false-positive ratio improves efficiency.

T. Subbulakshmi et al. [16] wrote an article to monitor the online network and deploy a security strategy in the event of any suspicious activity. This method can detect spoofed and non- spoofed IP addresses. To detect faked

IPs, the author use improved Support Vector Machines (ESVM) and Hop Count Filtering. To begin the defense, this IPs will be used. The Lanchester Rule establishes the attack force that is utilized to trigger the defense mechanism [16].

Rung-Ching Chen et al. [17] wrote a paper where RST and SMV were utilised to identify Dos Attacks using a feature

set (obtained from RST) fed to SVM; T.Subbulakshmi et al. [18] have written the report using Enhanced Support Vector Machines, we worked on developing and detecting the DDoS dataset (ESVCM). For a created dataset, the EMCSVM is used to detect attacks in different classes, and the SVM is used to evaluate the EMCSVM.

3.3 ML Techniques based on K-Means Clustering

It's a clustering approach that divides data into k groups automatically. The K-means clustering algorithm selects k initial cluster centers from a data collection and refines them in a recursive manner [19].

Mangesh, D. Salunke, and colleagues [20] proposed a concept that aggregates packets; the packet is controlled by the specification, which includes features such as selecting features. As a result, to detect whether the packet is normal or a DOS attack, k-means and naive Bayes approaches are needed[20].

4. Conclusion

Detection and protection measures against DDoS attacks have been examined in this study, both in the past and in the present. In addition, we've divided defence methods into two primary stages: network/transport layer and application layer, based on the layer type. Source-based, network-based (core), destination-based, and hybrid network/transport layers were created. The application layer is further divided into two groups: destination-based mechanisms and hybrid mechanisms. For each of these classes, we looked at and compared a number of potential tools. Source-based methods at the network/transport layer are incapable of distinguishing between attack and genuine traffic. If a section or a router fails, network-based mechanisms will fail. Traffic filtering and rate limitation using destination-based techniques is ineffective. As a result, the recommended methodologies should be implemented collaboratively in future projects, and a platform for their collaboration should be established. In addition, the application layer mechanisms' infrastructure should be strengthened. To provide an effective defence against attacks, better collaboration between the consumer and the server must be ensured.

References

[1] C. Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: Classification and state- of-the-art,” Computer Networks, vol. 44, no. 5, pp. 643–666, Apr. 2004, doi: 10.1016/j.comnet.2003.10.003.

[2] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks,” IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[3] A. Selamat, A. R. Yusof, and N. I. Udzir, “Systematic literature review and taxonomy for DDoS attack detection and prediction,” International Journal of Digital Enterprise Technology, vol. 1, no. 3, p. 292, 2019, doi: 10.1504/ijdet.2019.10019068.

[4] V. de M. Rios, P. R. M. Inácio, D. Magoni, and M. M. Freire, “Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms,” vol. 186, Feb. 2021, doi: 10.1016/j.comnet.2020.107792.

[5] Abdullah Akbar, S. Mahaboob Basha, and Syed Abdul Sattar, “Leveraging the SIP Load balancer to detect and mitigate DDos attacks,” 2015.

[6] Huey-Ing Liu, “Defending Systems Against Tilt DDoS Attacks,” 2011.

[7] H. O.-H. K. Jae-Hyun Jun, “DDoS flooding attack detection througha step-by-step investigation,” 2011.

[8] M. B. J. L. Luis von Ahn, TELLING HUMANS AND COMPUTERS APART, vol. 47. 2014.

[9] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, “DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection.” [Online]. Available: http://www.ece.rice.edu/networks

[10] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, “Discriminating DDoS attacks from flash crowds using flow correlation coefficient,” IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073–1080, 2012, doi: 10.1109/TPDS.2011.262.

[11] Guanhua Yan and Ritchie Lee, “Towards a Bayesian Network Game Framework forEvaluating DDoS Attacks and Defense,” p. 1070, 2012.

[12] J. Yu, C. Fang, L. Lu, and Z. Li, “A Lightweight Mechanism to Mitigate Application Layer DDoS Attacks,” 2009.

[13] Charles Tang and Edward Lee and Andrew Tang, “Mitigating HTTP Flooding Attacks with Meta- data Analysis,” p. 71, 2015.

[14] J. K. Bains, K. K. Kaki, and K. Sharma, “Intrusion Detection System with Multi Layer using Bayesian Networks,” 2013.

[15] V. Das, V. Pathak, S. Sharma, Sreevathsan, MVVNS. Srikanth, and T. Gireesh Kumar, “Network Intrusion Detection System Based On Machine Learning Algorithms,” International Journal of Computer Science and Information Technology, vol. 2, no. 6, pp. 138–151, Dec. 2010, doi: 10.5121/ijcsit.2010.2613.

[16] T. Subbulakshmi, P. Parameswaran, C. Parthiban, M. Mariselvi, J. A. Anusha, And G. Mahalakshmi, "A Unified Approach For Detection And Prevention Of Ddos Attacks Using Enhanced Support Vector Machines And Filtering Mechanisms," 2013.

[17] R. C. Chen, C. Dewi, S. W. Huang, and R. E. Caraka, "Selecting critical features for data classification based on machine learning methods," Journal of Big Data, vol. 7, no. 1, Dec. 2020, doi: 10.1186/s40537-020-00327-4.

[18] T.Subbulakshmi, Dr. S. Mercy Shalinie, V.GanapathiSubramanian, and K.BalaKrishnan, "Detection of DDoS Attacks using Enhanced Support Vector Machines with Real Time Generated Dataset," 2011.

[19] S. K. Singh and A. K. Gupta, "Application of support vector regression in predicting thickness strains in hydro-mechanical deep drawing and comparison with ANN and FEM," CIRP Journal of Manufacturing Science and Technology, vol. 3, no. 1, pp. 66–72, 2010, doi: 10.1016/j.cirpj.2010.07.005.

[20] M. Salunke, R. Kabra, and A. Kumar, "IRJET-Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-mea Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm," International Research Journal of Engineering and Technology, 2015, [Online]. Available: www.irjet.net