International Journal of
Science, Architecture, Technology and Environment

Detecting Distributed Denial of Service Attacks: Recent Developments and Future Techniques

Mrs. G. Sathya[1*], Dr. D. Rajakumari[2]

[1]*Ph.D Research Scholar,Department of Computer Science, Nandha Arts and Science College (autonomous), Erode, Tamilnadu, India*

[2]*Associate Professor, Department of Computer Science, Nandha Arts and Science College (autonomous), Erode, Tamilnadu, India*

[*]*Corresponding author, vasathyabca@gmail.com*

DOI: https://doi.org/10.63680/ijsate0326010.005

Abstract

Distributed Denial of Service (DDoS) attacks, which cause online services to breakdown by flooding them with excessive traffic, remain a major threat to network security. The necessity for sophisticated detection methods that can effectively identify and neutralize these threats has been brought to light by the growth of these assaults as well as the rise in connected devices. An overview of the conventional DDoS detection techniques, including threshold-based and approaches based on signatures, which have been widely employed because of their ease of use. Nevertheless, these techniques frequently fail to control new assault patterns, necessitating the use of more advanced strategies.The article then looks at contemporary methods that improve DDoS detection by combining artificial intelligence, deep learning, and machine learning. Because of their increased detection accuracy and capacity to adjust to novel assault patterns, these data-driven techniques have become increasing popularity. These methods make it possible to classify traffic in real-time and reduce false positives by using past traffic data, which increases their effectiveness in dynamic attacks. Surroundings. Additionally, the study discusses issues including scalability, real-time detection, and the intricacy of changing attack routes that make conventional detection techniques more difficult to use.Lastly, the research looks at hybrid detection models, which integrate many methods to provide a more complete defence against DDoS assaults. These models increase overall detection accuracy and system resilience by combining the best features of traditional and contemporary methodologies. The final section of the study discusses the potential applications of DDoS detection, highlighting the necessity of intelligent, scalable systems that can adjust to the rising assault complexity in a society that is becoming more interconnected.

Keywords: Distributed Denial of Service (DDoS), Network Security, Traffic Classification, Hybrid Detection Models

I. INTRODUCTION

One of the most common and disruptive dangers to networked systems is Distributed Denial of Service (DDoS)

assaults, which have the ability to render servers, websites, and online services inoperable by overloading them with traffic. These assaults have increased in frequency.sophisticated, focusing on essential infrastructure in a number of areas, including government, healthcare, and banking.The principle of "Distributor" is troubling since a DDoS assault involves sending tens or hundreds of thousands of requests per second to a server from various locations or IPs.These requests originate from hundreds of thousands of compromised computers (often referred to as "zombies") that are controlled by "botnets" simultaneously, such as SYN Flood and Smurf attacks, which are a combination of bandwidth, memory usage, and target processing that typically no server are capable of handling, leading to a service collapse because it is unable to respond to every request;SVM-based machine learning has been successfully applied in the domains of pattern recognition research and information security in various classification, prediction, and regression.

Since the model originates using a statistical model that adapts its behaviour based on the input parameters defined and a training rule that require human interaction, using techniques with an SVM supervised model has significant advantages over rule-based techniques. The prototype evaluation revealed that the correct classification rate of normal or abnormal requests in the training phase is directly related to standardization and appropriate input parameter selection. Due to their simplicity and convenience of use, traditional DDoS detection techniques including threshold-based and signature-based approaches have been employed extensively in the past. These techniques, however, are limited in their ability to identify new or changing attack patterns, which might result in high false positive rates or attacks that go unnoticed. An overview of the traditional DDoS detection strategies, such as threshold-based and signature-based methods, which have become increasingly popular simply due to their simplicity, is given in this article.

Nevertheless, these techniques frequently fail to manage new assault patterns, necessitating the use of more advanced strategies.Notwithstanding the progress made in DDoS detection technology, issues with scalability, real-time detection, and managing the massive amounts of traffic produced during an attack still exist. Detection systems must be able to adjust to new attack vectors as assaults continue to change, all the while preserving efficiency and causing the least amount of interference to legal traffic. To address these issues, hybrid detection models that incorporate.Numerous strategies are showing promise as a remedy. By utilizing the advantages of both conventional and contemporary approaches, these models seek to improve detection accuracy and open the door for more robust and flexible DDoS protection systems.

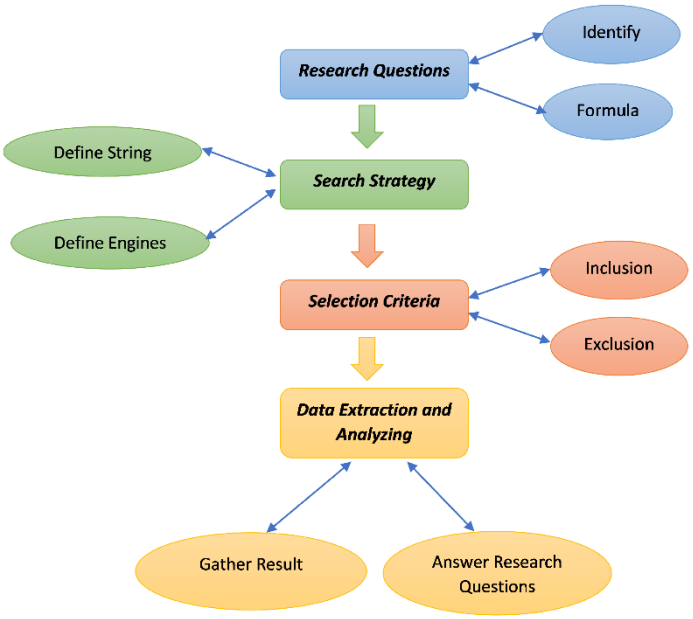


FIGURE 1. DDoS attack detection technology classification in SDN

Finally, SDN provides an open and programmable interface, which is convenient for network administrators to quickly develop according to requirements, simplify network management, and make the network architecture more convenient to maintain.The differences between traditional networks and SDN networks are shown in Table 1.

Table 1.Differences between traditional networks and SDN networks

Feature	**Traditional Networks**	**SDN Networks**
Control Plane	Distributed (on each device)	Centralized (SDN Controller)
Configuration	Manual/Device-by-device	Automated/Centralized
Flexibility	Rigid/Slow to change	High/Agile
Programmability	Low/Closed	High/Open APIs
Visibility	Limited/Isolated	Holistic/Real-time
Scalability	Slow/Complex	Rapid/Easy

As a result, it is imperative that the network security issues that SDN applications confront be resolved. Currently, several academics both domestically and internationally have investigated the detection and mitigation against DDoS attacks in an SDN context. Relatively few studies examine IDS and DDoS in SDN environments, but some examine the methods of IntrusionDetection Systems (IDS) in conventional networks. This study further explores the research development of DDoS attack detection from the viewpoints of statistical analysis, machine learning, and deep learning in order to investigate DDoS attack technology in SDN network architecture in a more methodical and thorough manner.

The following is a summary of this paper's contributions:

1)SDN's DDoS attack detection methods include examined in this work.
2) A detailed summary of the publicly available data sets and performance assessment criteria for DDoS attack detection in SDN networks is provided.
3) A thorough analysis of pre-processing techniques for handling data sets that are either self-generated or publically accessible.
4) The three kinds of DDoS attack detection technologies now in use in SDN include four entropy-based detection techniques, thirteen machine learning-based detection techniques, and learning model and eight deep learning model-based detection techniques, as well as the benefits and drawbacks of each technique.
5) In order to serve as a reference for further study and development, this work addresses the difficulties and potential paths for DDoS attack detection in SDN.

II. RELATED WORK

Strong detection systems that can adjust to shifting attack routes are necessary due to the DDoS assaults' quick growth and complexity. Numerous techniques, from machine learning techniques to statistical analysis, have been put forth over time to tackle this problem. In order to pinpoint developments, constraints, and potential paths forward in the area, this literature review looks at 10 recent and significant research studies on DDoS detection. The chosen research use a variety of methodology, including hybrid approaches, deep learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, and conventional statistical techniques. Shin and Gu [1] created a network scanning tool that could detect an SDN network and launched a denial-of-service attack on an SDN exploiting the control-data planes' separated logic of the SDN. Their approach, given that the data route had due to the controller's querying, the flow response times for the new and old flows altered. The scanner, which could scan the network to modify the network header fields, collected the time values based on the header fields. After the network was determined to be taken into The flow requests were sent to the target network as an SDN network, and the data path then sent them to the controller. Nevertheless, adding more flows to the data channel will cause the switches to experience flow setup requests on the controller, resulting in ultimately lead to the data path being broken. On the basis of Fonseca et al. [2], a DDoS assault on the SDN controller occurs when an attacker sends IP packets with random headers repeatedly in an attempt to interfere with the controller. shown the excellent detection accuracy of their approach, however the threshold and multi-element weight distribution required further technology. An ANN approach was presented by Saied et al. [6] to identify DDoS assaults. However, their approach was convoluted and ineffective since they had to make the distinction between the packet protocol. Ye et al. et al. [7] suggested creating the DDoS attack model by integrating Support Vector Machine (SVM) classification methods. Six feature values (SSIP, SSP, SDFP, SDFB, SFE, and RPF) were added to their technique. The TCP and UDP traffic had low false alarm rates, while the ICMP traffic had a significant false alert rate, according to their results of the experiments. Cui et al. [8] used Cognitive-Inspire to suggest a mechanism.

III. METHODOLOGY

I. SDN AND OVERVIEW FOR THE CLASSIFICATION OF DDoS ATTACKS

In this section, we survey the basics of the software defined network and discuss its architecture and features. In addition, an overview of the classification of the DDoS attacks is summarized. SDN is currently attracting abundant attention of researchers, aiming to provide open, centralized, decoupled, programmable, flow-based, and dynamic network switching mechanisms. In addition, there are some core differences that distinguish SDN networks from traditional networks. So, when implementing the networks, there are some details that are only specific to the SDN networks. Unlike the SDN, in traditional networks, the networking devices decide how an incoming packet should be solely handled based on its IP destination address. Meanwhile, the SDN carries out a flow-based forwarding scheme where multiple header fields clearly state how the incoming packet should be handled by a switch. Then, all the network devices record all the traffic statistics in the SDN network. However, some statistics are performed by only few devices in the traditional networks. Due to logically centralizing the network control plane and the introducing of programmability, the SDN simplifies both the network management and the run-time deployment of the security policies. With the help of the SDN, the network security systems can quickly respond to the network anomalies and the traffic status. In order to further set forth the SDN architecture and functionality, three main functional layers (i. e., the SDN planes) the SDN architecture is respectively composed of three parts: Application Plane, Control Plane and Data Plane. The application plane is on the top of the SDN architecture and contains the SDN applications for various functionalities, such as policy implementation, network management and security services. In the application plane, the SDN application can use the programmable method to submit the network behavior to the control plane. The control plane is a logically centralized control framework that runs the Network Operation System (NOS). In this plane, the hardware abstractions are provided to the SDN applications. It maintains a global view of the network. The entity that implements the control plane functionalities is represented as the SDN controller, which connects the application plane through the north-bound interface.

II. CLASSIFICATION OF DDoS ATTACKS

In this sub-section, we introduce the DDoS attack and its major classification. The DDoS attack is launched by multiple compromised computers called as bots or zombies targeting a single system. The attacker remotely controls these computers (i. e., bots and zombies) to attack other computers. In order to complete a DDoS attack, four major components must be included. One is the real attacker, and the second is the compromised hosts called as handlers or masters which are capable of controlling multiple agents using software programs. The third component is the agent hosts which generate a large number of packets towards the victim host. And the fourth component is the target host which is the victim. In the next paragraphs, the classification of the DDoS will be discussed. Specht and Lee introduced some tools used to launch the attack and analyzed in details the possible countermeasures. The classification of the DDoS attack is presented below. Flood Attacks: A flood attack involves zombies sending large volumes of traffic to a victim system. The flood attack has been launched using the packets of HyperText Transfer Protocol (HTTP), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) or Session Initiation Protocol (SIP). Hence, the flood attack is divided into the following four attacks: HTTP flood, ICMP flood, UDP flood and SIP flood attacks. The victim system is attacked by continuously sending UDP packets to a specific or a random port. In the ICMP flood attack, a large number of ICMP echo request packets with spoofed source IP addresses are sent to the victim. The HTTP flood attack is a volumetric attack done by sending abundant HTTP requests. In the SIP flood attack, the VoIP communications use Session Initiation Protocol (SIP) to send call signal. The SIP phone using SIP can be easily

flooded with messages so that it cannot obtain legitimate requests.

III.FEATURE SELECTION

Feature Selection is the method of reducing the input variable to your model by using only relevant data and getting rid
of noise in data. It is the process of automatically choosing relevant features for your machine learning model based on the type of
problem you are trying to solve.Relief feature scoring is based on the identification of feature value differences between nearest
neighbor instance pairs. If a feature value difference is observed in a neighboring instance pair with the same class (a 'hit '), the
feature score decreases.

TRAINING MODEL

The process of training an ML model involves providing an ML algorithm (that is, the learning algorithm) with training
data to learn from. The term ML model refers to the model artifact that is created by the training process.

PREDICTION MODEL

Predictive modeling is a mathematical process used to predict future events or outcomes by analyzing patterns in a given set of input data. It is a crucial component of predictive analytics, a type of data analytics which uses current and historical data to forecast activity, behavior and trends. This work is used KNN here.

GRU

GRU is a type of Recurrent Neural Network (RNN). An RNN performs the same task for every element of a sequence. The outputs are dependent on the previous computations. An RNN is trained using the back-propagation through time (BPTT) algorithm. However, BPTT for the RNN is usually hard to use due to the problem known as vanishing/exploding gradient. GRU networks can tackle this problem. GRUs have what is called an update gate and a reset gate. Using these two vectors, the model refines outputs by controlling the flow of information through the layers. GRU can retain information over a period. Thus, this model represents a system with memory. In the attack detection applications, GRU neural networks have demonstrated high-performance.

LSTM

LSTM model is another type of RNN capable of tackling the vanishing/exploding gradient. Its long-term memory capability could better capture the DDoS behavior in time than other methods that only include short-term memory, such as the MLP. The classification error is back-propagated in the network to update weights of the connections among the input, hidden, and output layers. LSTM has shown high effectiveness in detecting complex attacks to networks.

ALGORITHM

- we consider in our implementation of the algorithm. Therefore, distance metric and K value are two important
- considerations while using the KNN algorithm. Euclidean distance is the most popular distance metric.
- Firstly, we will choose the number of neighbors, so we will choose the k=3.
- Next, we will calculate the Euclidean distance between the data points. The Euclidean distance is the distance between two points.

KNN:

The K-NN working can be explained on the basis of the below algorithm:

- Step-1: Select the number K of the neighbors
- Step-2: Calculate the Euclidean distance of K number of neighbors
- Step-3: Take the K nearest neighbors as per the calculated Euclidean distance.
- Step-4: Among these k neighbors, count the number of the data points in each category.
- Step-5: Assign the new data points to that category for which the number of the neighbor is maximum.
- Step-6: Our model is ready.

IV. CONLIUSION

In this study, SDN-based detection systems developed for DDoS attacks were analyzed with machine learning systems. In the first proposed approach, by analyzing flow data, algorithms with 98.3% accuracy ensure the detection of attacks without discriminating the type of traffic. Among the proposed systems, the second approach proceeds by labelling DDoS attacks as normal traffic and attack traffic. With 97.7% sensitivity, KNN algorithms can perform this control by lightening the burden of the controller. With the feature selection methods used in the study, initially 12 features were selected and the selected subset of features was trained using classifiers. The number of features selected was determined either by the algorithm itself or by the threshold value given to the algorithm. By changing this threshold value, different numbers of features can be selected and trained by the classifier. Different numbers of features can change the accuracy. In general, we observed that the performance rate of all models is above 80% and the algorithms used for this dataset are successful. At the same time, network browsing, attacks between layers, and malicious software can be detected on SDN with this approach. For protecting and improving SDN structure, the second approach can be employed. In this study, SDN-based detection systems developed for DDoS attacks were analyzed with machine learning systems. In the first proposed approach, by analyzing flow data, algorithms with 98.3% accuracy ensure the detection of attacks without discriminating the type of traffic. Among the proposed systems, the second approach proceeds by labelling DDoS attacks as normal traffic and attack traffic. With 97.7% sensitivity, KNN algorithms can perform this control by lightening the burden of the controller. With the feature selection methods used in the study, initially 12 features were selected and the selected subset of features was trained using classifiers. The number of features selected was determined either by the algorithm itself or by the threshold value given to the algorithm. By changing this threshold value, different numbers of features can be selected and trained by the classifier. Different numbers of features can change the accuracy. In general, we observed that the performance rate of all models is above 80% and the algorithms used for this dataset are successful. At the same time, network browsing, attacks between layers, and malicious software can be detected on SDN with this approach. For protecting and improving SDN structure, the second approach can be employed.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

[1] M. Rahaman, P. Pappachan, B. Irawan, V. Arya, and K. T. Chui, "Vulnerabilities, attacks, and security aspects on the Internet of Things (IoT)," in Internet of Things Security: Elsevier, 2026, pp. 33-59.

[2] B. Fathimamary, M. Nasreen, and K. Velusamy, "An Efficient DDoS Attack Detection Using Optimized Long Short-Term Optimization Based on Improved Brainstorm Optimization," Indian Journal of Science and Technology, vol. 19, no. 5, pp. 298-312, 2026.

[3] K. Alrawashdeh, "Securing Internet of Things (IoT) networks," in Intelligent and Secure Solutions for Digital Transformation: CRC Press, 2026, pp. 48-67.

[4] M. Malini and N. Chandrakala, "DDoS attack detection in the cloud environment using an optimised long short-term memory with an improved firefly algorithm," International Journal of Communication Networks and Distributed Systems, vol. 32, no. 1, pp. 58-87, 2026.

[5] M. M. Saeed, R. A. Saeed, and Z. E. Ahmed, "An intelligent framework to secure fog computer and IoT service applications using artificial intelligence/machine learning," in Advances in Fog Computing and the Internet of Things for Smart Healthcare: Elsevier, 2026, pp. 27-54.

[6] H. Sharma, P. Kumar, and K. Sharma, "Security Solutions for the Internet of Things Using Machine Learning and Deep Learning: Current Trends and Future Directions," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 16, no. 1, p. e70059, 2026.

[7] A. A. A. Lateef, H. El Shenbary, A. A. Gouda, and M. A. Razek, "Optimization Algorithms for Path Routing and Security in Software-Defined Networking (SDN)," Appl. Math, vol. 20, no. 1, pp. 139-150, 2026.

[8] E. Osei Owusu et al., "A Systematic Review of Machine Learning and Deep Learning Techniques for DDoS Attack Mitigation in IoT and Edge Computing Systems," Security and Privacy, vol. 9, no. 1, p. e70147, 2026.

[9]P. Kuraś, M. Bolanowski, and M. Łoza, "Optimization of machine learning models for effective anomaly detection in industrial IoT systems," Advances in Science and Technology Research Journal, vol. 20, no. 1, pp. 203-221, 2026.

[10] Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. (2019). Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. 2019 Amity International Conference on Artificial Intelligence (AICAI). doi:10.1109/aicai.2019.8701238 .

[11] WU ZHIJUN , XU QING , WANG JINGJIE , YUE MENG (2020) Low-Rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network, Digital Object Identifier 10.1109/ACCESS.2020.2967478, VOLUME 8, 2020 .

[12] Yadav, S., & Subramanian, S. (2016). Detection of Application Layer DDoS attack by feature learning using Stacked Auto Encoder. 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). doi:10.1109/icctict.2016.7514608 .

[13] Bakker, J. N., Ng, B., & Seah, W. K. G. (2018). Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks? 2018 27th International Conference on Computer Communication and Networks (ICCCN). doi:10.1109/icccn.2018.8487445 .

[14] Khuphiran, P., Leelaprute, P., Uthayopas, P., Ichikawa, K., & Watanakeesuntorn, W. (2018). Performance Comparison

of Machine Learning Models for DDoS Attacks Detection. 2018 22nd International Computer Science and Engineering Conference (ICSEC). doi:10.1109/icsec.2018.8712757.

[15] Subbulakshmi, T., BalaKrishnan, K., Shalinie, S. M., AnandKumar, D., GanapathiSubramanian, V., & Kannathal, K. (2011). Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset. 2011 Third International Conference on Advanced Computing. doi:10.1109/icoac.2011.6165212

[15]. Hoyos Ll, M. S., Isaza E, G. A., Vélez, J. I., & Castillo O, L. (2016). Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype. Advances in Intelligent Systems and Computing, 33– 41. doi:10.1007/978-3-319-40162-1_4

[16]. Suresh, M., & Anitha, R. (2011). Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. Communications in Computer and Information Science, 441–452. doi:10.1007/978- 3-642-22540-6_42.

[17]. Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham. https://doi.org/10.1007/978-3-030-55180-3_49

[18]. Narasimha Mallikarjunan, K., Bhuvaneshwaran, A., Sundarakantham, K., & Mercy Shalinie, S. (2018). DDAM: Detecting DDoS Attacks Using Machine Learning Approach. Advances in Intelligent Systems and Computing, 261–273. doi:10.1007/978-981-13- 1132-1_21

[19]. Abid, K.: An efficient intrusion detection using J48 decision tree in KDDCUP99 dataset. Int. J. Emerging Technol. Adv. Eng. 6(2), (2016)

[20]. Sumathi, S., & Karthikeyan, N. (2020). Detection of distributed denial of service using deep learning neural network. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-020-02144-2