Comprehensive Survey of Machine Learning Techniques for Detecting and Preventing Network Layer DoS Attacks

Niraj Prasad Bhatta, Ashutosh Ghimire, Al Amin Hossain, and Fathi Amsaad(✉)

Wright State University, Dayton, OH 45435, USA
{bhatta.8,ghimire.18,hossain.116,fathi.amsaad}@wright.edu

Abstract. With the increasing reliance on computer networks in our daily lives, the threat of network layer DoS (Denial of Service) attacks has become more prevalent. Attackers use various techniques to disrupt network services and cause loss of data, revenue, and reputation. Recent development in machine learning approaches have shown promise in prevention and detection of such types of attacks by several orders of magnitude. In this paper a thorough overview of machine learning approaches for detecting and preventing network layer DoS attacks is presented. Firstly, the basics of network layer DoS attacks, their classification, and the impact of these attacks is discussed. Then, different machine learning techniques and the ways in which they can be utilized for attack detection and prevention is explored. Additionally, analysis on the strengths and limitations of each approach, and provide a comparative study of the most relevant works in this field is done. Finally, some obstacles in research and potential avenues for future exploration is presented. in the field of machine learning-based defense mechanisms against network layer DoS attacks is discussed. In this paper a detailed summary of the most up-to-date advancements or developments in machine learning-based defense mechanisms against network layer DoS attacks is shown and serve as a reference for one and all who are involved in this field.

Keywords: DOS attack · Machine Learning · Network layer · Detection

1 Introduction

At the outset of millennium, rising usage of Computer networks has brought about a significant escalation in the Volume and intricacy of network layer attacks. The primary goal of the attack is to stop a normal operation of a network by inundating it with an overwhelming volume of traffic or deluging it with resource-intensive requests. Dos attack create a severe vulnerability to

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 347–356, 2024.
https://doi.org/10.1007/978-3-031-45882-8_23

the reliability, accessibility, and protection of interconnected systems Which can result in adverse consequences on both enterprises and individuals [1,2]. Novel research for identifying and preventing network layer DoS attacks to manage this burgeoning issue are proposed. Specifically, Machine learning have become a viable method for Detecting and alleviating DOS attacks, owing to their capability to analyze previous network traffic patterns and identify unusual activities [3,4].

OSI represents open Systems Interconnection is a conceptual type diagram that describes how a computer or communications network communicates. There are seven levels total, and each one defines a particular set of protocols and functions [5]. A DoS attack refers to a malevolent effort to obstruct authorized users from accessing a network resource, such as a website or server, by overwhelming it with traffic or exploiting vulnerabilities in its communication protocols [6]. where multiple compromised systems are used to flood a targeted website or network with a large amount of traffic, overwhelming its capacity and causing it to become inaccessible to legitimate users [7].

Other sections are laid out as follows: Sect. 2, summarize DoS attacks targeting network layer, including their definition, types, and impact. Section 2, summarize network layer DoS attacks, including their definition, types, and impact. Section 3, we explore the machine learning approaches that are considered as alternatives for detecting DoS attacks targeting network layer. Section 4, machine learning techniques that have been proposed for preventing network layer DoS attacks IS discussed. Section 5, a comparison between various techniques based on novel concepts of ML to identify and hinder DoS attacks targeting on network layer is provided. Section 6, Identification of open research challenges and future directions for the field is provided. In conclusion, the paper ends with a discussion on Sect. 7 (Fig. 1).

2 DoS Attacks in Network Layer

Internet protocol consists of layer that pertains to the network stack provides logical addressing and routing services that enable communication between different networks. However, the network layer is susceptible to a range of DoS attacks that have the potential to cause disturbance or interruption. the availability and performance of network services. This section provides an overview of network layer DoS attacks, including their definition, types, attack methods, and impact on network security. attacks focuses on disrupting the functionality of the IP protocol stack's network layer to overwhelm infrastructure of the network with a flood of traffic, requests, or packets. The objective of these attacks is to deplete the network's resources, disrupt the network connectivity, or cause the target system to crash or freeze [8].

2.1 The Following Are Some Common Types of Network Layer DoS Attacks

IP Spoofing. In this category of attack, the attacker falsifies the original IP address of the packet to make it appear as if it is coming from a legitimate source. By doing so, the attacker can bypass the network security measures that rely on IP address filtering or authentication.

ICMP Flood. The attacker inundates the destinated system with a flood of ICMP packets, which can consume the network bandwidth and resources.

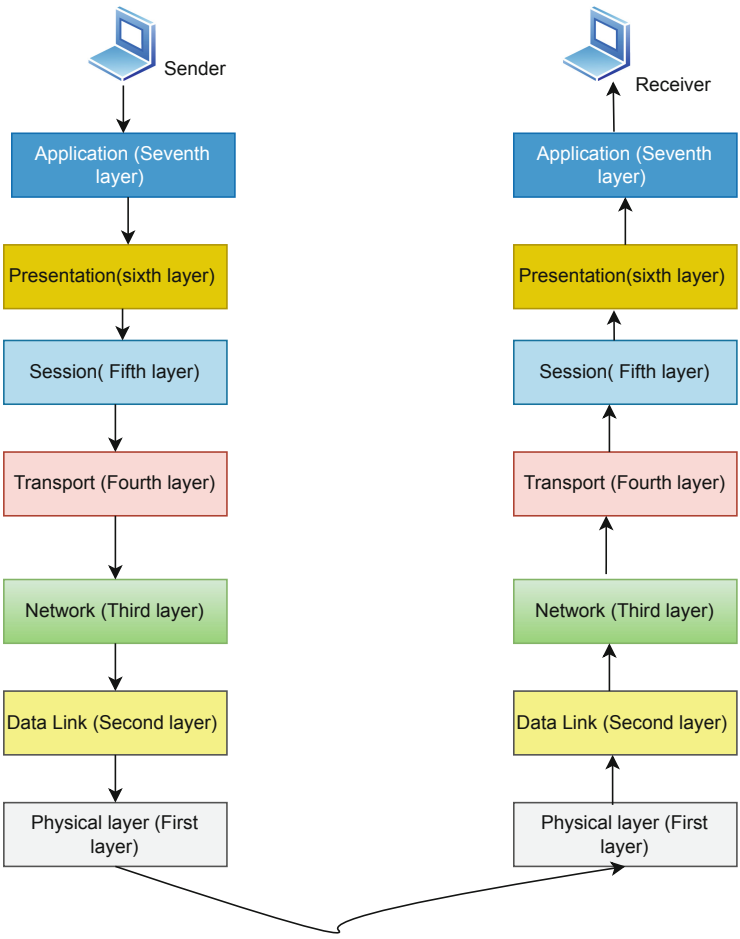

Fig. 1. OSI Reference Model Diagram

Smurf Attack. This category of attack takes advantage of the vulnerability of the Internet Group Management Protocol (IGMP), Sending ICMP echo requests to all devices in the network, rather than a specific device, causing all hosts on the network to respond to the target system.

2.2 Attack Methods and Strategies

Network layer DoS attacks can be launched using various attack methods and strategies, including the following (Fig. 2)

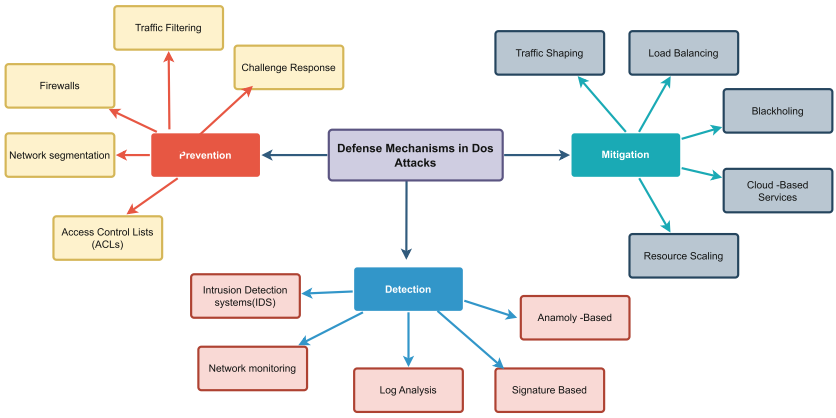

Fig. 2. Defense mechanisms in Dos attacks

Flood Attacks. In this method, the attacker inundates the target system with an enormous quantity of packets, requests, or connections. to consume the network resources and cause the system to crash or freeze

DDoS Attacks. In this method, the attacker uses a network of compromised computers, known as a botnet, to initiate a synchronized attack on the intended systemic.

Amplification Attacks. This method exploits the vulnerability of certain network protocols, such as DNS, NTP, or SNMP, to generate a large volume of traffic that can overwhelm the target system.

2.3 Impact and Consequences of Attacks

Network layer DoS attacks can have severe impact and consequences on the intended system and network infrastructure. Some of the typical outcomes of such attacks comprise

Degraded Network Performance. The network traffic generated by the attack can cause congestion, packet loss, and delay, resulting in degraded network performance.

Service Disruption. The attack can disrupt the availability of network services, making it difficult or impossible for legitimate users to access them.

Corruption. The attack can cause data loss or corruption if the target system crashes or becomes unavailable during the attack.

3 Machine Learning Approaches

The utilization of Machine Learning (ML) approaches has become increasingly popular in the detection DoS attacks in network layer because of its capacity to evaluate volumes of data in real-time. For DoS detection, several machine learning (ML) techniques have been suggested, including supervised, unsupervised, reinforcement, and hybrid learning (Fig. 3).

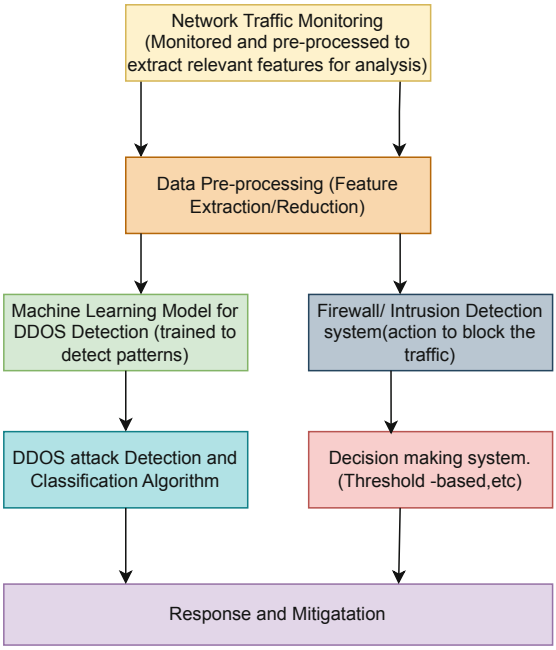

Fig. 3. Machine learning implementation

Approaches in deep learning can automatically learn features from raw network traffic data. Such type of approach includes CNNs and RNNs. Hybrid approaches combine multiple ML methods to enhance precision in detection and

lower the occurrence of false positives. Some examples of hybrid approaches include combining supervised and unsupervised learning, using ensemble methods, or combining ML with rule-based methods. By utilizing labeled data, supervised learning Concepts can build a model makes separation between genuine and malicious network traffic. decision trees and support vector machines play vital role. Unsupervised learning methods, such clustering and anomaly detection, could detect patterns and outliers in network traffic without the need for labeled data. Q-learning and deep Q-networks (DQNs) are examples of reinforcement learning algorithms that train themselves to make decisions depending on input from their surroundings. There are approaches that can be employed to detect network traffic anomalies automatically. For instance, RNNs and CNNs can automatically learn features from unprocessed network traffic data. Hybrid methods, which use a combination of multiple algorithms dealing with ML, which has the potential to enhance detection precision and lower the occurrence of false positive results. Hybrid approaches can be created by combining ensemble methods, rule-based methods, and both supervised and unsupervised learning.

4 The Machine Learning Techniques

The use of ML has gained popularity in preventing and mitigating the effects of DoS attacks by several orders of magnitude. ML approaches enable network administrators to detect and react to DoS attacks in real-time by doing analysis on patterns and behaviors in network traffic. Previous research has explored the utility of the use of ML for DoS attack prevention, including both attack mitigation techniques and defense mechanisms. For instance, A robust approach to identify Denial of Service (DoS) attacks employing an auto-encoder based on Support Vector Machines (SVM). The authors have tested the proposed method on the CICIDS dataset and achieved an accuracy of 99.32% for detecting DoS attacks [9]. SVM approach was initially proposed which has gained significant attention in ML research due to its excellent results. Through supervised learning methods, SVM can carry out both classification and regression tasks [10]. Subsequently, a dataset is formed, consisting of DDoS attacks, and is then employed to identify and detect these attacks using an advanced version of support vector machines (ESVM) [11]. Later, a DDoS attack detection model was developed by combining SVM classification methods [12].

Moreover, A novel approach called CSBW-Random Forest has been introduced, which outperforms existing methods regarding the measures of recall, accuracy, F1-score, and precision. The proposed technique achieves a high rating of 0.997 and shows significantly improved performance in comparison to previous literature. Additionally, experiments demonstrate that the suggested model performs better than related works in reference to the rates of three types of predictions: incorrect positives, correct positives, and incorrect negatives. KNN assigns classes Using the principle of proximity as a basis. This is a type of sluggish learning model that necessitates less training time but more prediction time. Most classes in the k nearest data points are used to assign the class. The

model can serve as both a classifier and a regressor, and the parameter K, which is a hyperparameter, can be adjusted to tune the model is easy to understand and implement but has disadvantages for instance, characteristics such as sensitivity to magnitude, high computational cost, and impracticality for handling large datasets [13].

In another study, feature selection techniques were employed to decrease the features from 41 to either 11 or 17, that includes LDA, PCS, RFE, and univariate feature selection. KNN was then used to classify the data, achieving an accuracy of 99.87% and 99.11% when using 17 and 11 features, respectively, with RFE. Similarly, an accuracy of 99.82% was achieved using PCA, and 99.79% using LDA and univariate feature selection techniques with 17 and 11 features [14].

Two studies investigated the effectiveness of the K Nearest Neighbors (KNN) algorithm on different datasets. The first study found that KNN achieved a ROC score of 0.985 on the WSN-DS type dataset. Furthermore, the second study evaluated KNN's performance on three datasets and found that it achieved a precision of 97.31% on the WSN-DS type dataset, 94.79% on the NSL-KDD type dataset, and 99.61% on the KDD-Cup99 type dataset [15].

A Bayesian network is a graphical model that utilizes probabilities in which a directed acyclic graph is used to illustrate the conditional relationships between variables. In wireless ad hoc network case, this approach can be applied to model network traffic behavior and identify unusual activity, including flooding-based denial-of-service attacks. The article outlines a technique that utilizes Bayesian inference to DoS attacks caused by SYN flooding in wireless ad hoc networks. Shifting towards the initial First part of the article, Bayesian inference is used to model the SYN traffic within the network statistically. This approach involves constructing a Bayesian network that considers the pertinent variables for SYN traffic, such as the quantity of incoming SYN packets, outgoing SYN-ACK packets, and the time intervals between SYN packets [16].

The second part of the article shows that Bayesian inference is equivalent to exponential weighted moving average (EWMA) in the case of a single variable. This equivalence results in a more effective method for identifying SYN flooding attacks in wireless ad hoc networks. The method can defend against various types of flooding-based DoS attacks with high accuracy and low false detection rate. Therefore, Bayesian inference is effective in detecting and protecting against SYN flooding-based DoS attacks [16]. Moreover, another proposed method employs a two-layer model to enhance the detection of minority attacks. The method employs statistical analysis to choose features relevant to the less frequent attacks, and then uses a separate dataset to train a multi-classifier artificial neural network, resulting in enhanced detection accuracy. The technique achieved a detection accuracy of 99.34% for minority attacks [17].

Moreover, another proposed model deals with an application of machine learning techniques for identifying SYN flood attacks, utilizing a dataset acquired from ethio telecom network. Four classification algorithms, Naive Bayes, AdaBoost, J48, and Artificial Neural Network (ANN), were tested, and J48 was found to have better detection performance. The paper suggests exploring

additional data mining methods and adopting a hybrid approach by integrating IDS and IPS to enhance network security [18].

In addition, some researchers have proposed using ML-based solutions for DoS attack prevention. They have presented two multi-party EdDSA [Edwards-curve Digital Signature Algorithm] Protocols designed for settings with partially trustworthy and untrustworthy participants. These aim to provide a secure method of maintaining a global state without the need for distributed hashing, possible for EdDSA-based blockchains. They have additionally expanded the malicious protocol to withstand DoS attacks by detecting corrupted parties in the event of execution interruptions.They tested their EdDSA protocols on Alibaba cloud servers and found that their protocol in the malicious setting is significantly quicker than recent threshold EdDSA protocols. The protocols possess characteristics that render them suitable for threshold wallets intended for EdDSA-based cryptocurrencies, including efficiency, identifiable abort, and high compatibility [19].

The proposed framework can reduce the workload of network administrators and enhance the efficiency of DoS attack prevention. Moreover, other studies have explored the use of ML-based defense mechanisms for DoS attack prevention. For example, LogDoS is a DDoS prevention system that relies on a unique process that utilizes GET messages and logging-relying filtering to establish inter-domain type routing. The system inserts GET messages at the ICN routers along the sender's path to eliminate packets that are not a reply to a preceding request. Combining NDN network and PID-based ICNs, this hybrid method generates a potent resolution for preventing data flooding attacks. LogDoS-enabled routers can filter packets and prevent them from causing flooding attacks. Overall, LogDoS is a powerful tool in preventing DDoS attacks and enhancing the security of ICN networks [5].

Overall, ML techniques hold great promise for preventing and mitigating DoS attacks at the network layer. Nevertheless, it is essential to emphasize that ML-based solutions also have their limitations and challenges, such as the need for large amounts of labeled training data and the potential for adversarial attacks. Future research should continue to explore and address these challenges to advance the development of effective ML-based solutions for DoS attack prevention.

5 Comparison of Machine Learning Approaches

The security and availability of computer networks are greatly endangered by Denial-of-Service (DoS) attacks. There are numerous methods suggested for detecting and preventing DoS attacks, including those that utilize machine learning techniques. The objective of this paper is to compare various machine learning-based techniques for detecting and preventing DoS attacks, as well as an assessment of the efficiency of machine learning techniques in combating network layer DoS attacks. This paper compares machine learning-based techniques for DoS attack detection and prevention, as well as their effectiveness in network

layer DoS attack prevention. SVM and RF have high accuracy for detection, but with higher computational overhead. KNN and NN have lower overhead, but lower accuracy. ANN and RF are effective for preventing DoS attacks with low overhead and good scalability. SVM and RF have a higher detection rate for network layer DoS attacks, but with higher overhead. DT and NB have lower overhead but lower detection rate. Overall, machine learning-based approaches are effective in enhancing network security against DoS attacks.

6 Open Research Challenges and Future Directions

Current machine learning-based techniques for detecting and preventing network layer DoS attacks face challenges such as limited availability and diversity of high-quality training data, difficulty in detecting sophisticated attacks, high false-positive rates or low detection rates, and limited interpretability. To address these gaps, emerging research trends include developing more robust and adaptive models using deep learning techniques, exploring explainable and interpretable machine learning models, and investigating transfer learning and federated learning approaches. Opportunities for further research and development include creating large and diverse datasets, exploring ensemble learning methods, investigating adversarial training, and integrating machine learning-based techniques with other security mechanisms.

7 Conclusion

In conclusion, the paper provides a comprehensive survey of ML techniques for detecting and preventing network layer DoS Type attacks. The paper highlights the strengths and limitations of different machine learning-based approaches, including rule-based methods, statistical methods, and deep learning methods. The study emphasizes the need for more robust and adaptive machine learning models, which can better detect sophisticated attacks and reduce false-positive rates. The paper also identifies emerging research trends and future research directions, such as exploring explainable and interpretable models, exploring transfer learning and federated learning methodologies., and integrating ML techniques with other security mechanisms. Overall, the study contributes to the understanding of the most advanced techniques in machine learning-based techniques for detecting and preventing network layer DoS attacks and provides insights for future research in this area.

References

1. Tayyab, M., Belaton, B., Anbar, M.: ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: a review. IEEE Access **8**, 170529–170547 (2020)

2. Xing, F., Wenye, W.: Understanding dynamic denial of service attacks in mobile ad hoc networks. In: MILCoM 2006–2006 IEEE Military Communications conference. IEEE (2006)
3. Verma, A., Saha, R., Kumar, N., Kumar, G., et al.: A detailed survey of denial of service for IoT and multimedia systems: past, present and futuristic development. Multimedia Tools Appl. **81**(14), 19879–19944 (2022). https://doi.org/10.1007/s11042-021-11859-z
4. Gebremariam, G.G., Panda, J., Indu, S.: Blockchain-based secure localization against malicious nodes in IoT-based wireless sensor networks using federated learning. Wireless Commun. Mobile Comput. **2023** (2023)
5. Kukreti, S., et al.: DDoS attack using SYN flooding: a case study. In: 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE (2022)
6. Patel, L., et al.: Machine learning methods in drug discovery. Molecules **25**(22), 5277 (2020)
7. Subbulakshmi, T., et al.: A unified approach for detection and prevention of DDoS attacks using enhanced support vector machines and filtering mechanisms. ICTACT J. Commun. Technol. **4**(2), 737–743 (2013)
8. Baarzi, A.F.: Efficient service deployment on public cloud: a cost, performance, and security perspective. The Pennsylvania State University (2021)
9. Allagi, S., Rachh, R., Anami, B.: A robust support vector machine based autoencoder for DoS attacks identification in computer networks. In: 2021 International Conference on Intelligent Technologies (CONIT). IEEE (2021)
10. Drucker, H., Donghui, W., Vapnik, V.N.: Support vector machines for spam categorization. IEEE Trans. Neural Networks **10**(5), 1048–1054 (1999)
11. Al Duwairi, B., et al.: LogDoS: a novel logging-based DDoS prevention mechanism in path identifier-based information centric networks. Comput. Secur. **99**, 102071 (2020)
12. Ye, J., et al.: A DDoS attack detection method based on SVM in software defined network. Secur. Commun Networks **2018** (2018)
13. Krishnan, D., Singh, S.: Cost-sensitive bootstrapped weighted random forest for DoS attack detection in wireless sensor networks. In: TENCON 2021–2021 IEEE Region 10 Conference (TENCON). IEEE (2021)
14. Pande, S., Khamparia, A., Gupta, D.: Feature selection and comparison of classification algorithms for wireless sensor networks. J. Ambient Intell. Humanized Comput. 1–13 (2021). https://doi.org/10.1007/s12652-021-03411-6
15. Singh, N., Virmani, D.: Computational method to prove efficacy of datasets. J. Inf. Optim. Sci. **42**(1), 211–233 (2021)
16. Nishanth, N., Mujeeb, A.: Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Syst. J. **15**(1), 17–26 (2020)
17. Shrivastava, U., Sharma, N.: Artificial neural network based dual layered predictive model for rare attack detection. In: 2020 International Conference on Computational Performance Evaluation (ComPE). IEEE (2020)
18. Mariam, W.B.W., Negash, Y.: Performance evaluation of machine learning algorithms for detection of SYN flood attack. In: 2021 IEEE AFRICON. IEEE (2021)
19. Feng, Q., Yang, K., Ma, M., He, D.: Efficient multi-party EdDSA signature with identifiable aborts and its applications to blockchain. IEEE Trans. Inf. Forensics Secur. **18**, 1937–1950 (2023). https://doi.org/10.1109/TIFS.2023.3256710
20. Gupta, B.B., Joshi, R.C., Misra, M.: Defending against distributed denial of service attacks: issues and challenges. Inf. Secur. J.: Global Perspect. **18**(5), 224–247 (2009)