# Detection System for DDoS Attacks

Subjects: Others
Contributor: Muhammad Saqib Javed

Distributed Denial of Service (DDoS) attacks, advanced persistent threats, and malware actively compromise the availability and security of Internet services. A DDoS attack is a vindictive attempt from numerous frameworks to make PC/network assets inaccessible to its expected clients, more often than not, by blocking/interrupting services associated with the organization of the network/Internet.

Keywords: Traffic Classification ; Machine Learning ; DDoS attacks

## 1. Introduction

A Distributed Denial of Service (DDoS) attack in late 2016, when three uninterrupted DDoS attacks were launched against the Domain Name System (DNS) provider Dyn, was a warning signal of the dangers of targeted DDoS attacks [1]. DDoS attacks have become one of the most severe threats to network security, with the first reported attack published by the Computer Incident Advisory Capability in 1999 [2]. While many mitigation systems have been developed in academia and industry, the threat of DDoS attacks is still severe and increasing yearly. In February 2018, a significant DDoS attack against GitHub overcame these mitigation systems [3]. Using BCP38 “Network Ingress Filtering” which, if deployed on the Internet, may stop packets with forged IP addresses from proceeding over the network, this type of attack could be mitigated [4]. However, research conducted using a random forest algorithm provided numerous benefits for the complexity, accuracy, and memory usage of DDoS attack detection systems [5]. The basis for this random forest algorithm in the recent research work is a main enhanced algorithm, Snort-based IPS. DDoS attack detection and mitigation using datasets enables the accuracy of the essential resource limitation rules in the systems concerned [6]. Other machine learning techniques create an intrusion detection system to detect DDoS attacks. A broader classification of these machine learning techniques involves the isolation of the IDS system [7], such as signature-based IDS anomaly-based rule-based specification IDS Markov models and hidden Markov models [8], and is at the heart of several IDS systems that are effective against these attacks. This technology is still under-researched but has advanced to state-of-the-art use in several specific cases [9]. Swarm intelligence has also been used to initiate and reduce IDS training time [10] and many hybrid schemes have been found to be more straightforward than conventional models in detecting attacks [11].

A DDoS attack is a vindictive attempt from numerous frameworks to make PC/network assets inaccessible to its expected clients, more often than not, by blocking/interrupting services associated with the organization of the network/Internet. The DDoS attacks on ideas/techniques have significantly altered over recent years. The importance of accessibility has been aimed at such influential attacks against network/web organizations, governments network/web, and private businesses. Multilayered barriers and collaboration requirements are essential. Procedures to mitigate DDoS attacks, initially through aversion are useful, however, in the end, outlining multilayered barrier systems should be standard.

DDoS threats should be considered in hazard arranging, like site choice, control blackouts, and characteristic fiascos. For these attacks, scholars concentrated on systems for securing the framework of IT from threats against accessibility. The exploration strategies/ideas will be demonstrated on DDoS threats by distinguishing proof and mitigation techniques that can successfully and productively react to DDoS attacks. DDoS does not depend on specific network protocols or framework outline shortcomings. It comprises an adequate number of traded hosts amassed to send futile packets toward a casualty around a similar time. DDoS becomes a significant threat because of the accessibility of various easy-to-understand attack tools and the absence of successful techniques to protect against them.

A DDoS attack [3] is unexpected network traffic sent to an objective. Under normal conditions, the utilization of bandwidth rate is in good esteem, and a specific pattern is available in the network movement. A sudden drop in the network performance due to an increase in either traffic, deferral, or CPU use will regularly be viewed as abnormal. The DDoS detection systems will search for such abnormalities in the network. When coordinated to the network layer, the attack causes a bottleneck and, when harmonized to the application layer, causes the fatigue of CPU resources. For the most

part, the abnormalities and the flow of data in the network are firmly related. Subsequently, understanding the kind of data and its qualities in the network can be named the first scheme to distinguish inconsistencies. These attributes can be a postponement, bundle header information, convention, parcel measure, etc. For example, a server reacting to TCP-SYN solicitations is well on its way to confronting the TCP-SYN and asking for flooding [2].

## 2. Detection System for DDoS Attacks

The rapid development and growth of the Internet and network structures have reformed the entire world of computers. The connected digital world also has gifted hackers and intruders with innovative facilities for their computing attacks. The most useful ways of detecting an attack are by abnormality, exploitation, anomaly, consolidated exploitation/anomaly detection, monitoring of the network, and recognition of the pattern. An anomaly detection mechanism distinguishes exercises that differ from setting up client patterns or gathering clients.

The authors in [12] proposed a method for detecting intrusions in computer systems using an anomaly-based intrusion detection system (IDS). The IDS was based on feature selection analysis and built from a hybrid efficient model. One drawback of the proposed method is that it relies on a fixed set of features to detect anomalies, which may only be suitable for some intrusion scenarios. The authors mention that the choice of components can affect the accuracy of the intrusion detection system, and there is a need for further study in this area.

Another potential drawback is the assumption that the system can accurately detect anomalies by comparing the system's current state to the average behavior profile. This assumption may not always hold in real-world scenarios where the system's normal behavior can change over time or where there are unexpected system behaviors.

Overall, the proposed method provides a starting point for building an intrusion detection system, but it is only a partial solution for some intrusion scenarios. Further research is needed to improve its accuracy and adaptability to different techniques and intrusion scenarios.

The paper proposed a machine learning-based intrusion detection system (ML-IDS) for detecting IoT network attacks. The system was developed using the UNSW-NB15 dataset along with approximately six proposed machine learning models; the results of the study showed a high accuracy of 99.9% and MCC of 99.97%, which are competitive with existing works. The paper aimed to address the privacy and security challenges of IoT.

Regarding MANETs and ensembles, hierarchical data gathering, processing, and a transmission structure with three hierarchy levels were proposed [13]. The anomaly index is calculated at each level, and the highest authority makes the ultimate call. The authors utilized the ROC curve and related area under the curve to describe the suggested scheme's efficiency (AUC). Regarding detection, the CFA algorithm relies on a decision tree, C4.5.

For identifying black hole attacks on AODV-based MANETs the authors in [14] proposed a complicated learning algorithm. A system for detecting malicious behavior in a network was built using a dynamic training system where the training data was updated periodically—an approach for detecting malicious nodes using a cluster. To assess the performance, detection rates against node mobility must measure from 70% to 84%, with node mobility between 0 and 20 m/s.

According to the framework, MAC, routing, and application layer anomalies may be detected using a Bayesian classification technique, a Markov chain construction approach, and an association rule mining algorithm created by [15]. The detection rate for the global integration module was 94.33%, with a false-positive rate of only 0.8% (FPR). However, around 90% of detection rates have substantial false alarms (more than 20%). Longer pause lengths have more significant detection thresholds, according to this theory. The Naive Bayes model, linear model, Gaussian mixture model, multi-layer perceptron model, and (SVM) model are among the well-known five supervised classification algorithms evaluated by [16]. These algorithms are employed in MANET detection engines for the detection method. The Naive Bayes classifier performed the worst, whereas the multi-layer perceptron classifier performed the best.

IoT device traffic was fed into a malware detection system trained on deep learning. An accuracy of 98.60, a precision of 98.37%, a recall of 98.17%, and F-measures of 98.18% were attained in this test. Five different machine-learning techniques were evaluated by Doshi et al. [17] to distinguish ordinary IoT packets from Denial-of-Service assaults on IoT networks. The random forest had the highest precision, recall, F1, and accuracy scores among the classifiers tested.

The authors of [18] proposed cascaded wormhole detection for an IoT-based network using deep learning. The attacks were evaluated based on their TPR, a 96.4% blackhole attack, 98.7% opportunistic attack, 98.7% DDoS attack, 99.9%

sinkhole attack, and 98% wormhole attack, with an overall accuracy of 96%. Detecting an attack method includes correlating a client's exercises with the acknowledged practices of attackers endeavoring to penetrate network systems.

The authors in [19] proposed a method for protecting web servers against application layer Distributed Denial of Service (DDoS) attacks using machine learning and traffic authentication. The system uses machine learning algorithms to extract features from network traffic and classify normal and attack traffic. The authors also introduced a traffic authentication mechanism to further enhance the system's security. The results of the experiments show that the proposed method effectively detects application layer DDoS attacks and has a low false positive rate. The main contribution of the paper was to provide a solution for protecting web servers against application layer DDoS attacks using a combination of machine learning and traffic authentication. The experiment's results demonstrated the proposed method's effectiveness in detecting DDoS attacks and provide insights for future research in this field.

The authors of [20] proposed a new approach for detecting cyber-attacks using the non-linear prediction of IP addresses. The system leverages big data analytics to analyze network traffic and identify abnormal behavior that may indicate an attack. The authors used an adaptive non-linear prediction algorithm to predict IP addresses and compare the predicted values with the actual values to detect anomalies. The experiments on real-world datasets showed that the proposed approach outperformed traditional intrusion detection systems in terms of accuracy and efficiency. The main contribution of the paper was to provide a new method for detecting cyber-attacks using the non-linear prediction of IP addresses and big data analytics. The experiment's results demonstrated the proposed method's effectiveness in detecting attacks and highlight the potential of big data analytics for improving cybersecurity.

In [21], a lightweight intrusion detection system (IDS) for detecting network intrusions based on feature selection and a multi-layer perceptron artificial neural network was proposed. The authors used the gain ratio method to select relevant features for attack and regular traffic before classification using the neural network. The proposed IDS was evaluated using the UNSW-NB15 intrusion detection dataset, and the results showed that the system is suitable for real-time intrusion detection with high accuracy.

The authors in [22] described a method for detecting DDoS attacks in computer networks. The authors proposed using an ensemble of neural classifiers to detect seizures instead of relying on a single classifier. The system uses a combination of data from multiple sources, such as network traffic statistics, to predict whether an attack is underway. The authors evaluated their method using real-world network data and reported that it outperformed other methods in terms of accuracy.

The authors of [23] presented a study on data mining techniques for detecting Distributed Denial of Service (DDoS) attacks. The authors aimed to improve the accuracy and efficiency of DDoS attack detection by using data mining techniques, specifically, decision trees and K-nearest neighbor algorithms. The study was based on actual network traffic data, and the results showed that the proposed approach effectively detects DDoS attacks.

In [24], a framework for detecting Distributed Denial of Service (DDoS) attacks in real time was proposed. The proposed framework, AIMM, consists of three modules: preprocessing, classification, and decision-making. The preprocessing module prepares the incoming data for analysis, then the classification module uses two different AI methods—neural networks and k-nearest neighbors—to identify potential DDoS attacks, and finally, the decision-making module aggregates the results from the classification module using techniques such as soft sets inference and weighted averaging to make a final decision on the attack status. The proposed framework was tested on the BOUN DDoS Dataset and achieved an accuracy of 99.5%. The results were compared to state-of-the-art techniques and found to be effective, with advantages such as a quick decision-making process and the ability to use various AI methods in the classification module. The authors claimed that their framework, AIMM, can effectively detect DDoS attacks by combining multiple artificial intelligence (AI) methods. However, the exact accuracy of the proposed AIMM framework is not stated in the paper. Further studies and evaluations are needed to verify the effectiveness and accuracy of the framework in detecting DDoS attacks in real-world environments.

Several papers [15][23][24] used supervised learning approaches to detect DDoS attacks, where the models are trained on labeled data. These approaches used neural networks [23], an ensemble of neural classifiers [23], and data mining techniques [24].

Other papers [16][22] used unsupervised learning approaches to detect DDoS attacks, where the models are trained on unlabeled data. These approaches used machine learning for intrusion detection [16] and the non-linear prediction of IP addresses [21].

Additional papers [17][18][19][20][21][25][26][27][28] presented other approaches to detect DDoS attacks. These include using deep learning [19], traffic authentication [20], a cascaded federated deep learning framework [19], and artificial intelligence merged methods [25].

In summary, the papers present various machine-learning techniques to detect DDoS attacks in various network systems such as mobile ad-hoc networks [15], IoT devices [18], and web servers [20]. **Table 1** compared the related works in terms of their methods, the drawback of their methods and the accuracy they achieved in their results.

**Table 1.** Comparison of the literature.

| Reference Number | Method | Drawback | ACC |
|---|---|---|---|
| [29] | Combined EA, SVM, and ANN | Limited dataset | 99.3% |
| [12] | Hybrid-based IDS | Fixed set of features | 96.64% |
| [13] | ML IDS for MIoT | Single dataset used | 99.9% |
| [15] | Dynamic Anomaly Detection Scheme | Only on AODV-based | 84.0% |
| [18] | Mix machine learning techniques | Small dataset, fixed features | 99.5% |
| [19] | Combined DTF, CNN, and LSTM | Only wormhole detection | 96% |
| [20] | Web-based DDoS detection | Only web single dataset | 99% |
| [21] | Mining sequences of IP's | Some worst performance | - |
| [22] | Building and evaluation using ANN-MLP | Single dataset: UNSW-NB15 | 76.96% |
| [23] | Detection by ensemble of neural classifiers | Overfitting | 99.4% |
| [24] | Detection by MLP, NB, and RF | Not applicable for all attacks | 98.63 |
| [30] | Detection by CNN and LSTM | Not applicable for low volumes | 96.7 |

## References


1. Collier, B.; Thomas, D.R.; Clayton, R.; Hutchings, A. Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks. In Proceedings of the Internet Measurement Conference, Amsterdam, The Netherlands, 21–23 October 2019; pp. 50–64.
2. Wang, M.; Lu, Y.; Qin, J. A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback. Comput. Secur. 2020, 88, 101645.
3. Singh, R.; Tanwar, S.; Sharma, T.P. Utilization of Blockchain for Mitigating the Distributed Denial of Service Attacks. Secur. Priv. 2020, 3, e96.
4. Dai, T.; Shulman, H. SMap: Internet-Wide Scanning for Spoofing. In Proceedings of the Annual Computer Security Applications Conference, Virtual, 6–10 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1039–1050.
5. Majidian, Z.; TaghipourEivazi, S.; Arasteh, B.; Babai, S. An Intrusion Detection Method to Detect Denial of Service Attacks Using Error-Correcting Output Codes and Adaptive Neuro-Fuzzy Inference. Comput. Electr. Eng. 2023, 106, 108600.
6. Alduailij, M.; Khan, Q.W.; Tahir, M.; Sardaraz, M.; Alduailij, M.; Malik, F. Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method. Symmetry 2022, 14, 1095.
7. Suaboot, J.; Fahad, A.; Tari, Z.; Grundy, J.; Mahmood, A.N.; Almalawi, A.; Zomaya, A.Y.; Drira, K. A Taxonomy of Supervised Learning for IDSs in SCADA Environments. ACM Comput. Surv. 2020, 53, 1–37.
8. García-Teodoro, P.; Díaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges. Comput. Secur. 2009, 28, 18–28.
9. Ravi, V.; Chaganti, R.; Alazab, M. Recurrent Deep Learning-Based Feature Fusion Ensemble Meta-Classifier Approach for Intelligent Network Intrusion Detection System. Comput. Electr. Eng. 2022, 102, 108156.
10. Nasir, M.H.; Khan, S.A.; Khan, M.M.; Fatima, M. Swarm Intelligence Inspired Intrusion Detection Systems—A Systematic Literature Review. Comput. Netw. 2022, 205, 108708.

11. Xinlong, L.; Zhibin, C. DDoS Attack Detection by Hybrid Deep Learning Methodologies. Secur. Commun. Netw. 2022, 2022, e7866096.
12. Aljawarneh, S.; Aldwairi, M.; Yassein, M.B. Anomaly-Based Intrusion Detection System through Feature Selection Analysis and Building Hybrid Efficient Model. J. Comput. Sci. 2018, 25, 152–160.
13. Kumar, S.; Dutta, K. Intrusion Detection in Mobile Ad Hoc Networks: Techniques, Systems, and Future Challenges. Secur. Commun. Netw. 2016, 9, 2484–2556.
14. Nakayama, H.; Kurosawa, S.; Jamalipour, A.; Nemoto, Y.; Kato, N. A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks. IEEE Trans. Veh. Technol. 2009, 58, 2471–2481.
15. Nishani, L.; Biba, M. Machine Learning for Intrusion Detection in MANET: A State-of-the-Art Survey. J. Intell. Inf. Syst. 2016, 46, 391–407.
16. Maglogiannis, I.G. Emerging Artificial Intelligence Applications in Computer Engineering: Real Word AI Systems with Applications in EHealth, HCI, Information Retrieval and Pervasive Technologies; IOS Press: Amsterdam, The Netherlands, 2007; ISBN 978-1-58603-780-2.
17. Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35.
18. Alghamdi, R.; Bellaiche, M. A Cascaded Federated Deep Learning Based Framework for Detecting Wormhole Attacks in IoT Networks. Comput. Secur. 2023, 125, 103014.
19. Ndibwile, J.D.; Govardhan, A.; Okada, K.; Kadobayashi, Y. Web Server Protection against Application Layer DDoS Attacks Using Machine Learning and Traffic Authentication. In Proceedings of the 2015 IEEE 39th Annual Computer Software and Applications Conference, Taichung, Taiwan, 1–5 July 2015; Volume 3, pp. 261–267.
20. Cuzzocrea, A.; Fadda, E.; Mumolo, E. Cyber-Attack Detection via Non-Linear Prediction of IP Addresses: An Innovative Big Data Analytics Approach. Multimed. Tools Appl. 2022, 81, 171–189.
21. Mebawondu, J.O.; Alowolodu, O.D.; Mebawondu, J.O.; Adetunmbi, A.O. Network Intrusion Detection System Using Supervised Learning Paradigm. Sci. Afr. 2020, 9, e00497.
22. Raj Kumar, P.A.; Selvakumar, S. Distributed Denial of Service Attack Detection Using an Ensemble of Neural Classifier. Comput. Commun. 2011, 34, 1328–1341.
23. Alkasassbeh, M.; Al-Naymat, G.; Hassanat, A.B.; Almseidin, M. Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. Int. J. Adv. Comput. Sci. Appl. 2016, 7, 436–445.
24. Jaszcz, A.; Połap, D. AIMM: Artificial Intelligence Merged Methods for Flood DDoS Attacks Detection. J. King Saud Univ. Comput. Inf. Sci. 2022, 34, 8090–8101.
25. Revathi, M.; Ramalingam, V.V.; Amutha, B. A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework. Wirel. Pers. Commun. 2021, 127, 2417–2441.
26. Kasongo, S.M. A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks Based Framework. Comput. Commun. 2023, 199, 113–125.
27. Zhao, R.; Mu, Y.; Zou, L.; Wen, X. A Hybrid Intrusion Detection System Based on Feature Selection and Weighted Stacking Classifier. IEEE Access 2022, 10, 71414–71426.
28. Almaiah, M.A.; Almomani, O.; Alsaaidah, A.; Al-Otaibi, S.; Bani-Hani, N.; Hwaitat, A.K.A.; Al-Zahrani, A.; Lutfi, A.; Awad, A.B.; Aldhyani, T.H. Performance Investigation of Principal Component Analysis for Intrusion Detection System Using Different Support Vector Machine Kernels. Electronics 2022, 11, 3571.
29. Hosseini, S.; Zade, B.M.H. New Hybrid Method for Attack Detection Using Combination of Evolutionary Algorithms, SVM, and ANN. Comput. Netw. 2020, 173, 107168.
30. Dora, V.R.S.; Lakshmi, V.N. Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM. Int. J. Intell. Robot. Appl. 2022, 6, 323–349.