# A Review on Distributed Denial of Service Detection in Software Defined Network

**Khadija Shazly[*1], Dina A. Salem[2], Nacereddine Hammami[3], Ahmed I. B. ElSeddawy[4]**

[1] Faculty of Computer and Information, Mansoura University, Egypt
[2] Misr University for Science and Technology (MUST) Faculty of Engineering Department of computer and software engineering, Egypt

[3]Computer Engineering Department, College of Engineering and Computer Sciences, Mustaqbal University, Buraydah 52547, Saudi Arabia

[4]Arab Academy for Science and Technology and Maritime Transport, Egypt

Emails: khadijashazly@students.mans.edu.eg ; dena.salem@gmail.com; nshammami-t@uom.edu.sa ; ahmed.bahgat@aast.edu

**Abstract**

Network security has become considerably essential because of the expansion of the internet of things (IoT) devices. One of the greatest hazards of today's networks is distributed denial of service (DDoS) attacks, which could destroy critical network services. Recently numerous IoT devices are unsuspectingly attacked by DDoS. To securely manage IoT equipment, researchers have introduced software-defined networks (SDN). This paper aims to analyze and discuss machine learning-based systems for SDN security networks from DDoS attacks. 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 attacks 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 deep learning methods are the ability to do both feature extraction along with data classification; the ability to extract 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 a graphics processing unit (GPU) rather than a central processing unit (CPU) for carrying out the matrix operations, making the processes computationally effective and fast.

**Keywords:** IoT; Botnets; Machine Learning; Feature Selection.

## 1. Introduction

For the header and the footer, just change the journal name and the abbreviation, then leave all other information for our production team at the ASPG editorial office to be updated after your paper acceptance. Lately, network security has come to be mainly crucial due to the fact that Distributed Denial of Service (DDoS) gravely threatens network threats network security [1]. Consuming the computing resources of a victim is the target of the attacker by sending a malicious message to the victim host, preventing the host to deliver services to users.

The Internet of Things (IoT) is a promising technology in the field of networking. It allows data transmission with the world wide web between IP-enabled networked devices [2]. The applications of IoT include self-driving cars, smartphones, cameras, printers, national finance data centers,

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

ZigBee, and Wireless Fidelity (Wifi) networks. The IoT is considered a huge network with 24 milliard terminals in 2019 and is expected to be 76 milliard terminals in 2026 [3]. The share of IoT in the global economy is $11 thousand milliard [4]

Unfortunately, the increase in applications of IoT allows numerous attacks and increases the threats. The pioneer companies in cyber security reported that one attack faces an IoT device every two minutes, and the total number of attacks reaches 121,588 in 2018 [5-6].

Different types of malware that attack IoT devices exist, such as Bashlite, Ashlite, and Mirai, which damage the IoT infrastructure, by reaching sensitive authentication authorizations. Mirai infected around two million IoT devices [7]. Mirai and Bashlit are considered botnet attacks; which are used to run bots on all devices connected to the internet [8-11]. The wide and rapid spread of botnet attacks between connected devices to the internet reflects the significant danger of these types of attacks. It is always required to build an effective and powerful algorithm to save IoT devices from botnet attacks.

Artificial intelligence (AI) is one solution to build an intrusion detection system (IDS) that has the ability to detect modern patterns of botnet attacks [12]. Deep learning, deep recurrent neural network, and machine learning are advances in AI that are used to prevent botnet attacks from IoT devices [13-15]. This paper proposes a new detection algorithm, which integrates the CNN algorithm into the SD-IoT controller. Developing a framework to detect and prevent botnet attacks attracts many researchers. The IDS is an effective mechanism that aims to protect the network from malicious attacks by detecting new attacks and batching them by matching them with signature attacks. There are two main algorithms for intrusion detection; anomaly-based detection and signature-based detection.

A deep learning algorithm for different applications, such as image recognition, localization, and security is introduced in [16]. An IDS for smart cities using neural networks and multilayer perceptron models with high accuracy is presented in [17]. A classification algorithm based on support vector machine (SVM), K-nearest neighbor (KNN), and native Bayes (NB) is presented in [18]. Machine learning is also used to extract features for improving the system depending on a method to renew krill herd position to obtain the optimal global solution proposed in [19]. Different advanced AI algorithms such as nature-inspired computation intelligence and other methods of machine learning are proposed in [20-26].

Botnet detection algorithms are divided into two main types network-based and host-based [27–31]. In [27-28] a comprehensive architecture for IDS and classifier is proposed, and more than a machine learning algorithm is used; ensemble learning algorithm, neural network algorithm, and kerenal algorithm. It achieves results better than any prior methods by 20 %. A port scanning attack detection mechanism is proposed and introduced in [29] it provides 99% accuracy in the detection of botnet attacks. The autoencoders are used to detect abnormality observation in wireless sensor networks (WSNs) which represent a part of IoT devices. The observation algorithm includes two locations; the first is in the IoT cloud while the second is in the sensor itself.

Autoencoders are mostly used for anomaly detection in wireless sensor networks (WSNs) that are embedded in IoT devices. The algorithm used for detection purposes involves two components—one is located in the IoT cloud, while the other is placed in the sensors. It was seen that the autoencoder learning features enabled adaptation to environmental changes in the IoT network.

The comparison between autoencoders and other deep learning models such as; recurrent neural network, self-taught learning, and vanilla deep neural net indicate that autoencoders provides efficient outcomes and met the constraints (storing capacity, computing power) of IoT system [32-35].

In [36] a novel algorithm is presented to detect attacks in IoT systems without the participation of humans. Another algorithm is based on multi-stages; reduction, support vector machine, and the feed forward neural network stage. The results indicate better results than other classification algorithms [37]. Another research [38] demonstrates the behaviors of network traffic by inspecting the packets using a deep learning method.

Another proposed system for the detection of a botnet for Linux is presented in [39]. The authors used 10033 files that include 4002 infected files. The results indicate the classifier achieves 94% accuracy. A different idea proposes a method using the office embedding method to recognize text

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

and convert attacks into an integer format. This method detects four attacks and evaluated them for loss and accuracy. The results show a better enhancement in the model while the processing time is increased [40]. Another detection system for botnet attacks is presented [41] and achieves 99% accuracy.

## 2. DDoS attacks

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 [42]. Therefore, SDN deployment in cloud computing and data center environments gives flexible and reliable network architecture [43].

On the other hand, SDNs are susceptible to several security challenges such as port scans, Trojans, Worms, denial of service attacks (DoS), etc. [44]. 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 [45]. All botnet is remotely placed under the supervision of a human operator known as a bot master [46]. A 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 [47].

In a DDoS attack, the incoming packet rate toward 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 attacks: 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 [48]. 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. 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) [49]. 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 onto the controller in cases where a malicious flow can be ruled within the flow table [50].

In addition, the flow format has several significant properties for SDN. The SDN controller utilizes a southbound protocol involving OpenFlow to act toward 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 [51].

Figure 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

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

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.

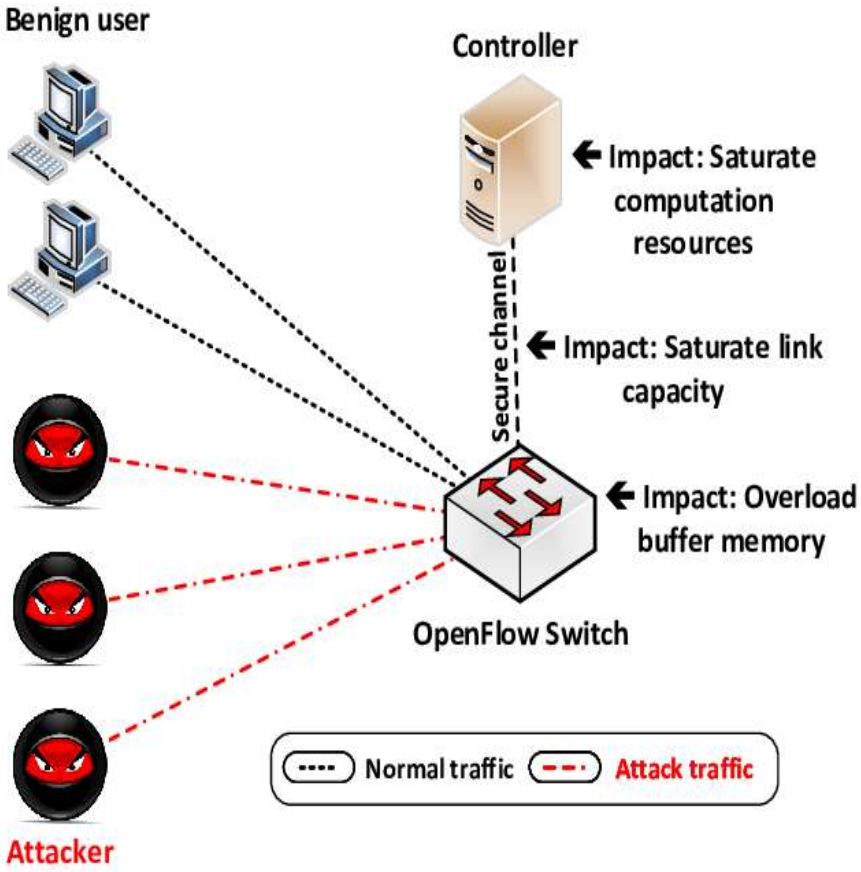


Figure 1: SDN DDoS attack resulting from compromised nodes.

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. Figure 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 [51-53].

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

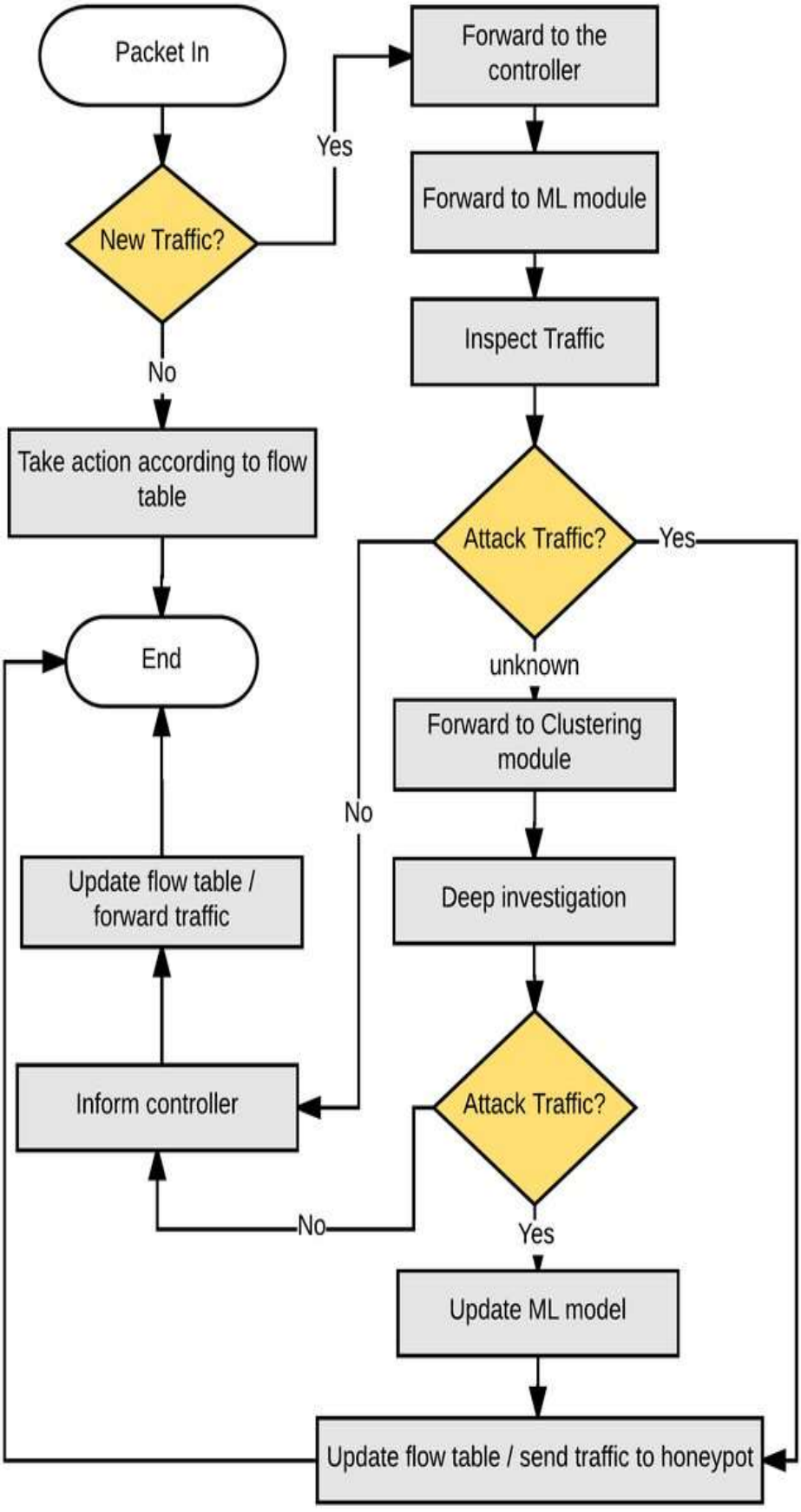


Figure 2: The Typical Attack detection module workflow.

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

## 3. Systems to detect DDoS

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) [54] 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) [55] 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) [56] 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. The 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) [57] 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) [58] 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) [59] 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) [60] designed a model that utilized 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 deep-learning algorithms in SDN-based constructions [48-50].

Other deep learning algorithms [51] were also applied in SDN architectures to identify DDoS and attack detection. Li et al. (2018) [61] presented a system that allows detecting and defending 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) [62] 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) [63] 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%. The goal of the optimization algorithm is to find the best path from origin to destination, making the most of the available SDN-

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

WAN resources. To accomplish this, it considers the desired flow and the existing network conditions [64-69].

Table 1: Previous Work

| Recent Researches | Method | Results |
|---|---|---|
| Karan (2018) [59] | DNN and SVM | DNN achieved higher accuracy (92.30%) which is higher than SVM |
| Liu (2018) [60] | 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) by about 3-9% and outperforms the performance of the Additive Increase Multiplicative Decrease (AIMD) algorithm by about 18-28% |
| Li (2018) [61] | 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) [62] | 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) [63] | 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. |
| Abhiroop (2018) [54] | 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) [55] | Based on six-tuple features collected from SDN data, SVM | Because ICMP packets do not contain a port address, detecting ICMP traffic was difficult. The achieved accuracy is 95.24%. |
| Santos and Moreno (2019) [56] | 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 model's results are: the DT achieves 99%, the MLP achieves 98%, and the SVM archive 92% |
| Elsayed and Jurcut (2019) [56] | J48 algorithm | J48 is a better method for detecting DDoS attacks compared with SVM, Naive Bayes, and Random Forest |
| Wang (2020) [57] | Artificial Neural Network-based Dynamic Multilayer perceptron (MLP) | The proposed model is better than the machine learning models investigated in this work which include, MLP, DT: J48, BN, and RNN |

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

From table 1, 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. 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, most study takes consecration to test a single dataset, while 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 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.

**Funding:** "This research received no external funding"

**Conflicts of Interest:** "The authors declare no conflict of interest."

**References**

[1] I. Cviti´c, D. Perakovi´c, B. Gupta, K. K. R. Choo, Boosting-based DDoS detection in the internet of things systems. IEEE Int. Things J., 2021.
[2] Albulayhi K.; Smadi, A.A. Sheldon, F.T. Abercrombie, R.K, "IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors 21, 6432, 2021.
[3] Statistical Portal. Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions). Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide.
[4] Rose, K.; Eldridge, S.; Chapin, L. The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. 2015.
[5] Cisco, Cisco Visual Networking Index (VNI) global Mobile data traffic Forecast update, 2017–2022, Cisco Systems Inc., San Jose, CA, USA, 2019.
[6] Broadcom, "Symantec Internet Security Threat Report 2019. 24, 2020.
[7] A. Marzano, D. Alexander, O. Fonseca et al., "The Evolution of Bashlite and Mirai IoT botnets. Proceedings of the IEEE Symposium on Computers and Communications, 813–818, IEEE, Natal, Brazil, 2018.
[8] Mohit kumar, "IoT botnets found using Default Credentials for C&C server Databases. 2020,
[9] Bankinfosecurity, "Massive botnet attack used more than 400,000 IoT devices. 2020, https://www.bankinfosecurity.com/massivebotnet-attack-used-more-than-400000-iotdevices-a-12841.
[10] Enigmasoftware, "BASHLITE Malware Hits Over One Million IoT Devices. 2020, https://www.enigmasoftware.com/ bashlite-malware-hits-one-million-iot-devices/.
[11] Thingbots,"The Future of Botnets in the Internet of Things. 2020, https://securityintelligence.com/thingbots-the-futureof- botnets-in-the-internet-of-things.
[12] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to Snort system .Future Generation Computer Systems, 80, 157–170, 2018.

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

[13] M. A. Ferrag and L. D.C. Maglaras, "A novel deep learning and Blockchain-based Energy Exchange framework for smart Grids. IEEE Transactions on Engineering Management, 67(4), 2019.
[14] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study. Journal of Information Security and Applications, 50,102419, 2020.
[15] O. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, "A deep Blockchain framework-enabled Collaborative intrusion detection for protecting IoT and Cloud networks. IEEE Internet Things J, 8(12), 2020.
[16] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. IEEE Communications Surveys & Tutorials, 22(3), 2018.
[17] X. Xie, D. Wu, S. Liu, and R. Li, "IoT Data Analytics Using Deep Learning," 2017, https://arxiv.org/abs/1708.03854.
[18] F. Alam, R. Mehmood, I. Katib, and A. Albeshri, "Analysis of eight data mining algorithms for smarter internet of things (IoT). Procedia Computer Science, 98, 437–442, 2016.
[19] X. Li, P. Yi, W. Wei, Y. Jiang, Tian, and L. Lnnls-Kh, "A feature selection method for network intrusion detection. Secur. Commun. Netw., Article ID 8830431, 22 pages, 2021.
[20] S. Yilmaz and S. Sen, "Early detection of botnet Activities using Grammatical Evolution," in Applications of Evolutionary Computation., 395–404, Springer International Publishing, Berlin/Heidelberg, Germany, 2019.
[21] M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University - Computer and Information Sciences, 31(4), 541–553, 2019.
[22] A. Al Shorman, H. Faris, and I. Aljarah, "Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection. Journal of Ambient Intelligence and Humanized Computing, 11 (7), 2809–2825, 2020.
[23] K.-C. Lin, S.-Y. Chen, and J. C. Hung, "Botnet detection using support vector machines with artificial fish Swarm algorithm. Journal of Applied Mathematics, pp. 1–9, 2014.
[24] Y. Yu, J. Long, F. Liu, and Z. Cai, "Machine learning combining with visualization for intrusion detection: a survey. Proceedings of the International Conference on Modeling Decisions for Artificial Intelligence, 239–249, Springer, Cham, Sant Juli`a de L`oria, Andorra, September 2016.
[25] K. Shinan, K. Alsubhi, A. Alzahrani, and M. U. Ashraf, "Machine learning-based botnet detection in software-defined network: a systematic review. Symmetry, 13 (5), 2021.
[26] M. Alauthman, N. Aslam, M. Al-kasassbeh, S. Khan, A. Al- Qerem, and K.-K. Raymond Choo, "An efficient reinforcement learning-based Botnet detection approach. Journal of Network and Computer Applications, 150, Article ID 102479, 2020.
[27] Abu Al-Haija, Q. Top-Down Machine Learning-Based Architecture for Cyberattacks Identification and Classification in Io Communication Networks. Front. Big Data 2022.
[28] Abu Al-Haija, Q.; Al-Badawi, A. Attack-Aware IoT Network Traffic Routing Leveraging Ensemble Learning. Sensors, 22, 241, 2022.
[29] Al-Haija, Q.A.; Saleh, E.; Alnabhan, M. Detecting Port Scan Attacks Using Logistic Regression. Proceedings of the 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Khobar, Saudi Arabia, 1-5, 2021.
[30] Tsogbaatar, E.; Bhuyan, M.H.; Taenaka, Y.; Fall, D.; Gonchigsumlaa, K.; Elmroth, E.; Kadobayashi, Y. DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT. Internet Things 2021.
[31] Rezaei, A. Using Ensemble Learning Technique for Detecting Botnet on IoT. SN Comput. Sci. 4, 2021.
[32] Tsogbaatar, E.; Bhuyan, M.H.; Taenaka, Y.; Fall, D.; Gonchigsumlaa, K.; Elmroth, E.; Kadobayashi, Y. DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT. Internet Things 2021, 14.
[33] Rezaei, A. Using Ensemble Learning Technique for Detecting Botnet on IoT. SN Comput. Sci. 4, 2021.
[34] Özçelik, M.; Chalabianloo, N.; Gür, G. Software-Defined Edge Defense against IoT-Based DDoS. Proceedings of the IEEE International Conference on Computer and Information Technology (CIT 17), Helsinki, Finland, 21–23 August 2017.
[35] Summerville, D.H.; Zach, K.M.; Chen, Y. Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices. Proceedings of the 2015 IEEE 34th International Performance

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

Computing and Communications Conference (IPCCC 15), Mamkomg, China, 14–16 December 2015.
[36] Yang, L.; Shami, A. A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams. IEEE Internet Things Mag. , 4, 96-101, 2021.
[37] Qaddoura, R.; Al-Zoubi, A.M.; Almomani, I.; Faris, H. A Multi-Stage Classification Approach for IoT Intrusion Detection Based on Clustering with Oversampling. Appl. Sci. 11, 2021.
[38] Shi, W.C.; Sun, H.M. DeepBot: A time-based botnet detection with deep learning. Soft. Comput. 24, 16605-16616, 2020.
[39] Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 118-122, September 2018.
[40] McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet Detection in the Internet of Things using Deep Learning Approaches. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 1-8, 2018.
[41] Stiawan, D.; Suryani, M.E.; Susanto; Idris, M.Y.; Aldalaien, M.N.; Alsharif, N.; Budiarto, R. Ping Flood Attack Pattern Recognition Using a K-Means Algorithm in an Internet of Things (IoT) Network. IEEE Access , 9, 116475–116484, 2021.
[42] 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, 192, 107981, 2021.
[43] M. Jammal, T. Singh, A. Shami, R. Asal, and Y. Li, "Software defined networking: State of the art and research challenges. Computer Networks, 72, 74-98, 2014.
[44] A. Bonguet and M. Bellaiche, "A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. Future Internet, 9, 43, 2017.
[45] 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.
[46] 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, 10, 337, 2019.
[47] 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, 13, 1550147717741463, 2017.
[48] 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, 15, 59-66, 2019.
[49] 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, 103, 14-76, 2014.
[50] 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.
[51] 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.
[52] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers. Proceeding of international conference on computing, networking and communications (ICNC), 77-81, 2015.
[53] K. Shinan, K. Alsubhi, A. Alzahrani, and M. U. Ashraf, "Machine learning-based botnet detection in software-defined network: a systematic review. Symmetry, 13, 866, 2021.
[54] T. Abhiroop, S. Babu, and B. Manoj, "A machine learning approach for detecting DoS attacks in SDN switches," Proceeding of National Conference on Communications (NCC), 1-6. 2018.
[55] 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, 2018.
[56] 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, 32, e5402, 2020.
[57] 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), 277-281, 2019.
[58] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Computers & Security, 88, 101645, 2020.

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022

[59] B. Karan, D. Narayan, and P. Hiremath, "Detection of DDoS attacks in software defined networks," Proceeding of International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), 265-270, 2018.
[60] Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks," Proceeding of IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1-6, 2018.
[61] 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, 31, e3497, 2018.
[62] 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), 8, 2019.
[63] 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, 8, 53972-53983, 2020.
[64] El-Kenawy, El-Sayed M., Marwa Eid, and Alshimaa H. Ismail. "A New Model for Measuring Customer Utility Trust in Online Auctions." International Journal of Computer Applications 975: 8887.
[65] El-kenawy, El-Sayed M., Hattan F. Abutarboush, Ali Wagdy Mohamed, and Abdelhameed Ibrahim. "Advance artificial intelligence technique for designing double T-shaped monopole antenna." CMC-COMPUTERS MATERIALS & CONTINUA 69, no. 3 (2021): 2983-2995.
[66] El-kenawy, El-Sayed M., Marwa M. Eid, and Abdelhameed Ibrahim. "Anemia estimation for covid-19 patients using a machine learning model." Journal of Computer Science and Information Systems 17, no. 11 (2021): 2535-1451.
[67] Ibrahim, Abdelhameed, Seyedali Mirjalili, Mohammed El-Said, Sherif SM Ghoneim, Mosleh M. Al-Harthi, Tarek F. Ibrahim, and El-Sayed M. El-Kenawy. "Wind speed ensemble forecasting based on deep learning using adaptive dynamic optimization algorithm." IEEE Access 9 (2021): 125787-125804.
[68] Mohamed Saber, Efficient Phase Recovery System. Indonesian Journal of Electrical Engineering and Computer Science, 5 (1), 123-129, 2017.
[69] Mohamed Saber, A novel design and Implementation of FBMC transceiver for low power applications. Indonesian Journal of Electrical Engineering and Informatics, 8(1), 83-93, 2020.

Doi: https://doi.org/10.54216/IJWAC.050201
Received: March 04, 2022 Accepted: October 30, 2022