IJCI V9-02(2022) 64–73
International Journal of Computers and Information (IJCI)
Available online at https://ijci.journals.ekb.eg/

Techniques for DDoS Attack Detection in SDNs: A Comparative Study

Ahmed Latif Yaser[a,b,*], Mahmoud Hussein[a], Hamdy M. Mousa[a]

[a] *Computer Science Department, Faculty of Computers and Information, Menoufia University, Shebin Elkom 32511, Egypt*
[b] *Department of Information Systems, College of Administration and Economics, University of Baghdad, Baghdad 10071, Iraq*
ahmedlatif82@gmail.com, mahmoud.hussein@ci.menofia.edu.eg, hamdimmm@hotmail.com

Abstract

Software-Defined Networking (commonly referred to as SDN) is a newer paradigm that develops the concept of a software-driven network by separating data and control planes. It can handle the traditional network problems. However, this excellent architecture is subjected to various security threats. One of these issues is the distributed denial of service (DDoS) attack, which is difficult to contain in this kind of software-based network. Several security solutions have been proposed recently to secure SDN against DDoS attacks. This paper aims to analyze and discuss machine learning-based systems for SDN security networks from DDoS attack. The results have indicated that the algorithms for machine learning can be used to detect DDoS attacks in SDN efficiently. From machine learning approaches, it can be explored that the best way to detect DDoS attack is based on utilizing deep learning procedures.Moreover, analyze the methods that combine it with other machine learning techniques. The most benefits that can be achieved from using the deep learning methods are the ability to do both feature extraction along with data classification; the ability to extract the specific information from partial data. Nevertheless, it is appropriate to recognize the low-rate attack, and it can get more computation resources than other machine learning where it can use graphics processing unit (GPU) rather than central processing unit (CPU) for carrying out the matrix operations, making the processes computationally effective and fast.

Keywords: machine learning ; Software-Defined Networking ; Network Security ; Distributed Denial of Service.

1. Introduction

The identification and qualification technologies regarding DDoS attacks within SDN environments are a significantly challenging task. In the DDoS attack, many packets are forwarded to the target network. In case the forwarded packets' source and destination IP (Internet Protocol) addresses may be counterfeit and switches do not find them in their flow table entries, unmatched flows will be deemed unprecedented. Next, the switch transmits that unprecedented packet towards the SDN controller or straightly forward the packet. Typically, the controller of SDN is in charge of locating these packets' forward paths. Many DDoS flows are hidden in legitimate traffic, indefinitely consuming the controller's resources. Eventually, the resources of the controller come to be not available ahead of the upcoming new packets.

Consequently, the SDN controller stops, and the complete network will go downstate. Regrettably, this security challenge occurs even now in the backup controller's existence [1]. The DDoS attributes attack inside an SDN environment is placidly various from that at conventional networks. According to [2], the differences between DDoS attacks in classic networks and SDNs represents as follows; in classic networks, the DDoS attackers focus on destination servers, while in SDN, the DDoS attackers aim for the controller. The principal objective is to ensure the controller resources are not available by failing an SDN single point.

The IP addresses of packets in classic networks are actual. Consequently, terminal servers are a popular choice for DDoS attacks. However, SDN attacks use new streams of uninterrupted machining in order to

impersonate the target's IP addresses and disrupt normal system operations. As a result, all of the controller's resources have been marked as unavailable.

In the event of a DDoS attack on a classic network, the server stops serving known users. Data packets can't be forwarded because of a DDoS attack on an SDN controller, which means it can't provide services.

In classic networks, DDoS attacks detection is mainly at the mature stage. DDoS attacks detection in the SDN environment remains an available security issue since the SDN is a relatively new paradigm shift in the system networks. In an SDN environment, the identification techniques mainly applied in the classic networks are adopted to detect DDoS attacks throughout SDN without the knowledge attack characteristics. Due to unique characteristics of the SDN architecture, existing DDoS attack detection approaches used on the SDN controller fail to identify the attack accurately [3]. To figure out the appearance of a DDoS attack, the SDN controller must constantly collect network traffic data from switches, increasing the controller's workload. As a result, a system addressing this security threat needs to be implemented [4]. As a result of the insufficiency of traditional methods, machine learning techniques have received more attention and trial in the field of DDoS detection. The viability and efficiency of using deep neural networks, specifically long short-term memory (LSTM), convolutional neural networks (CNNs), and recurrent neural networks (RNNs), in the workout for detecting and eliminating DDoS attacks on SDN controllers has been investigated in this paper. Many machine learning algorithms [5] have been investigated in the literature for detecting DDoS attacks in the different layers of the SDN architecture, including Artificial Neural Network (ANN) [6], Support Vector Machine (SVM) [7], and Nave Bayes (NB) [8]. It was used the deep strengthening learning-based algorithm in the SDN application layer to mitigate similar attacks [9]. In section 2 of the proposed study, the SDN environment's main concepts, including its advantage compared with the classic network, have been reviewed. In addition to the main aim of this study which represented DDoS attacks, security challenges that may face, including the main attacks, are also presented. Section 3 addresses the recent related works that utilized machine learning techniques to detect DDoS attacks. The selected reviewed paper highlighted both shallow and deep machine learning. Method and achievement of the selected reviewed paper are analyzed and compared. The main difference and results obtained from the reviewed paper have been pointed out and analyzed in section 4. Finally, the most challenging of these techniques and suggestions to overcome these issues have been investigated in section 5.

2. **DDoS Attack in SDN**

The SDN paradigm has gained vital interest in recent days. The operator networks and data centers are changing from classic networks to SDN networks since it gives greater flexibility, reliability, and a secure network environment [10]. Therefore, the SDN deployment in cloud computing and data center environments gives flexible and reliable network architecture [11].

On the other hand, SDNs are susceptible to several security challenges such as port scans, Trojans, Worms, denial of service attacks (DoS), etc. [12]. Several scientists have expressed interest in DoS attacks. Attempts to prevent innocent clients from accessing network resources were the goal of this attack. DDoS attacks began to take shape after that, with the attacker enlisting a slew of widely dispersed devices in order to launch a distributed attack. At the time of a DDoS attack, the attacker looks for vulnerabilities in the network and then sneakily inserts a malicious program called a Trojan Horse into the target computers. An army of infected computers can be created by redistributing this malware program across a network of connected computers. These affected machines are usually called bots, and these bots' group is known as botnet [13]. All botnet is remotely placed under the supervision of a human operator known as a bot-master [14]. DDoS attack is initiated by sending commands to all of the computers that are affected, and these computers then send useless traffic to the victim. Because so many devices were infected, it's possible the victim was overwhelmed by the flood of useless traffic packets. As a result, legitimate users are unable to access the victim's resources, and the victim is therefore considered to be the victim of a DDoS attack [15].

In a DDoS attack, the incoming packet rate towards the network increases. Therefore, the network resources are bound by spoofed packets, which makes the resources unattainable. In case of this process proceeds, the server begins to drop the packets, and it will become inaccessible for the newer incoming legitimate packets. There are three types of DDoS attack: volumetric, application-layer, and protocol-exploitation attack. The flooding attacks for both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are taken into account as volumetric attacks, where the Hypertext Transfer Protocol (HTTP) and domain name system (DNS) flood are referred to as application-layer attacks [16]. The plane to control the SD control unit has central network intelligence. Within a singular SDN controller architecture, there is a higher possibility of a Single point of failure (called SPF). In cases where the attacker will get access to the controller, it causes massive damage to the network's infrastructure [4]. Uppermost applications at the top of the control plane, such as firewall, routing, and load balancing applications, have been operated. If the attacker passes through the firewall application, the controller creates several Access control lists (ACL) [17]. Then, a TLS/SSL (Transport Layer Security/SSL (Secure Sockets Layer) is used to secure the connection between the controller and OF switch; if the TLS connection keeps on downstate, it requires a backup controller toward the switch. In this situation, the OF switch uses the flow table depending on his choices. A DDoS attack correctly generates on to the controller in cases where a malicious flow can be ruled within the flow table [18]. In addition, the flow format has several significant properties for SDN. The SDN controller utilizes a southbound protocol involving the OpenFlow to act towards the flow entries. In SDN, the same flow could have several rules for it. Typically, the flow has several fields: priority, counter, time-out, action field, etc. Each one has its particular task. For example, the time-out field gives the flow expiry time, and the instruction field determines the necessary action for a flow entry, while the counter field keeps the information relating to bytes per flow [19]. Fig. 1 describes an SDN-DDoS attack resulting from compromised nodes. In the normal detection process of DDoS attacks in SDN, machine learning (ML) algorithms are utilized. In that case, when the packet gets to the switch, where the switch can determine its flow table entry, and in case there is a rule allocated to it, in that case, it will take the saved action. In any other case, the message has been sent to the controller.

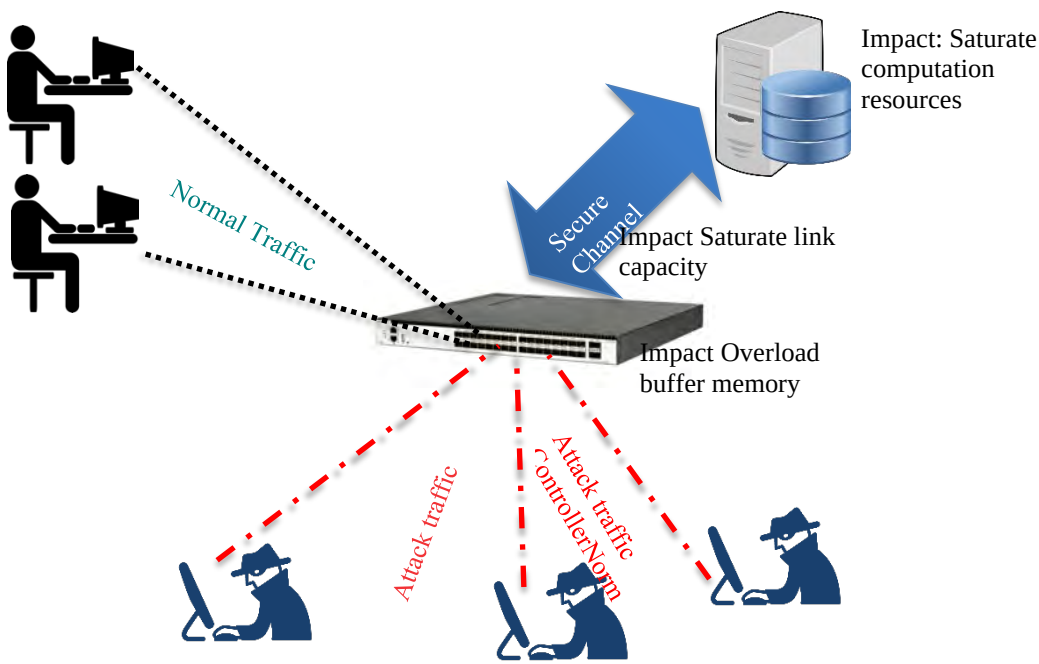

Fig. 1. SDN-DDoS attack resulting from compromised nodes [9].

According to these techniques, when the trigger is received, the controller can get the received packet information and bring the predetermined features that will be delivered to the machine learning model (ML) to identify if the traffic is malware. Depending on the result prediction of the machine learning model, the controller can be informed with the critical information, including (protocol type, IP destination, source address, destination port number, and source port number) to perform a task. Even so, if the trained model may not indicate whether the received packet is malicious or benign, the traffic can be considered suspicious (unidentified). The controller will recommend that the switches send unidentified traffic toward the deployed honeypot until a definite decision is performed. At the same time, the controller will forward unidentified traffic to the deep analysis module, which is undoubtedly the ML technique. Fig. 2 illustrates the detection module workflow for typical attacks. The deep approach can help outline and describe critical segments of the unidentified traffic and compare it with the known classes through a trained model [19-21].

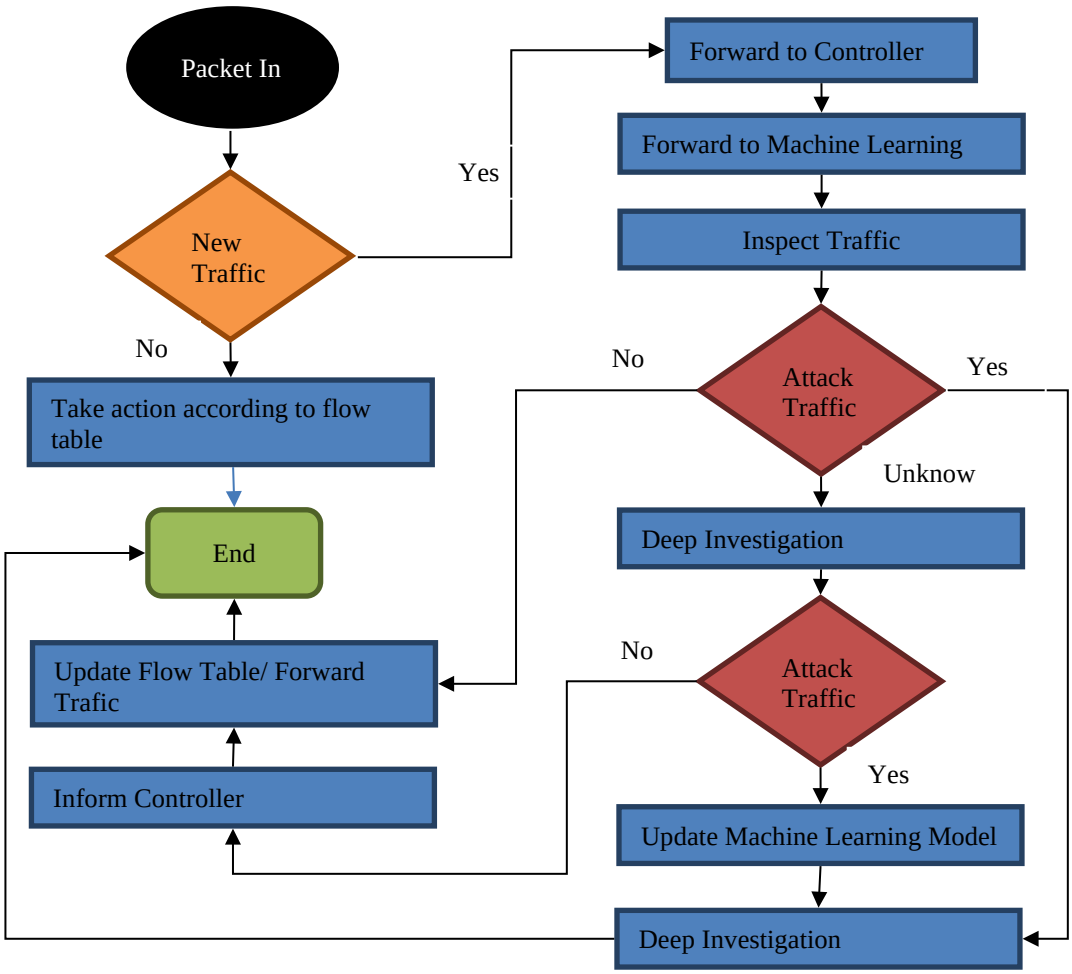

Fig.2. The Typical Attack detection module workflow.

3. Existing Techniques for DDoS Detections and Defense in SDN

This section reviews several articles on ML approaches used to recognize the DDoS attack in SDN. Some studies focused on utilizing ANN and SVM. Abhiroop et al. (2018) [22] proposed ANN, SVM, and Naive Bayes-based techniques. In their work, they used the same dataset for all models and separated it into 60% for training and 40% for testing. Their results show that the ANN and Naive Bayes models achieved an accuracy of 100%, while the SVM model achieved an accuracy of 99%. Ye et al. (2018) [23] presented a model to detect the DDoS attack in SDN. The model utilized the SVM method. The results demonstrated that the model obtained an average accuracy of about 95.24%. Santos and Moreno (2019) [24] researched the attack problem in SDN and utilized the solution by making use of several ML methods. These ML methods are SVM, Random Forest, decision tree, and multilayer perceptron (MLP).

SDN was able to classify DDoS attacks using these techniques. Scapy was used to run the entire proposed strategy through its paces. Implementation uses the real IP address catalog. The results of the tests show that the Random Forest algorithm is more accurate. In addition, the Decision Tree algorithm was faster.

Elsayed and Jurcut (2019) [25] systematically examined the present ML methods used to protect SDN against DDoS attacks. Their study analyzed the specific limitations observed in classic models. The testing of each method has been achieved based on several parameters. This study's four approaches for comparison were SVM, Random Forest, and Naïve Bayes. The test result showed that the Naïve Bayes algorithm of ML is a much better method to recognize the DDoS attack in SDN since this specific algorithm has much more accuracy than other present approaches. Wang (2020) [26] presented an ANN method to recognize known and unknown DDoS attacks. A dynamic multi-layer perceptron that works together with a feedback strategy will be able to detect attacks. For this purpose, they use several selected characteristics that cannot distinguish between DDoS attacks and standard traffic flows.

For applying machine learning and deep learning (DL) to detect DDoS in SDN, Karan et al. (2018) [27] presented a detection model that can recognize DDoS attacks in the SD environment. In this model, the two levels of security are already utilized. Initially, the proposed system detects the attack depending on its signature. Snort is utilized to determine the types of these attacks. Following that, the SVM and deep neural network (DNN) classifiers are employed to create a trained model. As a result of the comparison of these two classifiers, the DNN model overperforms SVM. The attained accuracies of DNN (Deep neural networks) and SVM classifiers are 92.3% and 74.3%, respectively. Liu et al. (2018) [28] designed a model that utilized a reinforcement learning dependent on an intelligent flood mitigation agent for DDoS. Their results of various protocols show that the agent could efficiently alleviate the effects of DDoS flood attacks. The issue of intrusion detection has been overcome using the deep-learning algorithms in SDN-based constructions [16-18].

Other deep learning algorithms [9, 19] were also applied in SDN architectures to identify DDoS and attack detection. Li et al. (2018) [29] presented a system that allows detecting and defense against DDoS attacks by employing the deep learning method. The presented model was able to obtain the result by making use of the traffic history of the network along with some other activities from several network attacks. The results showed that the deep learning method is more adequate, precise, and efficient when compared with traditional ML methods. Jose et al. (2019) [30] investigated the mitigation methods used in the SDN for DDoS attacks. Both regular methodologies of AI are compared to identify which model is much more accurate in reducing the DDoS attack in the SDN. The considered approaches in this survey are ML and deep learning. The DDoS attack detection is being performed using multiple properties or features of this particular attack. The results from these methods approve that deep learning gets higher accuracy than ML. Haider et al. (2020) [31] presented a new method by utilizing a deep convolutional network (DCNN). This model helps in detecting the DDoS attack with high efficiency. A specific benchmarked dataset is explored to test a model. A comparison is made between the adopted methods and those currently being used by other researchers and included in their published research work. The methods that were compared are SVM, hybrid Restricted Boltzmann machine and SVM

(RBM+SVM), LSTM, and recurrent neural network (RNN). The results showed that their proposed model is more accurate than other models, which is about 99.45%.

Table 1. *Compares previously proposed schemes in terms of technique, performance measures, datasets, and additional comments.*

Deep Learning Approaches		
Recent Works	***Method***	***Results***
Karan (2018) [27]	DNN and SVM	DNN achieved higher accuracy (92.30%) which is higher than SVM
Liu (2018) [28]	DRL	The researchers found that the agent could effectively counter DDoS flooding attacks using a variety of protocols. The accuracy reaches up to 94% after 20000 episodes. The model outperforms the performance of state-of-the-art (CTL) for about 3-9% and outperforms the performance of Additive Increase Multiplicative Decrease (AIMD) algorithm for about 18-28%
Li (2018) [29]	DL	The detection scheme of DDoS attacks depends on DNN, characterized by its high detection accuracy. Dependent on hardware devices and software is less than other types. Also, the network model is easy to update in real-time. Four DNN algorithm is used LSTM, CNN/LSTM, gate recurrent units (GRU) and 3LSTM. LSTM and 3LSTM get higher accuracy than others where archive 99.88% in LSTM and 99.79% in 3LSTM
Jose (2019) [30]	ML & DL	DL is more accurate than other ML techniques; ML algorithms perform well on small datasets while DNN Algorithms need large datasets to understand the data representations; learning from complex data representation is difficult for ML, while DNN has better performance and accuracy achieved for complex data representations.
Haider (2020) [31]	DCNN	The model achieved a high accuracy reaching up to 99.45% compared with other ML algorithms, which include: SVM, hybrid Restricted Boltzmann machine and SVM (RBM+SVM), LSTM, and RNN.
Other Machine Learning Approaches		
Recent Works	*Method*	*Results*
Abhiroop (2018) [22]	Naïve Bayes, ANN & SVM	ANN and Naïve Bayes achieved higher accuracy, reaching up to 100% compared to the SVM results that achieve relatively accuracy less than ANN & about 99%
Ye (2018) [23]	Based on six-tuple features collected from SDN data, SVM is used to classify the traffic as normal or attack traffic.	Because ICMP packets do not contain a port address, detecting ICMP traffic was difficult. The achieved accuracy is 95.24%.
Santos and Moreno (2019) [24]	SVM, decision tree, Multilayer perceptron, and Random Forest	The random forest is more accurate than the other models, achieving up to 100% accuracy; the other models results are: the DT achieves 99%, the MLP achieves 98%, and the SVM archive 92%
Elsayed and Jurcut (2019) [25]	J48 algorithm	J48 is a better method for detecting DDoS attacks compared with SVM, Naive Bayes, and Random Forest
Wang (2020) [26]	Artificial Neural Network-based Dynamic Multilayer perceptron (MLP)	The proposed model is better than the machine learning models investigated in this work which includes, MLP, DT: J48, BN and RNN

From table 1, the most ML and deep learning algorithms got the highest accuracy than traditional methods that can recognize both known and unknown DDoS attacks; however, till now, the high accuracy achieved in trained, but the accuracy in tests is still lower, and there is a need to investigate new methods that can improve accuracy for unknown DDoS attacks and find a solution to it accurately.

4. **Discussion**

Different Machine learning-based models are employed for attack detection/classification. Most machine learning methods give good accuracy in the detection of DDoS attacks. The common machine learning approaches involved; Artificial Neural Network (ANN), Naïve Bayes (it is the supervised learning algorithm that depends on Bayes theorem which is commonly utilized for solving problems of classification), support vector machine (SVM); J48 algorithm (It is one of the best algorithms for categorical and continuous data analysis in machine learning), Multilayer perceptron (MLP) and deep learning algorithms. From the literature, all machine learning algorithms achieved high accuracy ranging from 92% up to 100% in training. The test results showed that some algorithms are better for detecting the DDoS attack than others, such as J48, naive Bayes, and the random forest. However, the deep learning method shows it has achieved more accuracy and best decision-making compared to the other machine learning methods; this seems clear that most recent research focuses on it.

Despite the deep learning performance models, several solutions use conventional machine learning models, as shown in Table 1, because of their simplicity and ability to discover significant characteristics without human intervention. For time-series data where the present state is dependent on the initial state, RNN is the best option. In contrast, LSTM represents a particular type of RNN. Also, some researchers utilized a hybrid method between CNN and LSTM, in which LSTM has used for prediction in long-range sequence and CNN was used for feature extraction, this combination gives both an advantage in DDoS detection tasks. Nevertheless, those models are usually associated with several reduction methods.

Furthermore, as detailed by the literature analysis, the detection of DDoS attacks has attracted the attention of several researchers. In other words, because the SDN controller is the network's central brain, storing and processing data from all forwarding devices, it is vulnerable to DDoS attacks. Despite the deep learning performance models, several solutions use conventional machine learning models (shown in Table 1) because of their simplicity and ability to discover significant features without human intervention. For time-series data where the present state is dependent on the initial state, RNN is the best option. In contrast, LSTM represents a particular type of RNN. Also, some researchers utilized a hybrid method between CNN and LSTM in which LSTM has been used for prediction in long-range sequence and CNN has been used for feature extraction, which this combination gives both an advantage in DDoS detection tasks. Even so, these models are commonly accompanied by several reduction processes. Furthermore, as detailed by the literature analysis, the detection of DDoS attacks has attracted the attention of several researchers. In other words, because the SDN controller is the network's central brain, storing and processing information from all the forwarding devices, it is vulnerable to DDoS attacks.

5. **Challenges and Future Direction**

Research that utilizes machine-learning approaches with networks has developed a wide variety of novel methods. Applying machine learning, especially deep learning models to networking, makes various use solutions and cases. Even so, these solutions have several issues and challenges in practice. This review discussed the methodologies, challenges, weaknesses, and strengths in the existing methods related to the proposed taxonomy.

In this review, we focused on approaches-based machine learning rather than the statistical Methods because the related works in that field [32-34] show some Limitations: One of these limitations is that the statistical-based DDoS detection approaches work based on prior knowledge of network flow. Nevertheless, in the current days, malicious network flows have come to be a changeable target. Therefore, it is a difficult task to define the network traffic in the right way. The second issue is that most of the statistical DDoS detection strategies depend on various user-defined thresholds. Thus, all those thresholds should be modified dynamically to be up to date, considering variations in a network. In order to detect DDoS attacks using statistical approaches, an entropy technique is utilized, which uses just one feature, such as the source IP address, to make the detection model. However, it can easily adjust source IP addresses by attackers by using tools such as hping, scapy, etc. Thus, selecting this feature to recognize DDoS attacks is not a helpful tool. In addition, most statistical approaches, such as correlation, entropy, etc., need excessive computational time during the detection of a DDoS attack. Thus, they are not able to be performed in real-time.

Shallow Machine Learning methods like ridge regression (RR), support vector machine (SVM) principal components, and support vector regression have some limitations: It performs well-using rules through a small amount of data. The Shallow Machine Learning algorithm recognizes the attacks depending on statistical features, and after that, it can determine the value or class. Additionally, it needs regular updating of the model related to the variations in attacks. The Shallow Machine Learning approaches addresses the issue by breaking it into small sub-problems, then covering subproblems and providing the last result. In Shallow Machine Learning, several algorithms need less time in training, but it needs more extended time in testing. In contrast, the deep learning methods are appropriate for detecting DDoS attacks as deep learning techniques can perform feature extraction and data classification. Currently, there is a need for a scanning system in order to manage data unavailability.

However, the labeled authorized traffic is usually available, while the availability of labeled malicious traffic is fewer. Hence, deep learning techniques can extract specific information from partial data.

The deep learning techniques are appropriate to recognize the low-rate attacks. Hence, there is a requirement for historical information to recognize low-rate attacks, and the deep learning approaches can learn extensive dependencies of temporary patterns. Therefore, the deep learning methods are beneficial in such a case. The deep learning methods have complicated mathematical operations performed via multiple hidden layers by utilizing several parameters throughout the training phase. The deep learning approaches use numerous matrix operations compared with standard machine learning methods. In addition, it can use GPU rather than CPU for performing the matrix operations, which can give an advantage in making deep learning processes computationally effective and fast. Thus, for future work, the researchers should focus on developing a new deep learning approach and utilizing hybrid AI approaches to provide better results compared with traditional machine learning techniques and deep learning techniques in related areas.

6. **Conclusion**

This systematic research compares the various machine learning algorithms recently used to detect DDoS attacks in the SDN environment. The accuracy of each approach was considered when making the comparison. From the amylases of the related works, most ML algorithms achieve good results and high accuracy in detecting DDoS attacks. However, the most study takes consecration to test a single dataset, while the most study they avoid testing the model with other types of DDoS datasets, were mentioned in some studies that the change in the dataset could affect the accuracy of the model, whereas the new studies should take in consideration this point of view. According to the findings of the current review study, the deep convolutional neural network is an accurate, appropriate, and efficient way of detecting DDoS attacks or threats in a software-defined network environment. By analyzing previous works, we can give our point of view that newer studies need to be focused on developing a distributed DDoS detection based on deep learning techniques that consider combining two deep learning models or shallow and deep models. In addition, the researchers should take into their consideration one of the best deep learning methods that achieve higher detection results, which is a

convolution neural network that can make a hybrid with other machine learning algorithms such as ANN in order to improve the accuracy of classification detection and shorten the processing time of classification detection.

References

[1] H. S. Abdulkarem and A. D. Alethawy, "DDOS attack detection and mitigation at sdn enviroment," *Iraqi Journal of Information and Communication Technology,* vol. 4, pp. 1-9, 2021.

[2] C. Fan, N. M. Kaliyamurthy, S. Chen, H. Jiang, Y. Zhou, and C. Campbell, "Detection of DDoS attacks in software defined networking using entropy," *Applied Sciences,* vol. 12, p. 370, 2021.

[3] W. G. Gadallah, N. M. Omar, and H. M. Ibrahim, "Machine Learning-based Distributed Denial of Service Attacks Detection Technique using New Features in Software-defined Networks," *International Journal of Computer Network and Information Security (IJCNIS),* vol. 13, pp. 15-27, 2021.

[4] M. W. Nadeem, H. G. Goh, V. Ponnusamy, and Y. Aun, "DDoS detection in sdn usingmachine learning techniques," *Comput. Mater. Contin.,* vol. 71, pp. 771-789, 2022.

[5] P. S. Saini, S. Behal, and S. Bhatia, "Detection of DDoS attacks using machine learning algorithms," in *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2020, pp. 16-21.

[6] O. Ali and P. Cotae, "Towards DoS/DDoS attack detection using artificial neural networks," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2018, pp. 229-234.

[7] D. Li, C. Yu, Q. Zhou, and J. Yu, "Using SVM to detect DDoS attack in SDN network," in *IOP Conference Series: Materials Science and Engineering*, 2018, p. 012003.

[8] M. A. K. Akhtar and M. Kumar, "Detection of DDoS Attack Using Naive Bayes Classifier," in *Advancements in Security and Privacy Initiatives for Multimedia Images*, ed: IGI Global, 2021, pp. 214-225.

[9] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," *Technologies,* vol. 9, p. 14, 2021.

[10] S. Khorsandroo, A. G. Sánchez, A. S. Tosun, J. M. Arco, and R. Doriguzzi-Corin, "Hybrid SDN evolution: A comprehensive survey of the state-of-the-art," *Computer Networks,* vol. 192, p. 107981, 2021.

[11] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges," *Computer Networks,* vol. 72, pp. 74-98, 2014.

[12] A. Bonguet and M. Bellaiche, "A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing," *Future Internet,* vol. 9, p. 43, 2017.

[13] B. Chu, T. J. Holt, and G. J. Ahn, "Examining the creation, distribution, and function of malware on-line," *National Institute of Justice, Washington, DC,* 2010.

[14] E. C. Ogu, O. A. Ojesanmi, O. Awodele, and S. Kuyoro, "A botnets circumspection: The current threat landscape, and what we know so far," *Information,* vol. 10, p. 337, 2019.

[15] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks,* vol. 13, p. 1550147717741463, 2017.

[16] I. Sreeram and V. P. K. Vuppala, "HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm," *Applied computing and informatics,* vol. 15, pp. 59-66, 2019.

[17] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE,* vol. 103, pp. 14-76, 2014.

[18] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, pp. 493-501, 2019.

[19] B. Isyaku, M. S. Mohd Zahid, M. Bte Kamat, K. Abu Bakar, and F. A. Ghaleb, "Software defined networking flow table management of openflow switches performance and security challenges: A survey," *Future Internet*, vol. 12, p. 147, 2020.

[20] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *2015 international conference on computing, networking and communications (ICNC)*, 2015, pp. 77-81.

[21] K. Shinan, K. Alsubhi, A. Alzahrani, and M. U. Ashraf, "Machine learning-based botnet detection in software-defined network: a systematic review," *Symmetry*, vol. 13, p. 866, 2021.

[22] T. Abhiroop, S. Babu, and B. Manoj, "A machine learning approach for detecting DoS attacks in SDN switches," in *2018 Twenty Fourth National Conference on Communications (NCC)*, 2018, pp. 1-6.

[23] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Security and Communication Networks*, vol. 2018, 2018.

[24] R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine learning algorithms to detect DDoS attacks in SDN," *Concurrency and Computation: Practice and Experience*, vol. 32, p. e5402, 2020.

[25] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Machine-learning techniques for detecting attacks in SDN," in *2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)*, 2019, pp. 277-281.

[26] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Computers & Security*, vol. 88, p. 101645, 2020.

[27] B. Karan, D. Narayan, and P. Hiremath, "Detection of DDoS attacks in software defined networks," in *2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS)*, 2018, pp. 265-270.

[28] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," in *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, pp. 1-6.

[29] C. Li, Y. Wu, X. Yuan, Z. Sun, W. Wang, X. Li, *et al.*, "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN," *International Journal of Communication Systems*, vol. 31, p. e3497, 2018.

[30] A. Jose, L. R. Nair, and V. Paul, "Mitigation of Distributed Denial of Service (DDoS) Attacks over Software Defined Networks (SDN) using Machine Learning and Deep Learning Techniques," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, 2019.

[31] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K.-K. R. Choo, *et al.*, "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *Ieee Access*, vol. 8, pp. 53972-53983, 2020.

[32] P. Kaur, M. Kumar, and A. Bhandari, "A review of detection approaches for distributed denial of service attacks," *Systems Science & Control Engineering*, vol. 5, pp. 301-320, 2017.

[33] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, pp. 1-22, 2019.

[34] H. Majed, H. N. Noura, O. Salman, M. Malli, and A. Chehab, "Efficient and Secure Statistical DDoS Detection Scheme," in *ICETE (1)*, 2020, pp. 153-161.