

An ensemble-based approach for effective distributed denial of service attack detection in software defined networking

Mohammed Majid Ahmed¹, Hasan Abdulkader²

¹Department of Electrical and Computer Engineering, Altinbas University, Istanbul, Turkey

²Department of Software Engineering, Faculty of Engineering, Haliç University, Istanbul, Turkey

Article Info

Article history:

Received Jul 23, 2023

Revised Nov 2, 2023

Accepted Dec 2, 2023

Keywords:

Distributed denial of service attack

Ensemble learning

Machine learning

Software defined radio

ABSTRACT

Software defined networking (SDN) is a network framework that aims to redefine network characteristics through the programmability of network components, faster and larger network monitoring, centralized network operation, and effective detection of fraudulent traffic and special malfunctions. However, SDN networks are vulnerable to security threats that can cause complete network failure. To address this issue, in this paper, machine learning techniques are suggested for the swift detection of attacks. Various methods for detecting distributed denial of service (DDoS) attacks are evaluated, and the study identifies the most precise method for categorizing such attacks within a SDN network. The results indicate that the proposed system achieves high accuracy in detecting DDoS attacks, with ensemble learning achieving 99% accuracy. This indicates a remarkable improvement percentage in comparison to the approaches of decision tree (DT), k-nearest neighbors (KNN), and support vector machine (SVM).

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Hasan Abdulkader

Department of Software Engineering, Faculty of Engineering, Haliç University

Istanbul, Turkey

Email: hasanabdulkader@halic.edu.tr, hasan.abdulkader@yahoo.com

1. INTRODUCTION

With the rapid increase in internet availability, the need for enhanced security measures has become more crucial compared to the past. Among the significant challenges is the accurate detection of distributed denial of service (DDoS) malicious flows to prevent resource failures caused by discarding these malicious flows [1]. The current mitigation strategies rely on appliances, including firewalls [2], but these approaches utilize predefined security policies that often fall short in detecting and classifying novel attack patterns and responding appropriately [3]. Software defined networking (SDN) has emerged as a promising technique for mitigating DDoS attacks by offering centralized control and programmability.

The effectiveness of SDN-based DDoS detection and mitigation methods largely hinges on the accuracy of their underlying detection models [4]. Ensemble classification, which combines the outputs of multiple classifiers to improve accuracy, has shown potential in various domains, including network intrusion detection [5]. This study proposes an ensemble classification method to enhance the accuracy of DDoS attack detection in SDN.

SDN is a technology that enhances network management by allowing programmable network configuration to optimize performance. SDN is structured into three layers: the application layer, the control layer, and the data plane. The application layer communicates its requirements for network resources to the control layer through application programming interfaces (API), while the control layer communicates with the data plane through south bound API. SDN separates network packets from the routing process, allowing

for centralized intelligence in the control layer [6], [7]. This layer can have one or more controllers and is the brain of the SDN network. Centralized traditional static network architecture, SDN offers greater flexibility and easier troubleshooting, but its centralized architecture presents challenges in security, elasticity, and scalability [8].

DDoS attack detection has been studied merely in research and academic references. There have been numerous proposals to address DDoS attacks in networks, which have been organized into different categories. The proposed methods can be broadly divided into two types: those that rely on machine learning and those that are based on statistics [9], [10].

A DDoS attack involves flooding a network with malicious traffic, overwhelming the resources such as servers and bandwidth, and rendering the network inaccessible. As per the 2020 annual internet report by Cisco, it is projected that the global count of DDoS attacks will increase twofold, reaching 15.4 million by the year 2023 [11]. The report emphasizes the need to focus on preventing DDoS attacks, which have caused denial of service (DoS) in major companies like CNN, Netflix, and Twitter in the past [12]. The main objective of a security operation center (SOC) is to effectively identify and eliminate malicious DDoS flows, ensuring the protection of network resources and maintaining service availability. This research paper specifically concentrates on enhancing the precision of DDoS flow detection, which will be implemented within the centralized SDN controller, whether it is physical or conceptual in nature.

Dong and Sarem [13] created a network structure to initiate a DDoS attack on a host, consisting of one server and ten clients for network connectivity. They employed an enhanced k-nearest neighbors (KNN) algorithm to uncover the DDoS attack. These algorithms yielded a favorable prediction rate of 0.912 each. Indexing and abstracting services depend on the accuracy of the title, extracting from it keywords useful in cross-referencing and computer searching. An improperly titled paper may never reach the audience for which it was intended, so be specific.

Diaz *et al.* [14] devised a structure to identify and mitigate low-rate distributed denial-of-service (LR-DDoS) attacks in SDN. Within this framework, a machine learning-based intrusion detection system (IDS) has been incorporated, which exhibits a remarkable detection rate of 95%. The performance of the architecture was assessed in a simulated environment that closely resembles actual production networks. As a result, the IDS effectively thwarted all detected attacks.

Polat *et al.* [15] presented a model to detect DDoS attacks using machine learning techniques including support vector machine (SVM), KNN, Naïve Bayes, and artificial neural networks (ANN). Two datasets of SDN were utilized, containing instances of normal network conditions and instances of DDoS attacks, in order to capture their distinct characteristics. Additionally, a new dataset was generated by applying a feature selection approach to the existing dataset. The results of the study showed that the KNN classifier achieved an accuracy rate of 98.3%, surpassing the efficiency of previous models.

Rahman *et al.* [16] conducted a study where they utilized various machine learning algorithms, including J48, random forest, SVM, and KNN, to detect and prevent DDoS attacks in SDN network. They incorporated a script to assist in the mitigation and reduction of attacks and evaluated multiple models to identify the most suitable one for the proposed network. The findings demonstrated that J48 exhibited superior performance compared to the other algorithms, particularly in terms of training and testing time.

Nadeem *et al.* [17] conducted a study to compare different machine learning classifiers, such as KNN, Naïve Bayes, random forest, decision trees (DT), and SVM. The classifiers were assessed in terms of their accuracy, precision, recall, and specificity. The findings revealed that the random forest classifier, with feature subset elimination, outperformed the other algorithms in detecting DDoS flood attacks in the context of SDN.

Meti *et al.* [18] conducted a machine learning algorithm comprising Naïve Bayes, neural networks, and SVM. Machine learning models were introduced to detect DDoS flood attacks in SDN. The proposed algorithm achieved accuracies of 70% for Naïve Bayes, 80% for neural networks, and 80% for SVM.

Ahmad *et al.* [19] proposed the use of machine learning techniques for mitigating SDN DoS and DDoS attacks. Their objective was to derive significant insights by evaluating machine learning algorithms for security detection in forthcoming communication networks. Furthermore, they assessed these approaches based on their influence on the controller during DDoS attacks. The research revealed that SVM achieved an impressive accuracy rate of 97.5%.

Tan *et al.* [20] proposed a method for detecting and mitigating SDN DDoS attacks. Their approach involved monitoring the network to identify unexpected flows by utilizing a detection state specifically designed for DDoS on the data layer. They employed machine learning techniques such as k-means and KNN algorithms to detect abnormal flows based on the detection trigger mechanism and rate asymmetry characteristics of the streams. Subsequently, the controller implemented appropriate countermeasures to respond to the attacks. The authors successfully enhanced the accuracy and efficiency of detection while mitigating SDN threats by introducing a novel framework that combines control plane and data plane

cooperative detection techniques. In this paper suggests enhancing the security of DDoS attack detection in SDN controller by utilizing ensemble learning machine learning techniques.

This paper contributes to research on DDoS attacks detection using an innovative approach of ensemble learning. The composition of ensemble learning namely random forest, gradient boosting, and logistic regression has been tested and optimized to deliver high performance proved by computer simulation. Also, the paper made use of a recent dataset [21] published in 2020 issue from a network simulation using Mininet emulating ten topologies made up with switches connected to a unique controller. 23 features collected for the sake of SDN network traffic classification into benign and malicious patterns. In our work we analyze the importance of all features, including alphabetic and structured features after converting them into numeric format. This step reveals that some converted features have significantly much more vital than less important features in the original dataset. Our research continues by selecting the 5 most important features to leverage the problem of DDoS attacks classification.

The paper is structured into five sections: section 1 is the present introduction. Details of the dataset processing, machine learning models, and the research methodology are developed in section 2. Section 3 presents the results and discussion of founding. Finally, section 4 concludes the paper.

2. METHOD

This section will cover the proposed model in four subsections, which are proposed approach, dataset, feature extraction, selection, and machine learning models. The first subsection explains the proposed methodology consisting in using ensemble of machine learning such as a powerful tool to leverage complex problems. Machine learning models simulated in this research are presented in subsections 2.1 and 2.4. Subsections 2.2 and 2.3 develop the dataset attributes and features characteristics.

2.1. Proposed method (ensemble learning)

Protecting against DDoS attacks is of utmost importance in the context of SDN due to its centralized controller architecture. To effectively combat the constantly evolving nature of these attacks, it is essential to employ updated and innovative systems. This is where the evaluation of machine learning methods for DDoS detection becomes crucial. By training the detection system to recognize traffic patterns based on new information, machine learning offers a highly accurate and efficient solution compared to other detection methods. There are three primary categories for DDoS detection: information-theory based detection, machine learning-based detection, and ANN-based detection. In this study, machine learning-based detection was chosen due to its ease of implementation and relatively high precision compared to information-theory based models. The widely used DDoS attack SDN dataset was utilized to train the machine learning models. The trained models were then employed to predict whether the network data was anomalous or benign.

This research paper introduces ensemble learning to enhance the precision of detecting DDoS flows. To differentiate DDoS flows, the study utilizes three classification algorithms: DT, KNN, and SVM. The research proposes an ensemble learning method that combines three algorithms (gradient boosting, random forest, and logistic regression) to improve the accuracy of classification. The outcomes from each classifier are aggregated using a voter mechanism (soft voting). The DDoS attack SDN dataset, designed specifically for SDN, is employed in this project and was generated using the Mininet emulator. The dataset is divided into two sets, with 70% allocated for training and 30% for testing purposes. This concept is visually represented in Figure 1.

The model put forth in this study precisely differentiates between legitimate flows and DDoS flows. The results of the study illustrate this ability of the model. Moreover, the accuracy, precision, recall, and F-score of the model is evaluated in comparison to other models. These statistical metrics will be detailed in section 3. The proposed method in this paper uses an ensemble learning of machine learning consisting of gradient boosting classifier, random forest classifier, and k-neighbors classifier. The ensemble method combines the predictions of these classifiers using soft voting, which considers the predicted probabilities of each classifier rather than just the majority vote. The proposed model is depicted in Figure 2.

2.2. Dataset

The proposed approach made use of the DDoS attack SDN dataset, which had been collected by Bennett University. The dataset had been specifically designed for SDN and was generated using the Mininet emulator. It fulfilled the objective of traffic categorization, utilizing machine learning and deep learning algorithms. The simulation, various types of traffic were generated, including legitimate transmission control protocol (TCP), user datagram protocol (UDP), and internet control message protocol (ICMP) traffic. In addition to malicious TCP Syn attacks, UDP flood attacks, and ICMP attacks were also included. The dataset, as depicted in Table 1, consisted of 23 attributes [21].

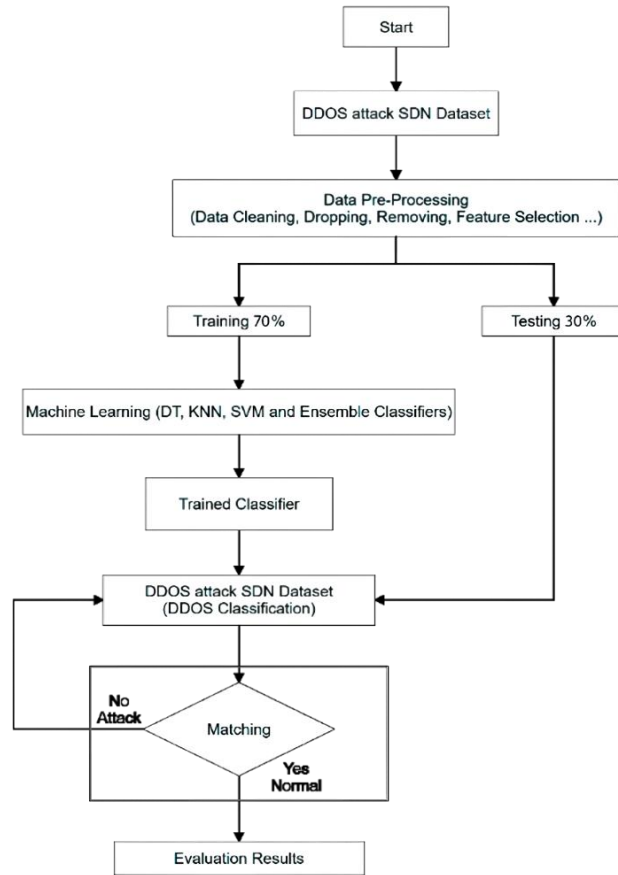


Figure 1. The architecture of the proposed method

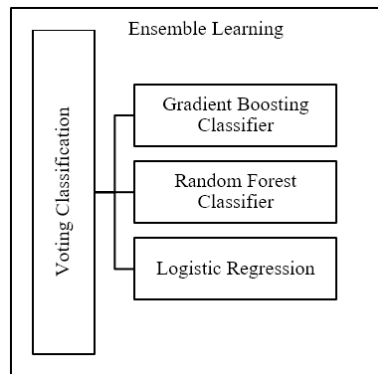


Figure 2. The suggested ensemble learning method for detecting DDoS attacks

Table 1. Main features in the dataset

No.	Features	No.	Features
1.	dt	13.	byteperflow
2.	switch	14.	pktrate
3.	src	15.	Pairflow
4.	dst	16.	Protocol
5.	pktcount	17.	port_no
6.	bytecount	18.	tx_bytes
7.	dur	19.	rx_bytes
8.	dur_nsec	20.	tx_kbps
9.	tot_dur	21.	rx_kbps
10.	flows	22.	tot_kbps
11.	pktperflow	23.	Label
12.	Packet_ins		

2.3. Feature extraction and selection

As mentioned, the dataset used in this study has 23 features that can be used for classification, however, not all of them are equally important. Including a high number of features can increase the complexity of the model, which in turn can lead to overfitting. Overfitting transpires when the model excessively conforms to the training data, resulting in subpar performance when presented with new data. To mitigate this, the analysis focused on the five most critical features, namely 'byteperflow', 'pktperflow', 'bytecount', 'pktrate', and 'pktcount'. These features, along with their corresponding details, are outlined in Table 2 and Figure 3.

Table 2. Features selection

Features	Description
'byteperflow'	The average number of bytes per flow in the dataset.
'pktperflow'	Average number of packets per flow in the dataset.
'bytecount'	Total count of bytes across all flows in the dataset.
'pktrate'	Packet rate, which refers to the number of packets transmitted or received per unit of time.
'pktcount'	Total count of packets across all flows in the dataset.

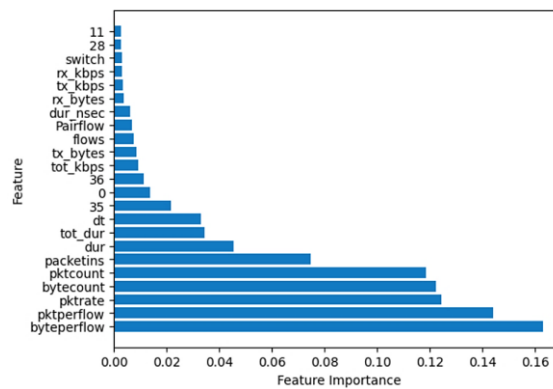


Figure 3. Top features of the dataset

2.4. Other machine learning models

In literature, a huge number of machine learning exists, and they have been applied in a variety of applications. Classification is an important field of study where machine learning excels and show good performance. In this subsection we focus on the classification algorithms DT, KNN, and SVM.

2.4.1. Decision trees

DT are known for their simplicity and remarkable accuracy in classification tasks. The algorithm functions by dividing the data recursively, using selected features, to create subsets that are more easily classified due to their homogeneity. At each internal node, a decision is made based on the value of a feature, dictating the branch to follow. This iterative process persists until a leaf node is reached, ultimately providing the final classification. The appeal and effectiveness of DT lie in their simplicity, interpretability, and capacity to handle diverse data types, all of which contribute to their widespread adoption and ability to achieve high accuracy in classification [22]. The ultimate classification is established by examining various attributes. In the DT algorithm, the Gini index is employed to perform the classification. Gini index is formulated as (1):

$$Gini = 1 - \sum_{i=1}^n (pi)^2 \quad (1)$$

In (1), pi is the probability of an object being classified to a particular class.

2.4.2. K-nearest neighbors

KNN is a supervised machine learning classifier that handles both classification and regression problems. It determines the class or value for new data by considering its KNN. In order to determine the separation between two data points, different distance functions such as Hamming, Manhattan, and Euclidean are utilized. The Euclidean distance function calculates the distance between the incoming data and the data already present in the training set. Based on the KNN, a selection is made from the classified set. The mathematical expression for Minkowski distance can be defined as (2):

$$d(x, y) = (\sum_{r=1}^d |x_r - y_r|^p)^{1/p} \quad (2)$$

where $d(x, y)$ represents the Minkowski distance between two points x and y , x_i and y_i denote the values of the i -th feature (or dimension) of points x and y , respectively and p is a parameter that controls the degree of the Minkowski distance. It is a positive real number.

2.4.3. Support vector machine

The SVM is a binary classifier in machine learning. It aims to create accurate decision boundaries to categorize data. These boundaries, known as hyper-planes, are constructed using unique support vectors. In classification, two classes are separated by a hyper-plane [23]. SVM can achieve high accuracy in classification but has a longer training time compared to other classification algorithms. The implementation of the SVM model involves utilizing a radial basis kernel function. In this approach, the optimal hyperplane is calculated as in (3):

$$k(x_1, x_2) = \exp\left(-\frac{\|x_1 - x_2\|^2}{2\sigma^2}\right) \quad (3)$$

$\|x_1 - x_2\|^2$ represents the squared Euclidean distance between the new data point x and the support vector x_i and γ is a hyperparameter that controls the width of the kernel and affects the smoothness of the decision boundary. It is a positive real number.

3. RESULTS AND EVALUATION

The effectiveness of the machine learning classifier was evaluated using different metrics such as accuracy, precision, recall, and F1 score. These metrics were assessed by constructing a confusion matrix based on actual and estimated probabilities. The composition of the confusion matrix in a binary classification case is given in Table 3. The mathematical formulas for calculating these metrics are as:

- True positive (TP) refers to the accurate identification of attack traffic as an attack.
- False positive (FP) indicates the erroneous detection of normal traffic as an attack.
- True negative (TN) represents the correct identification of normal traffic as normal.
- False negative (FN) denotes the misclassification of normal traffic as an attack.

Table 3. Confusion matrix composition

		Actual class	
		Positive	Negative
Predicted class	Positive	TP	FP
	Negative	FN	TN

A variety of evaluation metrics, such as accuracy, precision, and recall, have been selected to evaluate the effectiveness of machine learning classifiers. These metrics are calculated using a confusion matrix. Assessing the performance of these classifiers is vital for accurately detecting attacks in the SDN controller. The mathematical representation of these metrics is provided as (4) to (7):

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} \quad (4)$$

$$Precision = \frac{TP}{TP+FP} \quad (5)$$

$$Recall = \frac{TP}{TP+FN} \quad (6)$$

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (7)$$

Table 4 presents the simulation outcomes for each classifier. All metrics were evaluated in a computer simulation after adequate training of the machine learning models. These results correspond to a simulation conducted under the specified conditions described in this section. Based on the simulation results, it is evident that the proposed model exhibits a high level of accuracy in detecting DDoS attacks, surpassing 99%. This accuracy rate is exceptionally high, demonstrating the model's effectiveness. Furthermore, the application of ensemble techniques further enhances accuracy, approaching nearly 100%. This improvement in accuracy, pinpointed in Table 5, is particularly noteworthy and highlights the significance of the boosting ensemble approach in enhancing the model's performance.

Table 4. The results each classifier

Algorithm	Precision (%)		Recall (%)		F1 score (%)		Accuracy (%)	
	0	1	0	1	0	1	Training set	Test set
DT	98	94	96	97	97	96	96.5	96.5
KNN	97	94	96	96	97	95	96	95.8
SVM	93	97	98	91	95	94	92.4	92.3
Logistic regression	72	67	83	52	77	58	71	70
Gradient boosting	98	92	95	97	96	95	95.4	95.5
Random forest	1.00	88	91	99	95	93	94.2	94.2
Ensemble learning	1.00	1.00	1.00	1.00	1.00	1.00	99.9	99.8

Table 5. The results of the proposed method compared to state of art

Reference	Year	Dataset	Method name	Accuracy (%)
[24]	2021	NSL-KDD dataset	SVM-based IDS mechanism	95.98
[25]	2021	Real-Time dataset using Floodlight controller and Mininet	SVM	94.99
			DT	86.74
			Logistic regression	73
			Random forest	86
[26]	2023	KDD99 dataset	Improved SVM algorithm	98.8
[27]	2022	KDD cup99	Logistic regression	97.80
			KNN	97.80
			DT	99
[28]	2023	Dataset from Kaggle	Naïve Bayes	70
			SVM	80
			Naïve Bayes	96
Our proposed (ensemble learning)		DDoS attack SDN dataset [21]	Ensemble learning	99.8

4. CONCLUSION

The impact of DDoS attacks on networks is a significant concern, as they have the potential to cause complete disruption if not effectively addressed. These attacks are growing in complexity and can easily evade traditional protection techniques. To tackle network security challenges, machine learning techniques are being implemented in SDN. The DT, KNN, and SVM algorithms are employed to construct implicit or explicit models from available data. These models enable systems to learn from the data without explicit programming, uncover hidden patterns, and gain valuable insights. By leveraging machine learning, it is possible to enhance the effectiveness of network features, thereby contributing to the intelligent mitigation of DDoS attacks. Among the employed machine learning algorithms, ensemble learning achieved the best results with an accuracy of 99%, outperforming the other algorithms. In the future, there will be an emphasis on creating a mitigation module specifically designed for the studied attacks in this research. Developing an efficient and cost-effective mitigation plan entails tackling various obstacles. One such challenge involves guaranteeing the termination of all dubious communications by leveraging SDN's programmability capability, which can be achieved through the implementation of blocking rules in edge switches. Moreover, optimizing the utilization of controllers and switching resources to implement mitigation policies, reducing the response time of the mitigation system, and ensuring scalability of the solution are all important factors to consider in the process.

REFERENCES

- [1] A. A. Alashhab, M. S. M. Zahid, M. A. Azim, M. Y. Doha, B. Isyaku, and S. Ali, "A survey of low rate DDoS detection techniques based on machine learning in software-defined networks," *Symmetry*, vol. 14, no. 8, pp. 1-30, 2022, doi: 10.3390/sym14081563.
- [2] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, and P. Chinnasamy, "Detection of distributed denial of service attacks in SDN using machine learning techniques," in *2021 International Conference on Computer Communication and Informatics, ICCCI 2021*, IEEE, 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402517.
- [3] A. Shirmarz, A. Ghaffari, R. Mohammadi, and S. Akleylek, "DDoS attack detection accuracy improvement in software defined network (SDN) using ensemble classification," in *14th International Conference on Information Security and Cryptology, ISCTURKEY 2021*, IEEE, 2021, pp. 111-115, doi: 10.1109/ISCTURKEY53027.2021.9654403.
- [4] J. Wang and L. Wang, "SDN-defend: a lightweight online attack detection and mitigation system for DDoS attacks in SDN," *Sensors*, vol. 22, no. 21, pp. 1-21, 2022, doi: 10.3390/s22218287.
- [5] A. A. Aburomman and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers," *Computers and Security*, vol. 65, pp. 135-152, 2017, doi: 10.1016/j.cose.2016.11.004.
- [6] A. Shirmarz and A. Ghaffari, "Automatic software defined network (SDN) performance management using TOPSIS decision-making algorithm," *Journal of Grid Computing*, vol. 19, no. 2, pp. 1-21, 2021, doi: 10.1007/s10723-021-09557-z.
- [7] A. Shirmarz and A. Ghaffari, "An adaptive greedy flow routing algorithm for performance improvement in software-defined network," *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, vol. 33, no. 1, 2020, doi: 10.1002/jnm.2676.
- [8] S. Saraswat, V. Agarwal, H. P. Gupta, R. Mishra, A. Gupta, and T. Dutta, "Challenges and solutions in software defined networking: a survey," *Journal of Network and Computer Applications*, vol. 141, pp. 23-58, Sep. 2019, doi: 10.1016/j.jnca.2019.04.020.
- [9] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCSST)*, IEEE, 2019, pp. 1-8, doi: 10.1109/CCST.2019.8888419.




- [10] M. Al-Farttoosi and H. Abdulkader, "Botnet mobile detection using machine & deep learning techniques," in *2022 Iraqi International Conference on Communication and Information Technologies, IICCIT 2022*, IEEE, Sep. 2022, pp. 82–87, doi: 10.1109/IICCIT55816.2022.10010653.
- [11] Cisco, "Cisco annual internet report (2018-2023)," *White Paper Cisco Public*, pp. 1–35, 2020.
- [12] Deloitte, "Defending against distributed denial of service (DDoS) attacks," *Deloitte Canada*. [Online]. Available: <https://www2.deloitte.com/ca/en/pages/risk/articles/DDoSattacks.html> (accessed Sep. 24, 2023).
- [13] S. Dong and M. Sarem, "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.
- [14] J. A. P. -Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.
- [15] H. Polat, O. Polat, and A. Cetin, "Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models," *Sustainability*, vol. 12, no. 3, pp. 1-16, 2020, doi: 10.3390/su12031035.
- [16] 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 2019*, IEEE, 2019, pp. 184–189, doi: 10.1109/SERVICES.2019.00051.
- [17] M. W. Nadeem, H. G. Goh, V. Ponnusamy, and Y. Aun, "Ddos detection in sdn using machine learning techniques," *Computers, Materials and Continua*, vol. 71, no. 1, pp. 771–789, 2022, doi: 10.32604/cmc.2022.021669.
- [18] N. Meti, D. G. Narayan, and V. P. Baligar, "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks," in *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*, IEEE, Sep. 2017, pp. 1366–1371, doi: 10.1109/ICACCI.2017.8126031.
- [19] A. Ahmad, E. Harjula, M. Ylianttila, and I. Ahmad, "Evaluation of machine learning techniques for security in SDN," in *2020 IEEE Globecom Workshops*, IEEE, 2020, pp. 1-6, doi: 10.1109/GCWkshps50303.2020.9367477.
- [20] 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.
- [21] N. Ahuja, G. Singal, and D. Mukhopadhyay, "DDoS attack SDN dataset", *Mendeley Data*, V1, 2020, doi: 10.17632/jxpfjc64kr.1.
- [22] N. Ashodia and K. Makadiya, "Detection of DDoS attacks in SDN using machine learning," in *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, IEEE, 2022, pp. 1322–1327, doi: 10.1109/ICEARS53579.2022.9751879.
- [23] M. H. H. Khairi *et al.*, "Detection and classification of conflict flows in SDN using machine learning algorithms," *IEEE Access*, vol. 9, pp. 76024–76037, 2021, doi: 10.1109/ACCESS.2021.3081629.
- [24] P. Hadem, D. K. Saikia, and S. Moulik, "An SDN-based intrusion detection system using SVM with selective logging for IP traceback," *Computer Networks*, vol. 191, pp. 1-11, 2021, doi: 10.1016/j.comnet.2021.108015.
- [25] F. Khashab, J. Moubarak, A. Feghali, and C. Bassil, "DDoS attack detection and mitigation in SDN using machine learning," in *Proceedings of the 2021 IEEE Conference on Network Softwarization: Accelerating Network Softwarization in the Cognitive Age, NetSoft 2021*, IEEE, 2021, pp. 395–401, doi: 10.1109/NetSoft51509.2021.9492558.
- [26] M. Huang and B. Zhao, "A DDoS attack detection algorithm based on improved grid search to optimize SVM in SDN environment," in *2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms, EEBDA 2023*, IEEE, 2023, pp. 218–222, doi: 10.1109/EEBDA56825.2023.10090555.
- [27] M. Kavitha, M. Suganthy, A. Biswas, R. Srinivsan, R. Kavitha, and A. Rathesh, "Machine learning techniques for detecting DDoS attacks in SDN," in *International Conference on Automation, Computing and Renewable Systems, ICACRS 2022 - Proceedings*, IEEE, 2022, pp. 634–638, doi: 10.1109/ICACRS55517.2022.10029110.
- [28] A. K. Kurakula, K. Akhila, M. Bhavya, and M. V. Sai, "Detecting distributed DoS attacks on SDN using machine learning (ML) methods," in *International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings*, IEEE, 2023, pp. 767–772, doi: 10.1109/ICIDCA56705.2023.10099680.

BIOGRAPHIES OF AUTHORS



Mohammed Majid Ahmed    received the bachelor's degree in Computer Engineering from Al-Hussain University College in 2016. He is Master student in Electrical and Computer Engineering, Altinbas University 2021-2023. He can be contacted at email: 203720250@ogr.altinbas.edu.tr.



Dr. Hasan Abdulkader    received a Ph.D. in Computer Science and Telecommunications from the Institute National Polytechnique in Toulouse-France INPT. He worked in several universities in France and abroad and he is now working with the Halic University as an associate professor. He can be contacted at email: hasan.abdulkader@yahoo.com.