Comparative Analysis of DDos Attacks Detection Systems in Software Defined Networks

Anuja Sharma, Parul Saxena

Soban Singh Jeena University, Almora, Uttarakhand

Corresponding author: Anuja Sharma, Email: anu.sharma70@gmail.com

The software-Defined Network (SDN) is the pre-eminent network framework in the recent decades as it ensures more authority over the recent network architecture. The Controller, which is characterized as the system software of the SDN is liable for running different organization applications and conserving a few organization administrations and functionalities. In spite of all its potentials, the establishment of numerous constructive organization of SDN creates numerous security dangers and possible targets. The Distributed Denial of Services (DDoS) is one of the major security threats that deteriorate the performance of the SDN organization. More researchers are concentrated to restrain the DDoS attack as the control layer in the SDN is the most exposed to DDoS attacks.These days, in the field of SDN, different AI (ML) procedures are being conveyed to recognize DDoS attack. Hence in this paper, 15 papers related to the DDoS attacks detection are analyzed. The evaluation of the research is implemented with respect to the various factors such as performance metrics, achievement of the existing methods, classifier or the methods utilized and so on. Finally, this report elucidates the future direction of the research.

Keywords: SDN, Security, DDoS attacks, Machine learning techniques, SVM.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 283–296. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-29

1 Introduction

In the current scenario Software defined Network (SDN) now become a progressive organization standard. The SDN can fulfill the developing needs of future organizations, and it is progressively utilized in server hubs and administrator networks [6]. As of late the programming characterized network known as SDN standard has acquired huge interest from numerous analysts. The SDN standard offers a more noteworthy potential to give a reliable, adaptable, and secure organization framework [11]–[12]. Partition of the control plane from the hidden foundation layer is the principle development behind SDN. The centralized controller deals with the packet transmission gadgets that should be arranged through an all around planned interface like OpenFlow [13]. In SDN, the organization gadgets like switches have just sending rationale, while the control rationale and dynamic capacity are programmed at the regulator. This permits the regulator to direct the switches with new organization arrangements, and basic gadgets begin to follow the approaches keep up in the flow table. Right when a packet appears at a switch, it checks its stream table, and on the off chance that the stream matches, it progresses the bundles to its objective. If no match lays out in the stream table, OpenFlow engaged switch sends control bundle to the controller for making a fitting decision. The regulator can deal with different stream tables kept up by OpenFlow switch in order to accomplish programmability in the control layer of SDN [1]. SDN itself is confronted with various security challenges, among which the appropriated distributed denial of service (DDoS) attacks is a significant danger which is one of the denial of service (DoS) attack [4].The DoS attack comes from single location, it is easy to detect the server connection and the origin. Whereas, the DDos attack is the extension of the DoS attack, which generates from multiple location and use multiple hosts as attack. Hence, it is difficult to find its origin [25].

Distributed Denial of Service (DDoS) attacks are right now the most predominant and complex threat for associations, and are progressively hard to intercept [14]. For an instance GitHub was hit with one of the biggest DDoS attacks ever in 2018 [15][5][10]. This significant attacks comes in perhaps the most featured cyber attacks of the current digital age, shaking the ground premise of one of the support tool (accessibility) of the CIA reliability triplet. Aggressors use a huge number of botnets, machines and dump terminals to simultaneously dispatch DDoS attacks that in this manner exhaust the objective framework primary assets, making the whole administrations inaccessible. There are a possibly outrageous number of real and amazing assets accessible, which can be mishandled to dispatch DDoS attacks on enormous and little scopes appropriately [3]. The development of DDoS attacks can prompt irregularities in the connected organization administrations, causing tremendous monetary misfortunes and in any event, causing other cataclysmic results. DDoS attacks are one of the genuine organization security dangers confronting the Internet. It's anything but a key examination point in the security field to recognize DDoS attacks precisely and rapidly. In the conventional organization design, the principle techniques for DDoS attacks recognition innovation can be separated into attacks location dependent on traffic qualities and attacks identification dependent on traffic inconsistency [2] [6] [7].

The organization of the manuscript follows: the review of the literature is enumerated in section 2. The comparative methodology detailed in section 3. The result and discussion is deliberated in section 5. Finally, the conclusion of the paper is depicted in section 6.

2 Review of Existing Methods

This section elucidates the review of various methods utilized in the detection of the DDoS attacks in SDN. The DDoS attack detection methods are classified based on three major categories such as machine learning methods, collaborative machine learning methods and deep learning methods.

A new strategy for the detection and alleviation of DDoS attacks in SDN is presented by Kshira Sagar Sahoo *et al.* [1]. The multi-dimensional SVM is utilized for the recognition of DDoS attacks. The kernel principal component analysis (KPCA) in accompany with GA is utilized in the model to reduce the evaluation time and to attain enhanced accuracy. The most significant features from the DDoS dataset are extricated with the aid of KPCA. The best suited confusion matrix is of the test data is selected through

GA. The parameters of the SVM classifier is optimized with the aid of NKPCA+GA+SVM. The training period is further reduced through N-RBF. The experimental evaluation shows that KPCA exceed the traditional PCA methods. The accuracy of the NKPCA+GA+SVM model is found to be greater than 90%, which elucidates that the method effectively recognizes the DDoS attack in SDN. Furthermore the performance of the SVM classifier is improved through implementing kernel activity of PCA.

S. Perumal Sankar *et al.* [2] gathers the stream status data of the organization traffic to recognize the DDoS attacks in the SDN. S. Perumal Sankar *et al* extricate six-tuple attribute value associated to the DDoS attack and further utilize the SVM algorithm to determine the traffic in the organization to execute the DDoS attacks detection. In the article the author concentrated on the evaluation of the variation in the attribute value of the network traffic to determine the feasibility of the SVM classifier in the SDN framework. The enhanced recognition accuracy and the diminished false alarm rate is the main advantage of the review SVM classifier based DDoS detection method. In correlation, the test recognition precision pace of ICMP attacks stream is somewhat low. By evaluating the ICMP traffic, the researchers arrived at the resolution that the ICMP stream does not possess both the source location and objective location. Hence, RPF and SSP are nullified, which makes the six-tuple trademark esteems grid change into four tuple attribute framework, if attacked. In any case, this has little impact on the test results, and the analysis has accomplished the objective.

Shahzeb Haider *et al.* [3] Presented the prominent and versatile Deep CNN ensemble structure to resolve the complication of the most pervasive and complicated DDoS attacks recognition in SDNs. The Deep CNN ensemble structure is evaluated with standard deep learning ensemble and cross bread algorithm on a stream depends on SDN dataset. The Deep CNN ensemble frame work exhibits enhancements both in recognition precision and computational intricacy. Finally, the researcher embrace shifted deep learning ensemble based recognition and counteraction components for the arising huge scope dispersed organizations.

Jie Cui *et al.* [4] presented the DDoS recognition and shielding mechanism with the aid of cognitive–inspired processing in SDN. At this cognitive method, the information about the switch stream table were utilized to ascertain the variation measure of information bundles of the source and objective locations in every interval, the entropy standard of source along with objective locations are acquired by the formulation of entropy esteem computation. Source along with objective location entropy attributes are represented as attribute vectors. Further SVM algorithm is utilized to train the dataset so as to obtain explicit DDoS attacks recognition modes. Finally, a basic and compelling strategy is used to reestablish the correspondence capacity of the user host framework acquired by training, acknowledging DDoS attacks detection and shield over a solitary host. Evaluations were led on the standard dataset known as DDoS Attack 2007, and the outcome was contrasted with Scheme 1. The exploratory outcomes exhibit that the plan has minimize false rate while maintaining enhanced recognition rate and perceives the entire function of the recognition shield and retrieval. In a future report, the research is extended to multi-machine identification and planning a more productive retrieval algorithm are designed.

Liang Tan *et al.*[6] dissect the identification and safeguard system of DDoS attacks over SDN, which consolidates SDN's own benefits and AI algorithm, and embraces a more designated strategy to recognize and guard against DDoS attacks in the SDN controller. Experiments are developed to demonstrate that the discovery strategies presented in this article will accomplish the preferable outcomes. Besides, the recognition trigger instrument can successfully recognize the event of strange streams and save assets of the controller. The obtained safeguard technique can adequately moderate DDoS attacks. Yet, the burden of the regulator enhances with the deterioration in the effectiveness of DDoS identification when the organization is under bigger scope network traffic. Consequently, the researchers will attempt to utilize the innovation of streaming figuring to diminish the weight of a solitary controller to guarantee the productivity of DDoS identification and organization quality under enormous scope network traffic

Table 1: Review of literature papers

S.No	Author	Methods	Dataset used	Performance metrics	Pros	Cons
1	Kshira Sagar Sahoo *et al.*[1]	SVM- KPCA	NSL-KDD	Accuracy and execution time	SVM-KPCA indicates better performance as it reduces the quantity of principal components.	Even though SVM-KPCA effectively recognize attacks traffic in a solitary controller, it might fails to distinguish the attacks congestion in a multi-controller environment
2	Jin Ye *et al.*[2]	support vector machine algorithm	DDoS attack database	Packet size, accuracy, False alarm rate	Enhanced detection accuracy rate	Extremely small false alarm rate is the main drawback
3	Shahzeb Haider *et al.*[3]	Deep –CNN ensemble	CICIDS2017, NSL-KDD dataset	Accuracy, precision,, recall and F1-score	Attain advancements in detection accuracy	The high level FPR is less preferable in the basic setting of distinguishing interruptions on an organization.

4	Jie Cui *et al.*[4]	cognitive inspired computing	DDoS attack 2007 dataset	Accuracy, true positive rate and false positive rate	Cognitive inspired processing recognizes attacks rapidly with enhanced recognition rate and low FPR	It is not suitable for multi-machine detection.
5	Liang Tan *et al.*[6]	K-Means and KNN	KDD99 dataset	Accuracy	The recognition trigger component can adequately identify the event of strange streams and save assets of the controller	The burden of the SDN controller will increase and the effectiveness will decrease with the enhanced network congestion.
6	Shanshan Yu *et al.*[7]	A collaborative DDoS attacks recognition model based on ensemble learning and entropy	NSL-KDD dataset	Precision, Recall, False alarm rate	Recognize the DDoS attack prominentl y and rapidly	The computation al complexity of the ensample learning is the main drawback
7	Shi Dong *et al.*[8]	KNN algorithm	Flow-based dataset	CPU utilization,	KNN+ ML have achieved	KNN + ML is not suitable for

		depend on ML		Execution time	higher detection rates	real SDN environment
8	Afsaneh Banit alebi Dehkordi *et al.* [9]	ML and statistical methods	DDoS attack dataset	Detection accuracy	Increased accuracy in detecting DDOS	DDoS attackss are recognized only by solitary SDN controller
9	Fahad Ghalib Abdulkadhim *et al.* [18]	(SDN) and selforganizing map (SOM)	Evolved Node Base Controller (eNBC) and Roadside Controller (RSC)	Accuracy, specificity and sensitivity	This model offers better management, scalability and flexibility	This method fails to provide desired data due to limited features and missing data.
10	Nisha Ahuja *et al* [19]	Support Vector classifier with Random Forest (SVC-RF)	SDN traffic dataset	Average delay, packet delivery ratio and network throughput	This model is utilized in real-time for the classification of traffic based on the learned features	This model is still slow to provide the detection output
11	Jalal Bhayo *et al.*[20]	SDN-based secure IoT model	DDoS attack dataset	Accuracy, Cross Entropy loss and bandwidth	The average time of analyzing logs of 22 MB was 16 sec, and the detection time was 2.5 secs.	It is not developed to address large number of DDoS attack

12	Özgür Tonkal *et al.* [21]	Machine learning algorithms equipped with Neighbourhood Component Analysis (NCA)	DDoS attack SDN Dataset	Accuracy, detection rate and false positive rate	Provides high accuracy rate .	Requires further updation with feature selection algorithm.
13	Thapanarath Khempetchand Pongpisit Wuttidittachotti [22]	Deep Neural network	CICDDoS2019	Accuracy, sensitivity, specificity, precision and F-sore	This model detect more than 99.90% of all three types of DDoS attacks.	This model is expensive to train due to complex data models
14	Pajila *et al.* [23]	Fuzzy based DDoS attack Detection and Recovery mechanism (FBDR)	Real time dataset	Accuracy	Saves energy usage by up to 20 % compared with the related scheme	The inaccurate data will negatively influence the detection accuracy
15	Wang, J.*et al.* [24]	convolutional neural networks	Real time datset	Accuracy	This method has low processing overhead and high detection accuracy	This model requires large data to train and process neural network

Open issues and challenge:

- Machine learning depended DDoS detection model require high dimensional data due to the constant change in network topology [1].
- The selection of the most significant features is the main issues experienced in the traditional models , as it increase the detection accuracy of the model [1]
- The increase in number of false positive rate is the main issue experienced in the existing accuracy detection model [2].
- The computational overhead of the SDN controller is one of the issue that curbs the performance of the detection accuracy [7].
- The Neural Network based algorithm are inefficient and complex as it need to distinguish the protocols [8].

3 Comparative Methodology

The conventional methods such as [1], [3], [4] and [8] are utilized for the comparative analysis for which the metrics, such as accuracy, sensitivity and specificity. The brief description of key parameters such as accuracy, sensitivity and specificity as calculated in this paper is as follows:

3.1 Accuracy:

Accuracy is defined as the proximity of the estimation to a specific value and the mathematical representation of the accuracy

$$\alpha = \frac{(\mathrm{T}p + \mathrm{T}n)}{(\mathrm{T}p + \mathrm{T}n + \Gamma p + \Gamma n)} \tag{1}$$

where, α denotes the accuracy, $\mathrm{T}p$ is the true positive value, $\mathrm{T}n$ is the true negative value, Γp and Γn are false positive and false negative value respectively.

3.2 Sensitivity:

The sensitivity is defined as the proportion of number of correctly recognized true positive values to the sum of false negative and true positive value and it is mathematically expressed as

$$\beta = \frac{\mathrm{T}p}{\Gamma n + \mathrm{T}p} \tag{2}$$

where, β represents the sensitivity.

3.3 Specificity:

The specificity is characterized as the extent of number of accurately perceived true negative values to the amount of bogus positive and true negative value and it is mathematically expressed as

$$\lambda = \frac{\mathrm{T}n}{\mathrm{T}n + \Gamma p} \tag{3}$$

where, λ represents the specificity

4 Results and Discussion

This section elucidates the analysis of detection and optimization of DDoS attacks in software defined networks. The detection and optimization of DDoS attacks in software defined networks are implemented and the results are briefly explained in this section. The competition task was to create a network intrusion detector, a predictive model capable of distinguishing between ``bad'' connections, called intrusions or attacks, and ``good'' normal connections. This database contains a typical set of knowledge to be audited, which incorporates a good sort of intrusions simulated during a military network environment.

4.1 Performance Analysis of existing methods in terms of dataset:

The Table 2 illustrates the performance achieved by the conventional methods.

Table 2 : Performance evolution

S. No	Methods	Dataset used	Parameter	Achievement
1	SVM +KPCA[1]	NSL-KDD dataset	Accuracy	90.907%
2	Deep-CNN ensemble model [3]	Network-based intrusion detection system (NIDS)	Accuracy	90.45%
			Precision	99.57%
			Recall	99.64%
			F1	99.61%
3	Cognitive-inspired computing [4]	DDoS attack 2007 dataset	Precision	97.65%
4	ML based algorithm on K-Means +KNN [6]	NSL-KDD dataset	Recall	98.85%
			F1	98.47%

			False positive	0.97%
5	ML and statistical methods	ISCXSlowDDos-2016 database	Accuracy	83.39%
			TPR	88.60%
			FPR	16.88%
			Precision	22.00%
			F-measure	35.25%
		ISCX-IDS-2012 dataset	Accuracy	89.84%
			PR	59.87%
			FPR	7.84%
			Precision	37.08%
			F-measure	45.80%
		CTU-10 dataset	Accuracy	83.31%
			TPR	88.59%
			FPR	17.27%
			Precision	36.46%
			F-measure	51.66%
		CTU-11 dataset	Accuracy	71.87%
			TPR	100%
			FPR	32.72%
			Precision	33.33%
			F-measure	50.00%

4.2 Performance analysis of existing methods in terms of Classifier:

This section elucidates the performance of the conventional DDoS detection method with respect to the classifier. Table 3 elucidates the performance evaluation of the existing method with respect to the classifier.

Table 3 : Performance analysis of existing methods in terms of Classifier

S. no	Methods	Classifier	Parameter	Achievement
1	SVM assisted KPCA [1]	SVM	Detection accuracy	98.355%
			Time	1120sec
2	SVM algorithm [2]	SVM classifier	Average Detection accuracy rate	90.24%

			Average False alarm rate	0.9%
3	Deep-CNN + ensemble framework [3]	Ensemble CNN classifier	Accuracy	90.45%
			Precision	90.57%
			Recall	90.64%
			F1	90.61%
			Test time	0.061%
			Train time	39.52%
			CPU usage	6.02%
4	Cognitive-inspired computing [4]	SVM classifier	Detection rate	75%
5	Collaborative ML algorithm based on KNN and K-Means [6]	KNN	Accuracy	90.85%
			Recall	98.74%
			Precision	0.97%
6	KNN based on ML [7]	KNN	TPR	0.982
			FPR	0.024
			Precision	0.981
			Recall	0.982
			F-measure	0.9815
7	The DDoS attacks recognition through ML and statistical methods [9]	BayesNet	TRP	96.23%
			FPR	0.58%
			ACC	90.33%
			Precision	83.48%
			F-measure	89.40%
		J48	TRP	98.59%
			FPR	0.09%
			ACC	90.87%
			Precision	97.53%
			F-measure	98.06%
		Logistic regression	TRP	90.87%
			FPR	0.39%

			ACC	90.62%
			Precision	88.82%
			F-measure	94.02%
		Random tree	TRP	98.01%
			FPR	0.05%
			ACC	90.88%
			Precision	98.53%
			F-measure	98.27%
		REPTree	TRP	97.99%
			FPR	0.04%
			ACC	90.88%
			Precision	98.60%
			F-measure	98.29%

4.3 Comparative Discussion:

The customary strategies, for example, [1], [3], [4] and [8] are used for the similar investigation for which the measurements, like precision, awareness and particularity. Precision is characterized as the nearness of the assessment to a particular worth. The responsiveness is characterized as the extent of number of accurately perceived genuine positive qualities to the amount of misleading negative and genuine positive worth. The particularity is characterized as the extent of number of accurately perceived genuine negative qualities to the amount of bogus positive and genuine negative worth.

The comparative analysis of the comparative methods in terms of accuracy is demonstrated in the Figure 1 a). From the figure, it is illustrated that the accuracy attained by the comparative methods such as SVM, Deep-CNN, Cognitive-inspired computing and improved KNN are 80.6460%, 89.8375%, 84.2461% and 88.6660%, respectively which is found to be lower than the proposed DDoS detection method. Hence, it is proved that the DDoS method based on Deep CNN exceeds all the other conventional methods in terms of accuracy. The comparative analysis of the comparative methods in terms of sensitivity is demonstrated in the Figure 1 b). At the K-fold value of 10, the accuracy attained by the comparative methods such as SVM, Deep-CNN, Cognitive-inspired computing and improved attains the sensitivity of 81.5896%, 86.4537%, 85.1897% and 89.6096% respectively, in which the Deep learning method obtains the preferable output. However, none of the comparative model attains accuracy more than 90%. Hence, there needs deep exploration in the field of deep learning technique to obtain most accurate DDoS detection model.

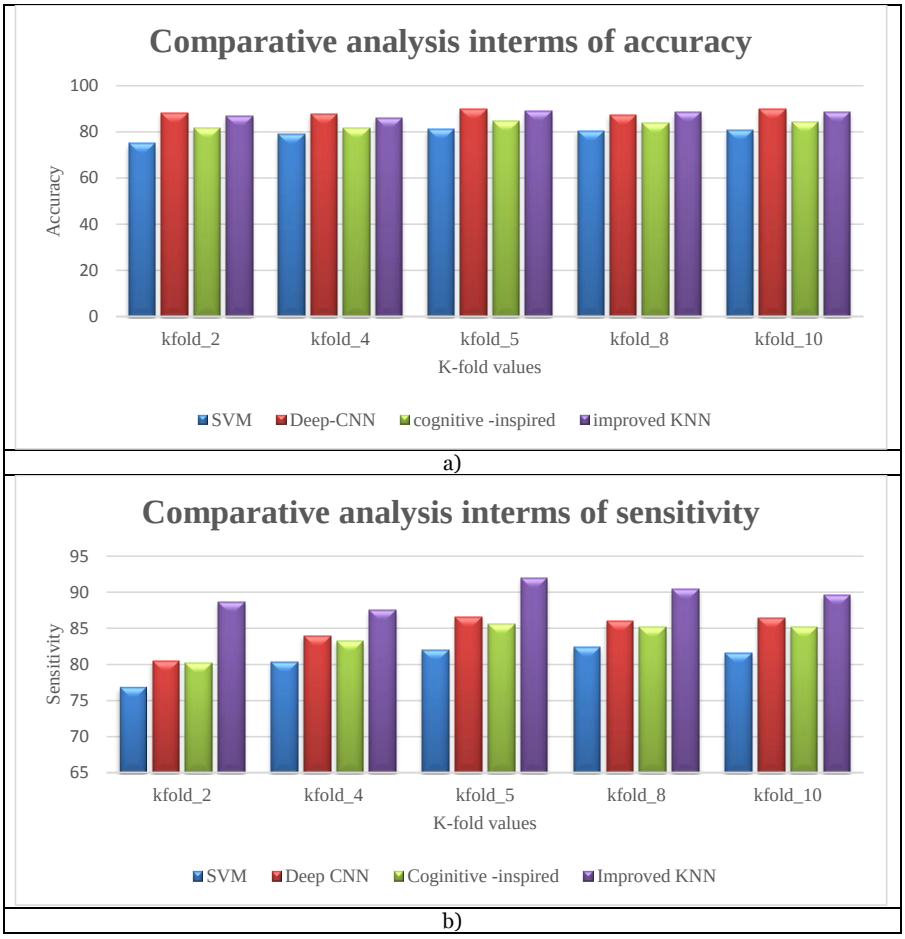

Figure 1. Comparative analysis, a) in terms of Accuracy, and b) in terms of Sensitivity

5 Conclusion

The SDN is the pre-eminent network structure which is applied in almost all domains due to its simplicity. Even though the SDN provides numerous benefits, it likewise faces the danger of DDoS attacks, the most widely recognized security danger in the organization. As a benefit of SDN, unified control additionally makes the regulator in SDN more powerless against security dangers from DDoS attacks. The modern innovative strategies and development in the deep-learning techniques are the significant measures to create a safe and reliable data transmission in SDN networks that detects the DDoS attacks. In this review paper, 8 papers related to the DDoS attack detection are analyzed. The evaluation of the research is implemented with respect to the various factors such as performance metrics, achievement of the existing methods, classifier or the methods utilized and so on. Furthermore, the analysis of DDoS attack detection methods in terms of their merits and demerits are presented in this research article. Finally this review paper elucidates the future direction of research.

References

[1] Kshira Sagar Sahoo, K.S., Tripathy, B.K., Naik, K., Ramasubbareddy, S., Balusamy, B., Khari, M. and Burgos, D., (2020) "An evolutionary SVM model for DDOS attack detection in software defined networks", IEEE Access, vol.8, pp.132502-132513

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

[3] Haider, S., Akhunzada, A., Mustafa, I., Patel, T.B., Fernandez, A., Choo, K.K.R. and Iqbal, J., (2020)"A deep cnn ensemble framework for efficient ddos attack detection in software defined networks", Ieee Access, vol.8, pp.53972-53983.

[4] Cui, J., Wang, M., Luo, Y. and Zhong, H., (2019)"DDoS detection and defense mechanism based on cognitive-inspired computing in SDN", Future generation computer systems, vol.97, pp.275-283.

[5] Yang, L. and Zhao, H., (2018)"DDoS attack identification and defense using SDN based on machine learning method", In proceedings of 15th IEEE International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN), pp. 174-178.

[6] Liang Tan., Pan, Y., Wu, J., Zhou, J., Jiang, H. and Deng, Y.,(2020) "A New Framework for DDoS Attack Detection and Defense in SDN Environment", IEEE Access, vol.8, pp.161908-161919.

[7] Shanshan Yu , Zhang, J., Liu, J., Zhang, X., Li, Y. and Xu, T.,(2021) "A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN", EURASIP Journal on Wireless Communications and Networking, vol.2021, no.1, pp.1-21.

[8] Shi Dong, S. and Sarem, M.,(2019) "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.

[9] Afsaneh Banitalebi Dehkordi, Soltanaghaei, M. and Boroujeni, F.Z.,(2021) "The DDoS attacks detection through machine learning and statistical methods in SDN", The Journal of Supercomputing, vol.77, no.3, pp.2383-2415.

[10] Myint Oo, M., Kamolphiwong, S., Kamolphiwong, T. and Vasupongayya, S.,(2019) "Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN)", Journal of Computer Networks and Communications.

[11] Zhang, Y., Cui, L., Wang, W. and Zhang, Y.,(2018) "A survey on software defined networking with multiple controllers", Journal of Network and Computer Applications, vol.103, pp.101-118.

[12] Visu, P., Lakshmanan, L., Murugananthan, V. and Cruz, M.V.,(2019) "Software-defined forensic framework for malware disaster management in internet of thing devices for extreme surveillance", Computer Communications, vol.147, pp.14-20.

[13] Mondal, A., Misra, S. and Maity, I.,(2019) "AMOPE: Performance analysis of OpenFlow systems in software-defined networks", IEEE Systems Journal, vol.14, no.1, pp.124-131.

[14] Sahoo, K.S., Panda, S.K., Sahoo, S., Sahoo, B. and Dash, R.,(2019) "Toward secure software-defined networks against distributed denial of service attack", The Journal of Supercomputing, vol.75, no.8, pp.4829-4874.

[15] Kottler, S.,(2018) "February 28th DDoS incident report", GitHub Engineering.

[16] Rajabioun, R.,(2011) "Cuckoo optimization algorithm", Applied soft computing, vol.11, no.8, pp.5508-5518.

[17] Jiankai Xue and d Bo Shen,(2020) " A novel swarm intelligence optimization approach: sparrow search algorithm', SYSTEMS SCIENCE & CONTROL ENGINEERING: AN OPEN ACCESS JOURNAL, vol. 8, no. 1, pp.22–34.

[18] Abdulkadhim, F.G., Yi, Z., Tang, C., Onaizah, A.N. and Ahmed, B.,(2021) "Design and development of a hybrid (SDN+ SOM) approach for enhancing security in VANET", Applied Nanoscience, pp.1-12.

[19] Ahuja, N., Singal, G., Mukhopadhyay, D. and Kumar, N.,(2021)"Automated DDOS attack detection in software defined networking", Journal of Network and Computer Applications, vol.187, p.103108.

[20] Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S. and Shah, S.A., (2021)"A time-efficient approach toward DDoS attack detection in IoT network using SDN", IEEE Internet of Things Journal, vol.9, no.5, pp.3612-3630.

[21] Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z. and Kocaoğlu, R.,(2021) "Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking", Electronics, vol.10, no.11, pp.1227.

[22] Khempetch, T. and Wuttidittachotti, P.,(2021) "DDoS attack detection using deep learning", IAES International Journal of Artificial Intelligence, vol.10, no.2, pp.382.

[23] Pajila, P.J., Julie, E.G. and Robinson, Y.H.,(2022) "FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks", Wireless Personal Communications, vol.122, no.4, pp.3053-3083.

[24] Wang, J., Liu, Y. and Feng, H.,(2022) "IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks", Mathematical Biosciences and Engineering, vol.19, no.2, pp.1280-1303.

[25] Eliyan, L.F. and Di Pietro, R.,(2021) "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges", Future Generation Computer Systems, vol.122, pp.149-171.