

DDoS attack detection in software defined networking controller using machine learning techniques

Abbas Jasem Altamemi, Aladdin Abdulhassan, Nawfal Turki Obeis
College of Information Technology, University of Babylon, Babylon, Iraq

Article Info

Article history:

Received May 28, 2022
Revised Jun 10, 2022
Accepted Jul 24, 2022

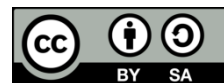
Keywords:

DDoS attacks
Feature selection
Logistic regression
Machine learning
Software defined networking

ABSTRACT

The term software defined networking (SDN) is a network model that contributes to redefining the network characteristics by making the components of this network programmable, monitoring the network faster and larger, operating with the networks from a central location, as well as the possibility of detecting fraudulent traffic and detecting special malfunctions in a simple and effective way. In addition, it is the land of many security threats that lead to the complete suspension of this network. To mitigate this attack this paper based on the use of machine learning techniques contribute to the rapid detection of these attacks and methods were evaluated detecting DDoS attacks and choosing the optimum accuracy for classifying these types within the SDN, the results showed that the proposed system provides the better results of accuracy to detect the DDos attack in SDN network as 99.90% accuracy of Decision Tree (DT) algorithm.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Abbas Jasem Altamemi
College of Information Technology, University of Babylon
51002, Babylon, Iraq
Email: abbas.j.altamemi@gmail.com

1. INTRODUCTION

Software defined networking (SDN) specified by the process of defining the software by separating the level of control from the level of data. SDN networks is the model that contributes to addressing the limitations of traditional network design [1], where it consists of three main levels: the private level is the data plane device, the level of the controller, and the level of the application. Depending on the controller's preference, the data plane carries network traffic. To decide traffic flow, the control plane computes routing tables [2]. A group of other applications that are dealt with, such as load balancing, firewalls, and quality of service applications [3], which SDN networks contribute to improving their performance by separating the control units and their functions in the network from the statement generating units [4]. Control applications running on a logically centralized controller will regulate several routers in the network [5].

Applications can only access the complete network's information via the SDN. Load balancing and intrusion detection are much easier when many apps are integrated [6]. The application instructs the controller to reprogramme the data plane whenever an abnormality is identified [7]. Where these devices within the network contain special open interfaces that are managed by software, therefore the control and data planes run on routers dispersed across the network [8].

It is possible to reconfigure several devices simultaneously in SDN architecture. Configuring network devices is done at this tier using the application layer [9]. The SDN architecture's control layer (control plane) consists of a single controller. APIs are used to communicate between the two levels [10].

DDoS attacks have a significant influence on the SDN's uptime. DDoS assaults have the greatest effect on the SDN controller since it is the most vulnerable point of failure. When it comes to SDN, there is only one point of failure: the centrally controlled controller. The data plane and control plane use a secure south-bound link to exchange messages. Even a little amount of channel congestion may cause enormous delays in the network.

Mehr *et al.* [11] a tree network architecture, they use the mininet emulator to conduct a DDoS attack on the ryu controller. Using a machine learning technology, support vector machines (SVM), they identify DDoS attacks via the installation of flows in switches and evaluate the time attack pattern of the DDoS assault when determining their detection. Using our detection technology, we were able to minimize the impact of DDoS assaults on the Ryu controller by 36%.

Rahman *et al.* [12] DDoS attacks in an SDN network were detected and blocked using a variety of machine learning algorithms, including J48, RF, SVM and K-NN. Complete reliance on a script that contributes to the process of mitigating, preventing and reducing attacks and their impact on SDN networks using the model that was trained and selected as the best fit for the proposed network during the assessment phase. The findings revealed that J48 outperformed the other algorithms, particularly in required time for training and testing states.

Sun *et al.* [13] proposed a way for SDN controllers to identify DDoS attacks in real-time. Entropy is initially used after an abnormal notification is provided, the DDoS attack feature in the SDN environment is studied to extract critical features linked to the attack. Flow entry of open flow switch is retrieved. Classification of real-time traffic in order to identify DDoS attacks is made with ANN method called BiLSTM-RNN. When compared to other approaches, this one has the ability to identify DDoS attacks and minimize controller overhead in an SDN context more effectively.

Dehkordi *et al.* [14] they suggested a unique method for identifying DDoS attack in SDN. This method's three collectors are entropy-based and classification-based. The UNB-ISCX, CTU-13, and ISOT datasets, the results suggest that the used method outperforms the competition in detecting SDN-DDoS threat.

Chen *et al.* [15] a multi-layer IoT DDoS attack detection based on M.L is suggested, which comprises IoT devices, gateways, SDN switches, and cloud servers. As a first step, they install eight sensor-equipped smart poles across the campus, collecting data from each one through wired or wireless networks. Then, depending on the sort of DDoS assault, they extract the characteristics. The used system was capable of properly detecting DDoS assaults in our tests. In addition, the used IoT DDoS assault detection system's blacklists may be used by the SDN controller to efficiently block harmful devices.

Sen *et al.* [16] on a private network dataset in an SDN setting, AdaBoosting was employed as a basic classifier with decision stumps. The model exhibited a 93 percent detection accuracy and a low false-positive rate. They reported their findings after evaluating and comparing the model's performance with several M.L approaches.

Tan *et al.* [17] the SDN DDoS environment detected and countered using this technology. First, they use the detection state for DDoS on the data layer to monitor the network for unexpected flows. They identify abnormal flows based on the detection trigger mechanism and the rate asymmetry characteristics of the streams were relied upon using the machine learning approach based on K-Means and K-nearest neighbors (KNN) algorithms. Finally, the controller will react to the assaults by implementing the appropriate countermeasures. New framework for control plane and data plane cooperative detection techniques they successfully enhance detection accuracy and efficiency while preventing SDN threats.

Ahmad *et al.* [18] SDN DoS and DDoS attacks may be mitigated using machine learning methods. In order to derive key implications relying on security detection based on machine learning algorithms for future communication networks and evaluating these methods based on the controller and the extent of their impact on them by DDOS. The SVM's accuracy was determined to be 97.5%.

Ahuja *et al.* [19] use a variety of deep learning algorithms to categorize traffic into normal and harmful groups depending on the characteristics in the dataset with one classes. According to the findings, using the SAE-MLP produced an accuracy score of 99.75%, the maximum possible. In this paper, improving the security of DDoS attack detection in SDN controller based on machine learning techniques has been proposed. It is totally presented as follows: 1. introduction, 2. the proposed method, 3. method, 4. results and discussion, and 5. conclusion.

2. THE PROPOSED METHOD

The proposed security of SDN controller with DDoS attack executed with the three main stages and it based on the three machine learning algorithms, which they are mentioned above and the system stages as follow: i) Stage one: data pre-processing on full data set to transform the row data of dataset in a useful and

efficient format; ii) Stage two: data classification depending on the machine learning classifiers; iii) Stage three: using machine learning algorithms and find results.

a. System implementation

The used system was implemented based on an environment based on the following specifications Table 1. Besides, the code of proposed the system has been written in python programming language.

Table 1. Environment specifications for the proposed system

Operating systems	Windows 10
CPU	Core (TM) I5-3630
RAM	16.00 GB
Implementation Tools	Python, Cloud Azure

b. Proposed approach

The proposed approach based on the three machine learning algorithms and the used dataset as real-time traffic dataset, it provides the most up-to-date and benign frequent DDoS assaults, which closely reflects the real-time data (PCAPs). The data traffic analyzed with CICflowmeter-V3 according to the labeled state for time stamp, addresses of source IP /destination IP, ports, protocols, and security issues methods are also included (CSV files).

A set of evaluation scales was relied upon, based on the concept of the confusion matrix, where a set of equations with a special description was relied upon as in (1) to (6).

1. Precision: it is the TP number divided by TP and FP numbers. It computed based on (2) [20].

$$\text{Precision} = \frac{TP}{TP+FP} \quad (1)$$

2. Accuracy: it is the correct predictions divided by the total predictions number. It calculated based on (2) [21].

$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FP + FN} \quad (2)$$

3. Recall: it is TP number divided by TP with FN numbers. This metric can be computed based on (3) [22].

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

4. F-measure: It is one of the statistical analysis methods for measuring the accuracy of the test, as it is based on the accuracy of the test and its retrieval, depending on the accuracy resulting from the real positive results divided by the number of all positive results, including those that have not been correctly determined. An of this metric can be computed based on (4) [23].

$$F - \text{Measure} = \frac{(2*TP)}{(2*TP+FN+FP)} \quad (4)$$

5. Detection rate (DR): It measures of identified positive (anomaly) iteams from all the actual positive instances. This metric can be computed based on (2.6) [24].

$$\text{Detection Rate(DR)} = \frac{TP}{TP+ FN} \quad (5)$$

6. False alert rate (FAR): it represents the proportion of negative prediction; this is mistakenly considered as positive (anomaly) for all negative predictions. The lower value is the better. This metric can be computed based on (6) [25].

$$\text{False Alert Rate(FAR)} = \frac{FP}{FP+ TN} \quad (6)$$

The confusion matrix as shown in Table 2 is a matrix used to describe the classification performance based on the test data.

- TP: It denotes to proper classified values.
- FN: It showed incorrectly classified.

- FP: It showed the negative values incorrectly predicted and classified.
- TN: It showed negative instances which properly predicted by the classification model [26].

Table 2. Confusion matrixes

Confusion Matrix		Predicated Class	
Actual Class	Positive +	TP	FN
	Negative -	FP	TN

3. METHOD

The used method based on LR, NB, DT machine learning algorithms and the main steps showed in Figure 1. The proposed matching strategy based on the matched the incoming request real-time from the nodes compared with the trained classifier stored data behavior as (SDN specific dataset generated by using mininet emulator and used for traffic classification by machine learning). It compared the source, destination IP, and MAC addresses if the incoming request has the authorized values as matched it will wait for process and classified as the normal traffic. In addition, the proposed trained model can classified as attack traffic if it is not matched packet details with the stored behavior, which matched, in the first step.

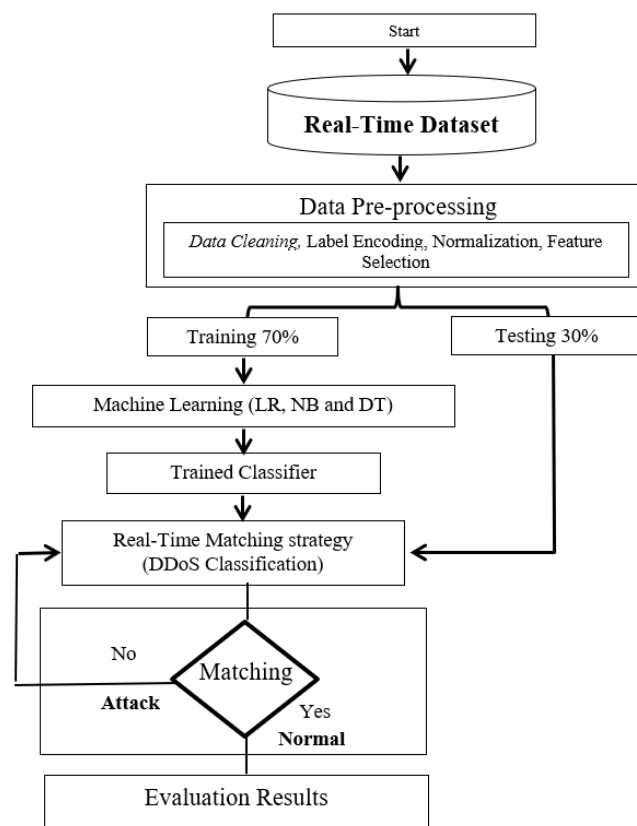


Figure 1. The proposed machine learning system model

4. RESULTS AND DISCUSSION

The proposed system implemented in online state to test and evaluated incoming request directly after different of operation matching incoming requests as DDoS attack traffic or normal data traffic. The results calculated based on three-machine learning algorithms are logistic regression (LR) algorithm, Naive Bayes (NB) algorithm, and Decision Tree (DT) algorithm. The proposed algorithms build implicit or explicit models from the given data to build systems that can learn from data without being programmed, which it helps to find the hidden patterns and leads for better insights. as showed in Figure 2.

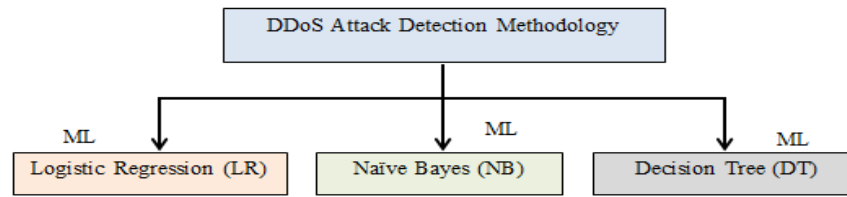


Figure 2. The used machine learning algorithms

4.1. The 1st case study

The 1st case study based on the logistic regression (LR) to build a model for detecting DDoS attacks from the training and testing SDN environment by providing a linear categorization model to demonstrate a likelihood of a group Y set a feature-vector X . This is done via utilizing a logistic methods to discover a relation between the class and the feature vector. It supposes the distribution $P(Y|X)$, here Y is the class and X is the feature-vector, is on a borderline shape and after that demonstrates it from the training data. Table 3 shows the accuracy and time details with the confusion matrix evaluated parameters as false positive rate and false negative rate of DDoS attack detection in SDN controller based on the LR. Besides, there are other evaluation metrics Table 4, Figure 3 of the proposed system based on LR classifiers.

Table 3. The results of LR algorithm for DDoS attack detection case study

Method Name	Accuracy	False Positive Rate	False Negative Rate	Time
Logistic Regression (LR)	72.65%	0	71511	7.844 sec

Table 4. Evaluation Details of the DDoS attack detection with LR

Evaluation Parameters	Machine Learning Algorithms
	Logistic Regression (LR)
Precision	0.73
Recall	1.0
F-Measure	0.84
Detection Rate (DR)	0
False Alert Rate (FAR)	0
TP Rate	0
TN Rate	190633

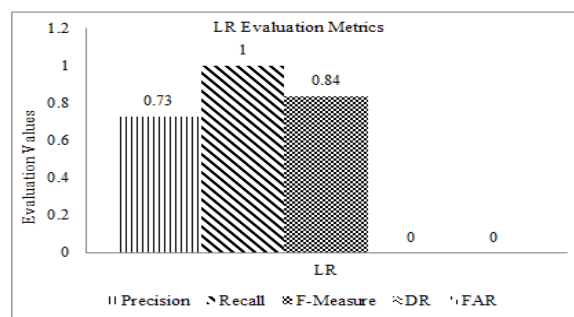


Figure 3. Precision, recall, F-measure, DR and FAR of LR case study

4.2. The 2nd case study

The 2nd case study is based on the naive bayes (NB) algorithm as a technique of naive bayes classifier depended on the so-called bayesian theorem to classify the traffic as normal and abnormal of DDoS attack in SDN. In spite of its simplicity but can superior to many sophisticated classification methods. It is possible to describe the used model classifier as a machine learning model that is used to discriminate between various objects based on certain characteristics. When it comes to machine learning, The probabilistic model naive bayes is used in the classification task. Table 5 show the main used NB evaluation metrics of DDoS attack detection, besides, there are other evaluation metrics show in Table 6, Figure 4 of the proposed system based on NB classifiers.

Table 5. The results of NB algorithm for DDoS attack detection case study

Method Name	Accuracy	False Positive Rate	False Negative Rate	Time
Naive Bayes (NB)	52.88 %	123371	0	1.910 sec

Table 6. Evaluation details of the DDoS attack detection with NB

Evaluation Parameters	Machine Learning Algorithms Naive Bayes (NB)
Precision	1.0
Recall	0.35
F-Measure	0.52
Detection Rate (DR)	1
False Alert Rate (FAR)	0.647
TP Rate	71511
TN Rate	67262

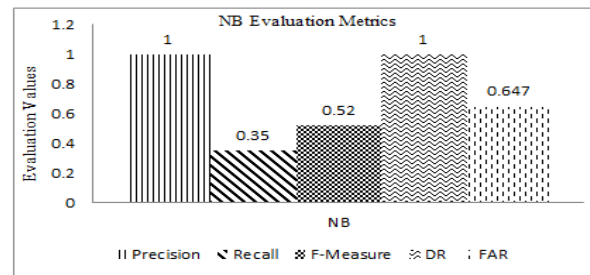


Figure 4. Precision, recall, F-measure, DR and FAR of NB case study

4.3. The 3rd case study

It is based on the decision tree (DT) algorithm and is used in SDN networks to automatically identify the classification approach as it consists of a group of nodes located inside the trees. which are pre-classified based on branches and a weighted test scale. It is possible to classify an integrated text document starting from the root, depending on the structure of the query, until a specific page is reached within the system. Table 7 shows the accuracy rate and required time to build a model of the DT algorithm. Besides, there are other evaluation metrics shown in Table 8 and Figure 5 of the proposed system based on DT classifiers.

Table 7. The results of DT algorithm for DDoS attack detection case study

Method Name	Accuracy	False Positive Rate	False Negative Rate	Time
Decision Tree (DT)	99.90 %	0	0	11.919 sec

Table 8. Evaluation details of the DDoS attack detection with DT

Evaluation Parameters	Machine Learning Algorithms Decision Tree (DT) Algorithm
Precision	1.0
Recall	0.99
F-Measure	0.99
Detection Rate (DR)	0.99
False Alert Rate (FAR)	0.01
TP Rate	71511
TN Rate	190633

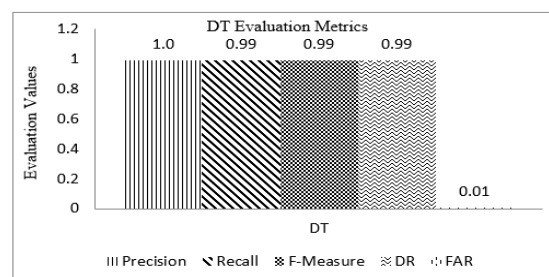


Figure 5. Precision, recall, F-measure, DR and FAR of DT case study

The proposed system compared with the different case studies and with other related works. Table 9, and Figure 6 showed the system comparison among the proposed machine learning algorithms. Furthermore, the proposed system compared with related works as in Table 10. In addition, the system comparison with the other related works the Table 10. The better accuracy result of the proposed system of all case studies are showed in the case of DT as 99.90%.

Table 9. Evaluation details of the used machine learning in DDoS attack detection in SDN environment

Evaluation Parameters	Machine Learning Algorithms		
	LR	NB	DT
Accuracy	72.65	52.88	99.90

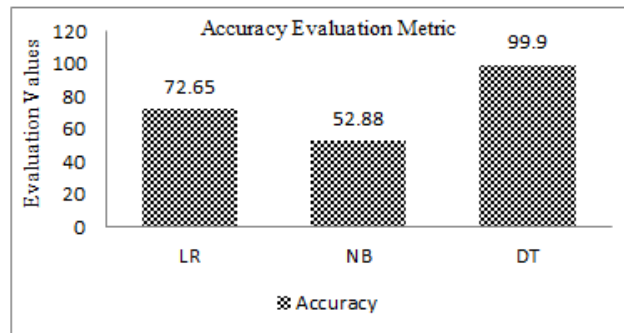


Figure 6. The proposed system accuracy comparison

Table 10. The results of proposed system with the DDoS attack of SDN compared systems

Ref.No	Year	Dataset	Method Name	Accuracy
[20]	2021	Real-Time dataset using RYU API-Mininet	Support-Vector-classifier with Random-Forest (SVC-RF)	98.8 %
			Logistic Regression (LR)	83.69%
[22]	2021	KDD99 dataset	Decision Tree (DT)	78 %
			Support vector machine (SVM)	85 %
[23]	2021	CICIDS2017 dataset	V-NKDE (Voting -Naive	99.67 %
		KDD dataset	Bayes, K Nearest Neighbors,	99.77
		UNSW-NB15 dataset	Decision Tree, and Extra Trees)	98.09
			Logistic Regression (LR)	72.65 %
Proposed system	Real-Time DDoS attack Classification		Naive Bayes (NB)	52.88 %
			Decision Tree (DT)	99.90 %

5. CONCLUSION





The impact of the DDoS is one of the great influences on the network, which may lead to its complete disruption if not dealt with correctly, as these attacks become more complex and are able to easily bypass many traditional protection techniques. Machine learning techniques are being implemented in SDN to overcome network security issues. DT, NB, and LR algorithms are used to build implicit or explicit models from the given data to build systems that can learn from data without being programmed, which it helps to find the hidden patterns and leads for better insights. It is also possible to increase the effective features of this network by relying on M.L, which contribute to the process of intelligent mitigation of attacks that cause DDoS attack. The best results of the machine learning algorithm was DT as 99.90% accuracy compared with the other algorithms.

Future work will involve the development of a mitigation module for the attacks explored in this study. Designing a mitigation plan that is both effective and economical requires addressing various issues, including how to close all suspicious communications utilizing SDN's programmability capability, such as placing blocking rules in edge switches. Among these problems are how to maximize the use of controller and switch resources to implement mitigation policies, how to decrease the mitigator's response time, how to acquire a scalable solution, etc.





REFERENCES

- [1] A. Nayyer, A. K. Sharma, and L. K. Awasthi, "Learning-based hybrid routing for scalability in software defined networks," *Computer Networks*, vol. 198, p. 108362, Oct. 2021, doi: 10.1016/j.comnet.2021.108362.
- [2] A. Hodaie and S. Babaie, "A survey on traffic management in software-defined networks: challenges, effective approaches, and potential measures," *Wireless Personal Communications*, vol. 118, no. 2, pp. 1507–1534, May 2021, doi: 10.1007/s11277-021-08100-3.
- [3] S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Computer Communications*, vol. 181, pp. 274–283, Jan. 2022, doi: 10.1016/j.comcom.2021.09.029.
- [4] A. Yazdinejad, A. Dehghantaha, H. Karimipour, G. Srivastava, and R. M. Parizi, "An efficient packet parser architecture for software-defined 5G networks," *Physical Communication*, vol. 53, p. 101677, Aug. 2022, doi: 10.1016/j.phycom.2022.101677.
- [5] N. M. AbdelAzim, S. F. Fahmy, M. A. Sobh, and A. M. Bahaa Eldin, "A hybrid entropy-based DoS attacks detection system for software defined networks (SDN): A proposed trust mechanism," *Egyptian Informatics Journal*, vol. 22, no. 1, pp. 85–90, Mar. 2021, doi: 10.1016/j.eij.2020.04.005.
- [6] S. Bhardwaj and S. N. Panda, "Performance evaluation using RYU SDN controller in software-defined networking environment," *Wireless Personal Communications*, vol. 122, no. 1, pp. 701–723, Jan. 2022, doi: 10.1007/s11277-021-08920-3.
- [7] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Computer Science Review*, vol. 37, p. 100279, Aug. 2020, doi: 10.1016/j.cosrev.2020.100279.
- [8] A. Saritha, B. R. Reddy, and A. S. Babu, "QEMDD: quantum inspired ensemble model to detect and mitigate DDoS attacks at various layers of SDN architecture," *Wireless Personal Communications*, Aug. 2021, doi: 10.1007/s11277-021-08805-5.
- [9] S. Mahrach and A. Haqiq, "DDoS flooding attack mitigation in software defined networks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, 2020, doi: 10.14569/IJACSA.2020.0110185.
- [10] M. Abdurrohman, D. Prasetyawan, and F. A. Yulianto, "Improving distributed denial of service (DDoS) detection using entropy method in software defined network (SDN)," *ComTech: Computer, Mathematics and Engineering Applications*, vol. 8, no. 4, p. 215, Dec. 2017, doi: 10.21512/comtech.v8i4.3902.
- [11] S. Y. Mehr and B. Ramamurthy, "An SVM based DDoS attack detection method for ryu SDN controller," in *Proceedings of the 15th International Conference on emerging Networking EXperiments and Technologies*, Dec. 2019, pp. 72–73. doi: 10.1145/3360468.3368183.
- [12] O. Rahman, M. A. G. Quraishi, and C.-H. Lung, "DDoS attacks detection and mitigation in SDN using machine learning," in *2019 IEEE World Congress on Services (SERVICES)*, Jul. 2019, pp. 184–189. doi: 10.1109/SERVICES.2019.00051.
- [13] W. Sun, Y. Li, and S. Guan, "An improved method of DDoS attack detection for controller of SDN," in *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)*, Aug. 2019, pp. 249–253. doi: 10.1109/CCET48361.2019.8989356.
- [14] A. Banitalebi Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *The Journal of Supercomputing*, vol. 77, no. 3, pp. 2383–2415, Mar. 2021, doi: 10.1007/s11227-020-03323-w.
- [15] Y.-W. Chen, J.-P. Sheu, Y.-C. Kuo, and N. Van Cuong, "Design and implementation of IoT DDoS attacks detection system based on machine learning," in *2020 European Conference on Networks and Communications (EuCNC)*, Jun. 2020, pp. 122–127. doi: 10.1109/EuCNC48522.2020.9200909.
- [16] S. Sen, K. D. Gupta, and M. Manjurul Ahsan, "Leveraging machine learning approach to setup software-defined network(SDN) controller rules during DDoS attack," 2020, pp. 49–60. doi: 10.1007/978-981-13-7564-4_5.
- [17] L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang, and Y. Deng, "A new framework for DDoS attack detection and defense in SDN environment," *IEEE Access*, vol. 8, pp. 161908–161919, 2020, doi: 10.1109/ACCESS.2020.3021435.
- [18] A. Ahmad, E. Harjula, M. Yliantila, and I. Ahmad, "Evaluation of machine learning techniques for security in SDN," in *2020 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2020, pp. 1–6. doi: 10.1109/GCWkshps50303.2020.9367477.
- [19] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DLSN: deep learning for DDOS attack detection in software defined networking," in *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Jan. 2021, pp. 683–688. doi: 10.1109/Confluence51648.2021.9376879.
- [20] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," *Journal of Network and Computer Applications*, vol. 187, p. 103108, Aug. 2021, doi: 10.1016/j.jnca.2021.103108.
- [21] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," *IEEE Access*, vol. 9, pp. 108495–108512, 2021, doi: 10.1109/ACCESS.2021.3101650.
- [22] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, and P. Chinnaamy, "Detection of distributed denial of service attacks in SDN using machine learning techniques," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, Jan. 2021, pp. 1–5. doi: 10.1109/ICCCI50826.2021.9402517.
- [23] O. E. Tayfour and M. N. Marsono, "Collaborative detection and mitigation of DDoS in software-defined networks," *The Journal of Supercomputing*, vol. 77, no. 11, pp. 13166–13190, Nov. 2021, doi: 10.1007/s11227-021-03782-9.
- [24] M. Hossin and M. N. Sulaiman, "A Review on evaluation metrics for data classification evaluations," *International Journal of Data Mining & Knowledge Management Process*, vol. 5, no. 2, pp. 01–11, Mar. 2015, doi: 10.5121/ijdkp.2015.5201.
- [25] S. A. Abbas and M. S. Almhanna, "Distributed denial of service attacks detection system by machine learning based on dimensionality reduction," *Journal of Physics: Conference Series*, vol. 1804, no. 1, p. 012136, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012136.
- [26] S. Kumar *et al.*, "DDoS detection in SDN using machine learning techniques," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 771–789, 2022, doi: 10.32604/cmc.2022.021669.





BIOGRAPHIES OF AUTHORS

Abbas Jasem Altamemi     received the bachelor degree in computer technology engineering from Al-Mustaqbal university college in 2016. He is Master student in Information Networks, University of Babylon 2021-2022. He can be contacted on email: abbas.j.altamemi@gmail.com.



Aladdin Abdulhassan     received his BS and MSc in computer science from University of Babylon in Iraq in 2005 and 2011, respectively. From 2005 to 2011, he worked as a lecturer in the Faculty of Sciences at the Department of Computer Science in the University of Babylon. In September 2014, he enrolled in the Faculty of Engineering at the Department of Computer Engineering and Information Technology, University of Razi, Kermanshah, Iran as a full time PhD student. At January 2019, he received his PhD. At 2019, he started working as a lecturer in the Faculty of Information Technology at the Department of Information Network in the same university, in addition to managing the International Ranking Division at the university and participating in the discussion of many master's theses, as well as the administrative committees. His research interest includes Information security, SDN, packet classification, software-defined networking, and network processing. He can be contacted on email: aladdin.alsharifi@uobabylon.edu.iq.



Nawfal Turki Obeis     received his BS and MSc in computer science from University of Babylon in Iraq in 2005 and 2013, respectively. From 2005 to 2011, he worked as a lecturer in the Faculty of Sciences at the Department of Computer Science in the University of Babylon. In September 2014, he enrolled in the Faculty of Information Technology at the Department of Software, University of Babylon, Babylon, Iraq as a PhD student. At April 2019, he received his PhD. At 2019, he started working as a lecturer in the Faculty of Information Technology at the Department of Information Networks in the same university, in addition to participating in the discussion of many master's theses, as well as the administrative and scientific committees. His research interest includes Information security and networking. He can be contacted on email: nawfal.aljumaili@uobabylon.edu.iq.