International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Detection of DDoS Attack in Software-Defined Networking Environment and Its Protocol-wise Analysis using Machine Learning

Ashwani Prasad[1], Sanjana Prasad[2], Karmel Arockiasamy[3*], Karthika P[4], Xiaohui Yuan[5]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract: Distributed-denial-of-service (DDoS) attacks can cause a great menace to numerous organizations and their stakeholders. On a successful launch of such attacks, the intended users of the network become deprived of its services, which eventually causes a loss of time and money. Not just the traditional networks were victims of DDoS attacks, even the modern networks based on software-defined networking (SDN) technology are susceptible to them. The objective of this research work is to take into account a DDoS afflicted SDN specific dataset and detect the malicious traffic by using various machine learning algorithms namely., K-Nearest Neighbours, Logistic Regression, Multilayer Perceptron, Iterative Dichotomiser 3, and Stochastic Gradient Descent. Additionally, the categories of malicious traffic based on the protocol as ICMP attack, TCP SYN attack and UDP flood attack are analyzed and compared. The experiment results suggested that some algorithms were able to detect malicious traffic with accuracies up to 99.993%. The models used in this paper are further evaluated and validated with Area Under the Curve of Receiver Operator Characteristic (AUC-ROC) curves. Therefore, through the methodologies presented in this paper, the most suitable techniques for DDoS detection are suggested and thus contribute towards the DDoS mitigation in network management of SDN environments.

Keywords: *DDoS detection; TCP SYN attack; ICMP attack; UDP flood attack; Software-Defined Networking; Machine Learning*

1. Introduction

A Distributed denial service of attack refers to a suspicious attack that can disrupt the normal functioning of a system server by flooding the target and its subordinate components with immense server traffic. A DDoS attack is successfully launched by making use of multiple source computers to launch an attack on the target system. Mostly the target system could either be a network of machines configured to a common network or other systems connected in a network such as IoT devices. In a convention, the attacker, who uses DDoS attacks, consists of a huge number of machines and bombards a huge number of packets onto the victim server [1]. In a simple analogy, A DDoS attack can be visualized in a way similar to an unpredictable traffic jam blocking a road due to which the regular traffic of vehicles remains stagnated in a place.

The objective of an application layer attack is to drain the resources possessed by the target system to facilitate the attack. Such an attack as the name suggests is meant for web pages wherein a response is provided to HTTP requests. The intensity of such an attack is so strong due to the volume of traffic it can generate. An HTTP attack is a result of multiple requests flooding the server, wherein the attack is launched by gaining access to IP addresses and URLs. Protocol attacks are a result of over-exhaustion of the target server's resources namely load balancers or firewalls. Protocol attacks take advantage of the vulnerabilities in layer three and layer four of the protocol stack, thereby affecting the target server and rendering it useless. An SYN flood attack plays a role similar to that of a receptionist, who can take incoming requests from multiple customers. The process starts with the worker, who upon receiving a request, waits for confirmation to forward that to a target server. Upon reaching a maximum level of requests, the server gets overwhelmed due to which there will be no responses for the requests received. Such an attack is known for affecting the TCP handshake mechanism, which plays an important role in facilitating a network connection, by flooding the target with lots of SYN packets with spoofed IP addresses. Volumetric attacks cause traffic by excessively consuming the bandwidth between the target and the internet, wherein the target is bombarded with an enormous amount of data, by using botnets for creating multiple requests. In such an attack, Identifying the attacker becomes challenging, because the IP addresses that are used are spoofed and randomly generated.[2] suggests a possible solution, the use

[1,2,3,4] *School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu 600127, India*
ORCID ID:0000-0002-7031-4190, 0000-0002-3602-4990, 0000-0003-2706-2239, 0000-0002-8319-9371
[5]*Associate Professor, Department of Computer Science and Engineering University of North Texas, Denton, TX 76203*
** Corresponding Author Email: karmel.a@vit.ac.in*

of the entropy concept to study the network traffic on all phase using cluster analysis techniques.

This research articcle is organized as follows: Section 2 makes a survey about various mechanisms and machine learning algorithms that have been implemented to diagonise the attack, the proposed methodology is explained in section 3. Section 4 gives a detailed explanation of the results of the simulation. Section 5 covers the future work and conclusion.

2. Related Work

In a study of [3], traffic records in the network were recorded as images. Later multivariate coherence analysis was deployed for detecting the traffic with utmost accuracy, following the conversion of the data onto images. This technique of computer vision is also known as the Earthmovers distance method, which is based on the measured distance between the probability distributions. In [4] Artificial neural networks were deployed, wherein an algorithm was used for training a given dataset. This methodology was contrasted with other techniques such as back-propagation, support vector machines (SVMs), chi-square, and Snort, thereby delivering an attack detection accuracy of 98%. Yan et al. took into consideration different features to detect the occurrence of an attack [5]. Since more than one parameter plays a role in determining the occurrence of the attack, the objective is related to how the detrimental features are determined. The internet protocol address of the destination is taken to be one of the major parameters that are detected using entropy. Cui et al. [6] deployed the neural network algorithm to reduce the controllers and switch workload, as a means of detecting the attack in a faster way. This made use of entropy-based classification algorithms to observe low and high-volume DDoS attacks. Researchers in [7] implemented their model using 2 data mining algorithms namely Ripper and C5.0. This model was deployed on UNB-ISCX datasets wherein 99% Accuracy of detecting the attack was achieved. A [8] feature selection technique was utilised in conjunction with a dynamic multilayer perceptron to identify the attack, with a feedback mechanism used to reset the system if the detection was not precise. As the complexity of the network traffic increases, some of the features may fail to distinguish between traffics and attacks and may fail in accurately detecting the attack. Liang and Znati used statistical approaches for predicting the attacks [9] in contrast to Machine learning techniques. In this method, in addition to computing distance measurements, traditional distributions were utilised to forecast the network's normal and abnormal behaviours, and classifiers such as K-means, SVMs, and decision trees were used. Criscuolo used an entropy-based method along with a classification algorithm to distinguish between low and high volume DDoS attacks [10]. The primary methodology of such a mechanism is a two-class classification task used to differentiate between normal flows and attacks. The statistics of network flows and communications are recorded using switches for a defined period of time. The statistics collected comprise the total bytes of data transmitted, the count of data packets transmitted, and the transmission time of the packets. Once two hosts have established a connection, the packet to be stored next to the IP source is delivered to the controller, together with the source port, destination IP, packet bytes, and packet arrival time[11]. This procedure is carried out for each data packet. When all of the flows are ready, the statistics between the two hosts are made available and supplied to the controller. Zhong and Yue proposed an attack mitigation model [12] based on a data mining algorithm, in which an FCM cluster algorithm a priori association algorithm extracted the network traffic model and the network packet protocol status model, followed by the definition of a detection model threshold. Wu et al. [13] presented a detection approach involving a decision tree and grey relational analysis. Detecting an attack in a normal network context is a classification issue, with 15 different attributes available not only to monitor the flow of data packets across the network channel, but also to combine the TCP SYN and ACK Flag rates to reflect the flow of traffic in the channel. Taking into account the specified qualities, the decision tree model was utilised to detect irregular traffic flows in the network. To categorise traffic and detect DDoS attacks, Chen et al. [14] presented a probabilistic neural network-based classification approach. Bayes decision rule for In order to classify DDoS attack traffic, Bayes interferences were combined with a radial basis function neural network. The accuracy of detecting the attack was found to improve by combining SVMs with other techniques in the study by Li et al. [15]. SNORT and a firewall were used to develop an intelligent system module for prevention. To boost detection accuracy, the SVM classifier was integrated with SNORT.

3. Proposed Methodology

3.1. Architecture

Figure 1 shows the complete architecture of the proposed method. The data management module comprises the data collection, data pre-processing, and the creation of subsets of the original dataset based on the protocol. The data collection is achieved from the SDN dataset obtained from During the data pre-processing step, the null values or the missing values are removed from the dataset, if there are any. Next, three subsets of the pre-processed dataset are created based on the three protocols (TCP, UDP, and ICMP).

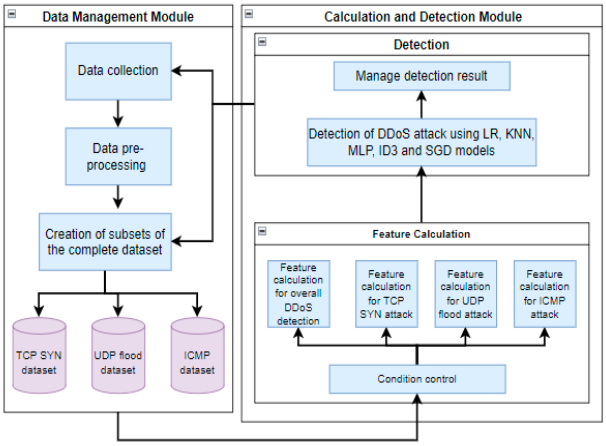

Fig.1 The architecture of the proposed method.

Thus, for this research work, four pre-processed datasets are under consideration:

a. The complete SDN dataset for detection of DDoS attacks irrespective of the protocol involved.
b. The dataset based on the TCP protocol for the detection of TCP SYN attacks.
c. The dataset based on the UDP protocol for the detection of UDP flood attacks.
d. The dataset based on the ICMP protocol for the detection of ICMP attacks.

The calculation and detection module calculates the features and performs the required detection of the DDoS attacks. The features (or attributes of the dataset) showing higher covariances amongst themselves are selected for training and testing of the models used for the prediction of the attacks. The dataset under consideration is split into training and testing data sets in the ratio of 70:30. Thus, 30% of the data is set aside for validation purposes.

The calculation and detection module then uses a variety of machine learning algorithms to detect the DDoS attack, including Logistic Regression (LR), K-Nearest Neighbors (KNN) with three nearest neighbours, Multilayer Perceptron (MLP) with an alpha value of 0.005, Iterative Dichotomiser 3 (ID3), and Stochastic Gradient Descent (SGD). Finally, the detection results obtained from each of the models are evaluated and compared with each other. This method has some essential control conditions:

a. Feature calculation is separately done for the complete dataset, the TCP SYN dataset, the UDP flood dataset, and the ICMP dataset.
b. Only the features with higher correlation values are to be selected for the training and testing purposes from each dataset.

3.2. Feature Selection for DDoS Detection

The overall DDoS attack detection feature selection from the given dataset consists of 19 characteristics that were chosen as "priori" for pre-processing. They are: dt, switch, pktcount, bytecount, dur, dur_nsec, tot_dur, flows, packetins, pktperflow, byteperflow, pktrate, Pairflow, port_no, tx_bytes, rx_bytes, tx_kbps, rx_kbps, and tot_kbps. The "label" attribute is taken as the target variable. The correlation value is greater than 0.70. Finally, there were 12 accepted features: dt, pktcount, bytecount, dur, flows, packetins, pktrate, Pairflow, tx_bytes, rx_bytes, rx_kbps, and tot_kbps. This selection of features reduces overfitting while making the prediction.

3.3. Feature Selection for the detection of TCP SYN Attack

The feature selection for the TCP SYN attack detection consists of a total of 19 features selected as "priori" for pre-processing. They are switch, Pairflow, pktcount, bytecount, dur, dur_nsec, tot_dur, port_no, tx_bytes, rx_bytes, dt, flows, pktperflow, byteperflow, pktrate, packetins, tx_kbps, rx_kbps, and tot_kbps. The "label" attribute is taken as the target variable.

3.4. Feature Selection for ICMP Attack

For the detection of ICMP attacks, there are 19 important features selected as "priori" for pre-processing. There are switch, Pairflow, pktcount, bytecount, dur, dur_nsec, tot_dur, port_no, tx_bytes, rx_bytes, dt, flows, pktperflow, byteperflow, pktrate, packetins, tx_kbps, rx_kbps, and tot_kbps. Again, the target variable is "label" attribute. A total of 6 features are selected because of high correlation values viz. bytecount, packetins, pktrate, byteperflow, pktperflow, and pktcount.

The predictive accuracy and control over-fitting, can be improved applying a random forest classifier to find the correlation values as listed in Table 1 for all three types of attacks. For TCP SYN attack, there were 8 accepted features: bytecount, dt, packetins, pktrate, byteperflow, pktperflow, pktcount, and dur. These features are chosen as they show higher correlation values as compared to the rest.

Table 1. The correlation values obtained from Random Forest Classifier

SI. No.	Features	Correlation		
		TCP SYN attack	UDP flood attack	ICMP attack
1	packetins	0.263485	0.019465	0.001993
2	pktperflow	0.185474	0.295532	0.133582
3	pktrate	0.160153	0.274402	0.079557
4	byteperflow	0.123263	0.307648	0.140347
5	dt	0.092269	0.005794	0.001025
6	bytecount	0.044658	0.014034	0.363368

7	pktcount	0.0275	0.010009	0.218542
		87		
8	dur	0.0200	0.031652	0.026462
		19		
9	tot_dur	0.0167	0.033385	0.017009
		72		
10	dur_nsec	0.0121	0.004576	0.001536
		20		
11	tot_kbps	0.0117	0.000498	0.002173
		91		
12	tx_bytes	0.0114	0.001702	0.000341
		07		
13	flows	0.0112	0.000667	0.000350
		12		
14	switch	0.0058	0.000368	0.002232
		07		
15	rx_bytes	0.0056	0.000231	0.000227
		80		
16	rx_kbps	0.0050	0.000009	0.002403
		20		
17	tx_kbps	0.0026	0.000012	0.002173
		15		
18	port_no	0.0006	0.000016	0.000007
		69		
19	Pairflow	0.0000	0.000000	0.003985
		00		

4. Results and Discussion

4.1. Model Performance Comparison

The performance measures such as the accuracy, precision, F-measure (F1 score), True Positive Rate (TPR) also known as Recall or Sensitivity, False Positive Rate (FPR), True Negative Rate (TNR), also called Specificity, and False Negative Rate (FNR) are used to evaluate the performance of the models.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$TPR = \frac{TP}{TP + FN}$$

$$TNR = \frac{TN}{TN + FP}$$

$$FPR = \frac{FP}{FP + TN} = 1 - TNR$$

$$FNR = \frac{FN}{TP + FN}$$

$$F - \text{Measure} = \frac{2 * \text{Precision} * TPR}{\text{Precision} + TPR}$$

The values of TP, FP, FN, and TN are obtained from the confusion matrix for each model. Figure 2 depicts a bar graph that showcases the accuracy of the models in ascending order for the overall DDoS attack detection. While Figure 2 illustrates the accuracy in detecting TCP SYN attacks, UDP flood attacks, and the ICMP attack for different models in the form of a line graph. From Figure 2, it is observed that the decision tree algorithm (ID3) is showing the best accuracy in detecting the DDoS attack, while the LR model shows the least score for the same. KNN and MLP are also performing comparably with respect to the ID3.

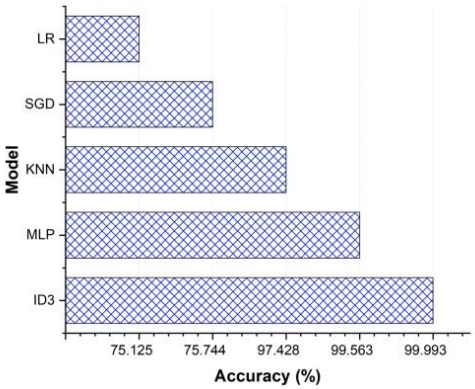

Fig 2 Accuracy of the models in detecting the overall DDoS attack

In Fig 3, for the TCP SYN detection, KNN and ID3 are performing better than the rest with accuracy values greater than 99%. However, the MLP, LR, and SGD are showing decent performance with respect to accuracy. Next, for the UDP flood attack, all the models show high accuracy with values greater than 90 %. Lastly, for the ICMP attack detection, all the five models are showing high values accuracy which is more than 98%. LR, KNN, MLP, and ID3 are showing 100% accuracy in detecting the ICMP attack. Overall, it is observed that the ID3 model is the best fit for predicting the attacks based on the three protocols as well as for the overall DDoS attack detection.

Fig 4 (a-d) illustrate the accuracy, precision, F1-score, and recall for all the five models in each case. The value ranges from 0 to 1. Moreover, Table 4 shows the complete summary of the performance measure excluding accuracy of all the proposed models for label 1 (i.e., when the traffic is malicious).

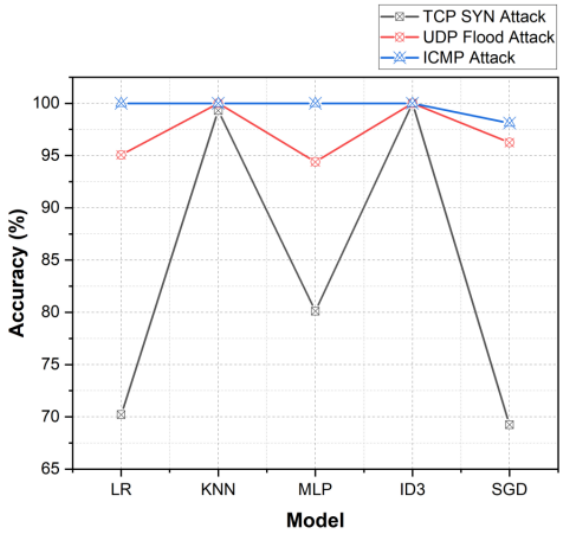

Fig. 3 Accuracy of the models in detecting the TCP SYN attacks, UDP flood attacks, and the ICMP attacks

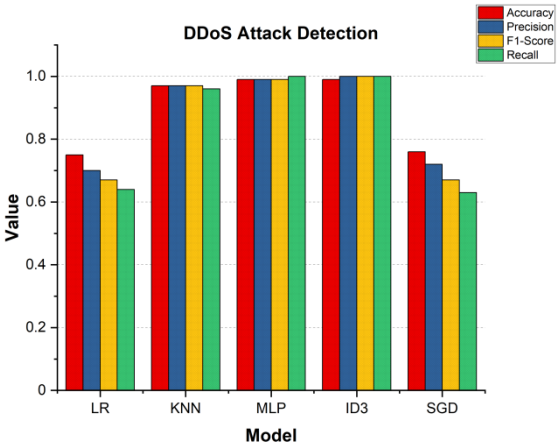

Fig 4(a): DDoS Attack Detection

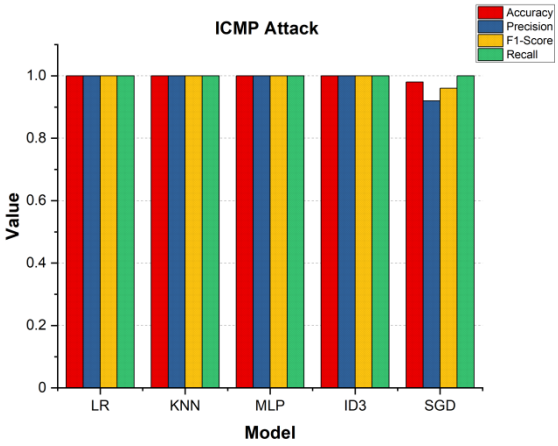

Fig 4(d): ICMP Attack

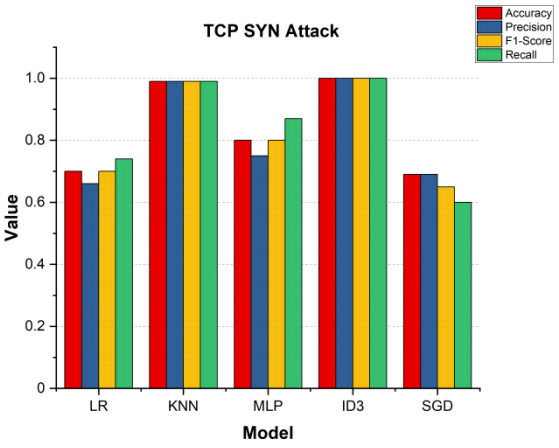

Fig 4(b): TCP SYN attack

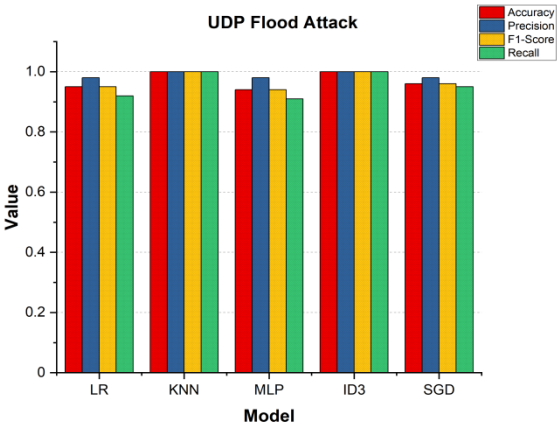

Fig 4(c): UDP Flood Attack

4.2. Model Evaluation

A binary classification evaluation statistic is the Receiver Operator Characteristic (ROC) curve. It's a probability curve that compares TPR to FPR at various thresholds to effectively extract the "signal" from the "noise." The AUC (Area Under the Curve) is a summary of the ROC curve that indicates how well a classifier can distinguish between classes. The AUC measures the model's ability to distinguish between positive and negative classes. The model's performance improves as the AUC increases. Table 2 shows the AUC score of the five models for the detection result.

Table 2: AUC scores of the detection result

	Models				
Category	LR	KNN	LP M	ID3	SGD
DDoS detection	0.83	0.99	0.99	0.99	0.81
TCP SYN Attack	0.80	0.99	0.82	1	0.5
ICMP Attack	1	1	1	1	0.5
UDP flood Attack	0.99	1	0.94	1	0.5

The model can distinguish between all positive and negative class points when AUC = 1. When the AUC is 0.5, the model is very likely to be able to differentiate between positive and negative class points. As observed in the case of the SGD model for detecting TCP SYN, UDP flood, and ICMP attacks, if AUC = 0.5, the model is unable to distinguish between positive and negative class points. This is due to the model's ability to recognise more number of rue positives and True negatives compared to False negatives and False positives.

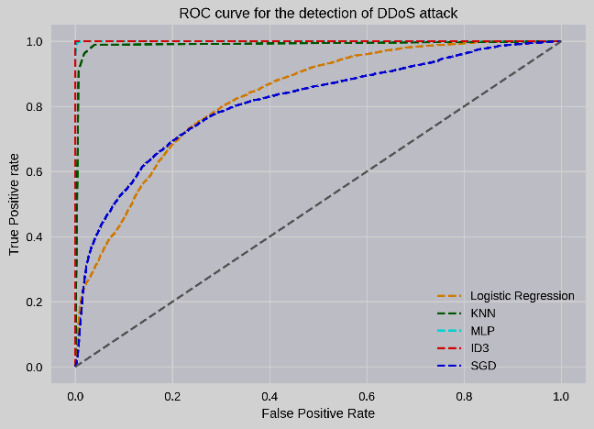

Fig 5(a): TCP SYN attack

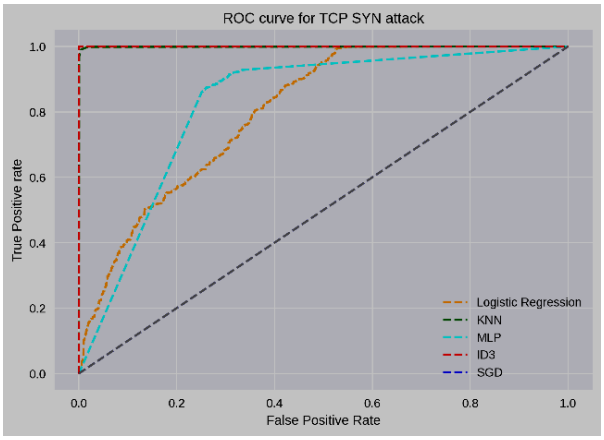

Fig 5(b): ROC curve for the detection of DDos Attack

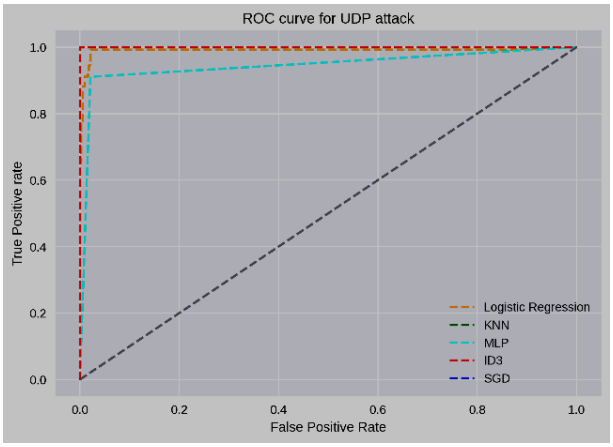

Fig 5(c): ROC curve for the detection of UDP attack

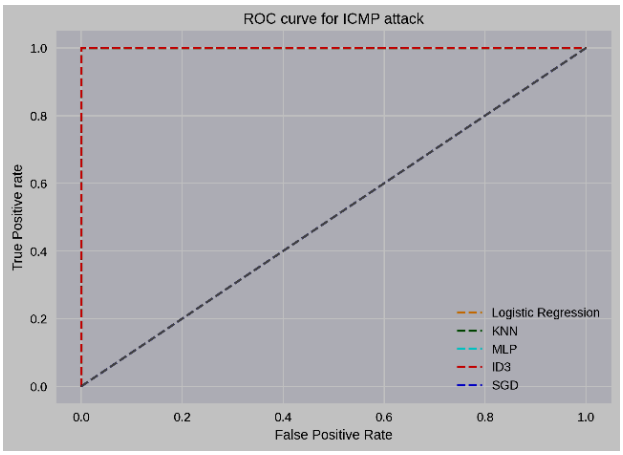

Fig 5(d): ROC curve for the detection of ICMP attack

Figures 5(a-d) consist of four ROC plots for each kind of detection. It is evident from Figures 5(a), 5(b), and 5(c), that AUC for the ID3 ROC curve is higher than that of the other models. This indicates that ID3 is outperforming other models in classifying the positive class in the respective datasets. But in plot 5(d), the AUC for the ROC curves of all the models are overlapping which implies that all the models are doing a better job of classifying the positive class in the ICMP attack dataset.

5. Conclusion and Future Work

Machine learning algorithms namely K-Nearest neighbours, linear regression, multi-layer perceptron, decision tree, and stochastic gradient descent were exploited to observe DDoS attacks in the SDN environment. Most of the algorithms were able to detect the attack with an accuracy of more than 90 percent. The attack was also investigated and discovered based on their protocols. TCP SYN attacks, ICMP attacks and UDP flood attacks were analysed with the same set of algorithms. The detection result achieved a high-performance metric which shows that the proposed methodology shows a high-performance metric for the DDoS attacks detection in an SDN environment. The algorithms and their performance were validated using ROC-AOC curves.

As far as future work is concerned, the same dataset can be researched thoroughly by considering a different set of features on which the models shall run. Other machine learning algorithms could also be used to implement which are relatively recent and potentially more efficient like the XGBoost and Lasso Regression. Furthermore, protocol-specific analysis can be performed using deep learning methods such as Convolutional Neural Networks and Long Short-term Memory, and the results can be interpreted. Similar algorithms can also be implemented on a more recent SDN-based dataset to determine their efficacy and reliability in terms of the detection of cyber-attacks like DDoS.

References

[1] Wankhede, S., & Kshirsagar, D. (2018). DoS Attack Detection Using Machine Learning and Neural Network. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).

[2] Lee, K., Kim, J., Kwon, K. H., Han, Y., & Kim, S. (2008). DDoS attack detection method using cluster analysis. Expert Systems with Applications, 34(3), 1659–1665. doi:10.1016/j.eswa.2007.01.040

[3] Tan Z, Jamdagni A, He X, Nanda P, Liu RP, Hu J (2014) Detection of denial-of-service attacks based on computer vision techniques. IEEE Trans Comput 64(9):2519–2533

[4] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[5] Saied A, Overill RE, Radzik T (2016) Detection of known and unknown DDoS attacks using artificial neural networks. Neurocomputing 172:385–393

[6] Yan Q, Gong Q, Deng F-A (2016) Detection of DDoS attacks against wireless SDN controllers based on the fuzzy synthetic evaluation decision-making model. Adhoc Sens Wirel Netw 33

[7] Patil, V. N., & Ingle, D. R. (2022). A Novel Approach for ABO Blood Group Prediction using Fingerprint through Optimized Convolutional Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 60–68. https://doi.org/10.18201/ijisae.2022.268

[8] Cui Y, Yan L, Li S, Xing H, Pan W, Zhu J, Zheng X (2016) SD-Anti-DDoS: fast and efficient DDoS defense in software-defined networks. J Netw Comput Appl 68:65–79

[9] Fallahi N, Sami A, Tajbakhsh M (2016) Automated fow-based rule generation for network intrusion detection systems. In: 24th Iranian Conference on Electrical Engineering (ICEE). IEEE, pp 1948–1953

[10] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[11] Wang M, Lu Y, Qin J (2020) A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Comput Secur 88:101645

[12] Liang X, Znati T (2019) On the performance of intelligent techniques for intensive and stealthy DDoS detection. Comput Netw 164:106906

[13] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[14] Criscuolo, P. J. (2000). Distributed denial of service Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht CIAC-2319. Department of Energy Computer Incident Advisory (CIAC), UCRLID-136939, Rev. 1, Lawrence Livermore National Laboratory

[15] Haghaghi A, Kaafar MA, Buyya R, Jha S (2020) Software-defined network (SDN) data plane security: issues, solutions, and future directions. In: Handbook of Computer Networks and Cyber Security. Springer, pp 341–387

[16] RZhong and G. Yue, "DDOS detection system based on data mining," in Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2010, pp. 2–4

[17] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[18] YC. Wu, H.-R. Tseng, W. Yang, and R.-H. Jan, "DDOS detection and traceback with decision tree and grey relational analysis," International Journal of Ad Hoc and Ubiquitous Computing, vol. 7, no. 2, pp. 121– 136, 2011

[19] JH. Chen, M. Zhong, F.-J. Chen, and A.-D. Zhang, "DDOS defense system with turing test and neural network," in IEEE International Conference on Granular Computing (GrC). IEEE, 2012, pp. 38–43.

[20] H. Li and D. Liu, "Research on intelligent intrusion prevention system based on snort," in International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), vol. 1. IEEE, 2010, pp. 251–253

[21] Ahuja, Nisha; Singal, Gaurav; Mukhopadhyay, Debajyoti (2020), "DDOS attack SDN Dataset", Mendeley Data, V1, doi: 10.17632/jxpfjc64kr.1.

[22] Liu, Z., Hu, C., & Shan, C. (2021). Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method. Computers & Security, 109, 102392. https://doi.org/10.1016/J.COSE.2021.102392

[23] Ahuja, Nisha; Singal, Gaurav; Mukhopadhyay, Debajyoti (2020), "DDOS attack SDN Dataset", Mendeley Data, V1, doi: 10.17632/jxpfjc64kr.1

[24] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[25] C. Liu, Z., Hu, C., & Shan, C. (2021). Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method. Computers & Security, 109, 102392. https://doi.org/10.1016/J.COSE.2021.102392