SDN based DDoS Detection using Machine Learning and Deep Learning Techniques

Abstract:

Software-Defined Networking (SDN) is an emerging paradigm, which evolved in recent years to address the weaknesses in traditional networks. The SDN's main goal is to separate the control and data planes, making network management easier and enabling for more efficient programmability. The centralized structure of SDN brings new vulnerabilities. Distributed Denial-of-Service (DDoS) is one of the most prevalent and sophisticated threat. DDoS attack tries to disrupt the available services of a victim to block the victim from providing service to the legitimate users, by sending massive malicious requests from a large number of hijacked machines. DDoS attacks are easy to initiate, hard to defend and strong destructive effect. So that accurate detection of DDoS attack is necessary. In recent years, many studies have been done to secure SDN using Machine Learning and Deep Learning techniques. In this work Supervised Machine Learning algorithms such as Logistic Regression, Gaussian Naive Bayes, SVM, Decision Tree, Random Forest and Gradient Boosting are employed for DDOS detection in SDN environments. The unsupervised Machine Learning technique such as K Means clustering with PCA and TSNE dimensionality reduction technique is used. In case of Deep Learning techniques DNN, Auto Encoder and XGBOOST, CNN, LSTM, BiLSTM, TabNet and TCN are used for DDoS detection. The dataset used is DDoS attack SDN DDoS dataset. This is a publically available DDoS dataset created in SDN environment. The experimental result shows that TCN performs well in SDN DDoS dataset and achieve an accuracy of 99.69%. The results are validated using another dataset called INSDN dataset. It is a comprehensive SDN dataset to verify the performance of intrusion detection systems. TabNet gives highest accuracy of 99.98% in INSDN dataset and TCN gives 99.96% accuracy in INSDN dataset.

Introduction:

We are in the era of exponentially growing digitalization. The role of emerging information and communication technologies in our day-to-day life is undeniable. Moreover, it creates new security concerns. These systems are vulnerable to various cyber threats and attacks. The Software-Defined Network (SDN) is a new network paradigm promises more dynamic and efficiently manageable network architecture. The network intelligence is logically decoupled and centralized into the Control layer. The major benefit of SDN is that it separates the control and data planes, making the network more versatile and easier to manage. The entire system can be managed by a single distant computer known as the controller. Many business-related and industrialized enterprises are implementing SDN technology in their network environments.

The centralized structure of SDN brings new vulnerabilities to the system. Distributed Denial of Service (DDoS) are the most prevalent and sophisticated attack. DDoS attack tries to overwhelm the available resources of a victim from providing service for normal users, by sending massive malicious requests from a huge number of hijacked machines. DDoS attacks are easy to initiate, there have been a certain number of easily obtainable DDoS attack tools. DDoS attacks are hard to defend and it has strong destructiveness. Many companies such as Amazon, Facebook,

Twitter, GitHub suffered DDoS which leads to big losses. So it is necessary to accurately detect DDoS attack and protect the system.

The first line of defense against these attacks are Network Intrusion Detection System (NIDS). Artificial Intelligence is now commonly used in defensive measure. The Machine Learning algorithms such as SVM, Naïve bayes, Decision Tree, Random Forest are used for the DDoS detection. The Deep Learning Techniques such as DNN, Auto Encoders, CNN, LSTM, TabNet and TCN can significantly improve the performance of DDoS detection systems.

This work concentrates on implementation and testing of detecting DDoS attack in SDN environment by three approaches.

a. Supervised with traditional ML algorithms
b. Unsupervised approach of clustering and dimensionality reduction
c. Supervised with Neural Networks

This paper is organized as follows: Section II briefly discusses recent related works in DDoS detection in SDN environments. Section III presents the methodology. An exhaustive discussion on the experimental results is summarized in Section IV. Section V presents the conclusion.

Literature Review:

SL NO	TITLE	TECHNIQUES USED	ADVANTAGES	DISADVANTAGES
1	Machine Learning Approach Equipped with Neighborhood Component Analysis for DDoS Attack Detection in Software-Defined Networking [1] (2021)	NCA KNN Decision Tree ANN SVM	NCA gives most relevant features by feature selection, UpToDate dataset	Does not give optimal number of features to be selected, The performance depends on the selected features
2	Clustering based semi-supervised machine learning for DDoS attack classification [2] (2019)	Agglomerative clustering K means clustering KNN, SVM, Random Forest	Optimizing and validating the model improves the performance	Clustering approach leads to high false positive values
3	Detection of DDoS attacks with feed forward based deep neural network model [3] (2021)	DNN	High accuracy	Failed to detect adversarial attack

4	A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks [4] (2020)	RNN LSTM CNN RNN+LSTM	Improved accuracy Minimal computational complexity	Failed to detect adversarial DDoS attacks
5	DDoSNet: A Deep-Learning Model for Detecting Network Attacks [5] (2020)	RNN AutoEncoder	Temporal correlation of data is considered	Vanishing Gradient problem
6	Intrusion Detection in SDN-Based Networks: Deep Recurrent Neural Network Approach [6] (2019)	GRU-RNN GRU-DNN	The method offers a lot of potential for real-time detection	The model is not optimized for improving accuracy and reduce controller overhead

Methodology:

Many studies have shown that Machine Learning capabilities produce excellent results in a variety of applications. Here supervised Machine Learning techniques, unsupervised Machine Learning techniques and Deep Learning techniques such as DNN, Auto Encoder, CNN, LSTM, BiLSTM, TabNet and TCN are employed for DDoS detection in SDN environment.

Dataset:

DDoS Attack SDN Dataset: This is a SDN specific data set generated by using mininet emulator and used for traffic classification by Machine Learning and Deep Learning algorithms. The network simulation is run for both benign TCP, UDP, and ICMP traffic. The dataset contains a total of 23 features. Last column denotes the class label which indicates whether the traffic type is benign or malicious. Benign traffic has label 0 and malicious traffic has label 1. Network simulation is run for 250 minutes, and 1,04,345 rows of data is collected.

DDoS Attack SDN Dataset Pre-processing: Before applying Machine Learning and Deep Learning techniques, we have to preprocess the dataset. The first step is to convert the Categorical variables such as source-destination IP and protocol that do not have numeric values. The rx_kbps and tot_kbps features having missing values in the dataset and that is filled with the mean value. The IP address is grouped based on 'dt' feature and count the number of request coming from the IP. Find the correlation between features by using heat map graph. Then standardize the data using standard scalar.

INSDN Dataset: Comprehensive SDN dataset to verify the performance of intrusion detection systems. Total 84 features and 136743 network flows are available in the data set. The INSDN dataset includes different attacks that can strike the data, control, and application layers. The INSDN dataset consist of 5 types of attacks including DDoS, Dos, Probe, BFA and U2R.

INSDN Dataset Pre-processing: In the pre-processing stage the distribution of five category of attack is plotted. Removed the duplicate values from the dataset. The categorical variables such as Flow ID, Source and destination IP and Time stamp are converted into numerical values. The source IP is grouped based on 'Timestamp' feature and count the number of request coming from the IP. Find the correlation between features by using heat map graph. Then standardize the data using standard scalar.

Supervised Machine Learning Techniques: The supervised Machine Learning algorithms such as Logistic regression, SVM, Gaussian Naïve Bayes, SVM, Decision Tree, Random Forest and Gradient Boosting are used for DDoS detection.

Logistic Regression: Logistic regression is a linear model for binary classification problems. The dataset is loaded and splitted in to features and labels. Then the dataset is divided in to training and testing set (20% for testing and 80% for training). The logistic regression model is created, model is trained on the dataset and test the model.

Gaussian Naïve Bayes: A variant of Naïve Bayes algorithm that follows Gaussian normal distribution and supports continuous data. The Bayes Theorem is used to create Naive Bayes Classifiers. These classifiers make the assumption that the value of one feature is unrelated to the value of any other characteristic. The Gaussian Naïve bayes model is created, model is trained on the dataset and test the model.

Support vector Machines (SVM): The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane. SVM chooses the extreme points that help in creating the hyperplane, these are support vectors.

Decision Tree: It is a tree structured classifier; a decision tree is drawn upside down with its root at the top. In a Decision tree, there are two nodes, which are the Decision Node and Leaf Node. Internal nodes represent the features of a dataset, branches represent the decision rules, and each leaf node represents the outcome. Decision nodes are used to make any decision and have multiple branches, whereas Leaf nodes are the output of those decisions and do not contain any further branches. This methodology is more commonly known as learning decision tree from data and the tree is called Classification tree as the target is to classify whether the traffic is Normal or DDoS. The dataset is divided into training and testing sets. The training set is applied as the input to the root of the tree. The prone procedure is carried out and repeated until all nodes becomes leaf nodes.

Random Forest: Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset. Random forest takes the prediction from each tree and based on the majority votes of predictions it predicts the final output. The model is created with Random forest and trained on the dataset, test the model on the test set.

Gradient Boosting: Powerful ensemble machine learning algorithm that uses decision trees. Decision trees are used as the weak learner in gradient boosting. A gradient descent procedure is used to minimize the loss when adding trees. The objective is to minimize the loss. The gradient boosting model is created, trained on the training set and test on the test set.

Unsupervised Techniques: The goal of this unsupervised machine learning technique is to find similarities in the data point and group similar data points together. Clustering is the important technique in case of unsupervised learning.

K Means Clustering: K Means tries to group the data into a predetermined number of clusters. The purpose of K Means is to find data points that are similar and cluster them together while attempting to distance each cluster as far as possible. Here PCA and TSNE dimensionality reduction techniques are used and compared with K Means clustering. The dataset is loaded and apply K means on the original dataset. Feature reduction is done by PCA and apply K means on the PCA components. Then feature reduction is done by using TSNE, apply K means on the TSNE components. Finally compared the PCA and TSNE K means derived clusters.

PCA: PCA or principal component analysis, is a well-known approach for reducing high-dimensional data to a low-dimensional space. The data or differences from our original features are "squeezed" into what PCA refers to as main components (PC). The majority of the information from the original features will be stored on the first PC. The second PC will have the second-largest quantity of data and so on. The PCs are not correlated (orthogonal), which means that each one has its own set of data.

T-SNE: T-SNE is a method for reducing high-dimensional data to a low-dimensional graph. It is also a strategy for reducing dimensionality. T-SNE can decrease dimensions with non-linear relationships, unlike PCA.

Deep Learning Techniques: Deep Learning is capable of automatically finding correlations in raw data, and it has the advantage of supervised and unsupervised learning. Deep Learning techniques can significantly improve the performance of DDoS detection. To classify the network traffic into normal and DDOS attack traffic, DNN, Auto Encoder and XGBOOST, CNN, LSTM. BiLSTM, TabNet and TCN are employed for DDoS detection.

Deep Neural Network (DNN): The DNN model is created with sequential model having input layer, 3 hidden layer and output layer. The input layer having 22 neurons corresponds to 22 features in the dataset and relu activation function used. The hidden layers consist of equal number of 30 neurons and relu activation function is used. There are also two dropout layers with dropout ratio 0.2. The output layer consists of 2 neurons with softmax activation function because it is a binary classification problem. Compile the model using ‘Sparse categorical cross entropy’ loss function and ‘ADAM’ optimizer. Fit the model with 20 epochs and batch size selected is 16.

Auto Encoder and XGBOOST Classifier: Auto Encoder is a type of neural network that can be used to learn a compressed representation of raw data. Auto Encoder is used for the feature

extraction. The encoder compresses the input, and the decoder attempts to recreate the input from the compressed version provided by the encoder. After training, the encoder model is saved, and the decoder is discarded. The encoder can then be used as a data preparation technique to perform feature extraction on raw data that can be used to train XGBOOST classifier. XGBoost, which stands for extreme Gradient Boosting, is a scalable, distributed gradient boosted decision tree.

Convolutional Neural Network (CNN): CNN has proven to be effective in many various studies and applications specifically in image classification field. CNN consists of multiples layers: input layer, convolutional layers, pooling layers, fully connected layer and output layer. Deepness of the CNN dependence on the number of layers used. 1D CNN is used for the DDoS detection in SDN environment. The CNN model is created with sequential model having input layer, 2 convolution layer, batch normalization layer, max pooling layer, 2 dropout layer, flatten layer and 2 dense layer. The input layer consist of 22 neurons corresponds to 22 features selected and relu activation function used. The output layer consists of 2 neurons with softmax activation function. CNN model is compiled with Sparse categorical cross entropy and Adam optimizer.

Log Short Term Memory (LSTM): Long-term and short-term memory model is a special RNN model, which is proposed to solve the problem of vanishing gradient and short term memory of RNN model. LSTM model replaces RNN cells in the hidden layer with LSTM cells to make them have long-term memory ability. The LSTM model is created with sequential model. The LSTM architecture consist of one LSTM layer with 22 neurons and tanh activation function and the kernel regularizer is l2. The Dense layer having relu activation function and l2 regularizer. The output layer having softmax activation function. The model is compiled with sparse categorical cross entropy loss function and Adam optimizer.

Bi Directional Log Short Term Memory (BiLSTM): BiLSTMs are an extension of traditional LSTMs that can improve model performance on sequence classification problems. In bi-directional, we can make the input flow in both directions to preserve the future and the past information. Bidirectional LSTMs train two instead of one LSTMs on the input sequence. The first on the input sequence as-is and the second on a reversed copy of the input sequence. The BiLSTM model is created with sequential model. The BiLSTM architecture consist of one BiLSTM layer with 22 neurons and tanh activation function and the kernel regularizer is l2. The Dense layer having relu activation function and l2 regularizer. The output layer having softmax activation function. The BiLSTM model is compiled with sparse categorical cross entropy loss function and Adam optimizer.

TabNet: TabNet is a deep neural network specifically designed to learn from tabular data, developed by the research team at Google Cloud AI. TabNet inputs raw tabular data and is trained using gradient descent-based optimization, enabling flexible integration into end-to-end learning. Use sequential attention to choose which features to reason from at each decision step, enabling interpretability and better learning as the learning capacity is used for the most

salient features. TabNet employs a single deep learning architecture for feature selection and reasoning. TabNet enables two kinds of interpretability: local interpretability that visualizes the importance of features and how they are combined, and global interpretability which quantifies the contribution of each feature to the trained model. TabNet trains on each row from a table, selects the relevant features in each step using a sparse learnable mask, and aggregates the predictions from each step to emulate an ensemble-like effect when making predictions. The TabNet classifier from Pytorch is used. The TabNet classifier model is defined and fit the model with 30 epochs.

Temporal Convolutional Network (TCN): TCN is a variation of Convolutional Neural Networks for sequence modelling tasks, by combining aspects of RNN and CNN architectures. TCN employs technique like multiple layers of dilated convolutions and padding of input sequences to handle different sequence lengths and detect dependencies between items that are not next to each other. The causal convolutions are used, where output at time *t* is convolved only with elements from time *t* and earlier in the previous layer, that is no information leakage from future to past. TCN uses a 1D fully-convolutional network (FCN) architecture, each hidden layer is the same length as the input layer. TCNs possess very long effective history sizes using a combination of very deep networks and dilated convolutions. When using dilated convolutions, it is common to increase the dilated factor d exponentially with the depth of the network. This ensures the receptive field covering each input in the history, and enabled to get an extremely large receptive field as effective history by using deep networks. For the receptive field size of the TCN depends on the network depth n as well as filter size k and dilation factor d. Residual connections have proven to be very effective in training deep networks. In a residual network, skip connections are used to speed up training process and avoid vanishing gradient problems. The Keras TCN model is used. Defined the model with the compiled TCN from Keras TCN. The model is fitted with 20 epochs.

Results and Discussion:

The experimental result of supervised Machine Learning techniques is summarized in the table II

Evaluation Metrics	LR	GNB	SVM	DT	RF	GB
Accuracy (%)	77.11	67.35	78.44	99.95	100	98.52
Precision (%)	72.68	57.54	76.16	99.93	100	97.97
Recall (%)	66.29	62.41	65.17	99.95	100	99.04
F1 score (%)	75.54	66.17	76.67	99.95	99.95	98.46

From Table II it is clearly visible that the Decision Tree, Random Forest and Gradient Boosting performs well and gives accuracy, precision, recall and F1 score near to 100 %.

The experimental result of unsupervised Machine Learning techniques is summarized in the table III.

Techniques	Sillhoutte Score
Kmeans on original dataset	0.1961007339513506
Kmeans on PCA	0.4613677492070967
Kmeans on TSNE	0.34130406379699707

We achieved a silhouette score of 0.196 in K Means on original dataset which is on the low end. We can see a definite improvement in K Means ability to cluster our data when we reduce the number of dimensions to 2 principal components. We get a K Means PCA Scaled Silhouette Score of 0.4613677492. Applying K Means to our 2 t-SNE derived components we were able to obtain a Silhouette score of 0.3413. When we compare the PCA and TSNE derived K Means cluster, PCA gives the better silhouette score.

The experimental result of Deep Learning techniques is summarized in the table IV.

Techniques	Accuracy(%)
DNN	98.39
Auto Encoder and XGBoost	97.66
CNN	99.50
LSTM	95.06
BiLSTM	95.09
TabNet	99.00
TCN	99.67

From the table IV, it is evident that the Deep Learning techniques can achieve very good results in case of DDoS detection SDN environments. The TCN gives the best accuracy in SDN DDoS dataset 99.67%. CNN, TabNet, DNN, Auto Encoder, LSTM, BiLSTM are also achieves good results 99.50%, 99.00%, 98.39%, 97.66%, 95.06%, 95.09% respectively.

Validation in INSDN dataset:

The experimental results of Deep Learning models in INSDN dataset is summarized in table v.

Techniques	Accuracy(%)
DNN	99.95
Auto Encoder and XGBoost	99.93
CNN	99.96
LSTM	99.61
BiLSTM	99.62
TabNet	99.98
TCN	99.96

From the table V, we can understand the in INSDN dataset, TabNet gives the best accuracy of 99.8% and TCN gives the second highest accuracy 99.96%. The other Deep Learning models can also achieve best accuracy for DDoS detection.

Conclusion:

This work focuses on propose and demonstrate the design, implementation, and testing of detecting DDoS by Machine Learning and Deep Learning solution that would allow end users to identify DDoS attack. The supervised Machine Learning technique such as Logistic regression, Gaussian Naive Bayes, SVM, Decision Tree, Random Forest and Gradient Boosting are employed for DDoS detection. The experiment results show that the decision Tree, Random Forest and Gradient Boosting achieves better results than other algorithms. In case of unsupervised Machine Learning techniques, K Means clustering with PCA and TSNE dimensionality reduction technique are employed for DDoS detection. The experimental result show that K Means with PCA gives the better silhouette score. In case of Deep learning techniques DNN, Auto Encoder and XGBoost, CNN, LSTM, BiLSTM, TabNet and TCN are used. For SDN DDoS dataset TCN gives the highest accuracy 99.69%. The experimental results in INSDN implies that TabNet model performs well in INSDN dataset achieves an accuracy of 99.98% and TCN gives the second highest accuracy 99.96% in INSDN dataset. The Machine Learning and Deep Learning techniques are used for the DDoS detection in SDN environment. The Deep Learning models achieves better results for DDoS detection. TabNet and TCN model performs very well and achieves highest accuracy than other Deep Learning models in both the datasets.

References:

[1] 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*, *10*(11), p.1227.

[2] Aamir, M. and Zaidi, S.M.A., 2021. Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University-Computer and Information Sciences*, *33*(4), pp.436-446.

[3] Cil, A.E., Yildiz, K. and Buldu, A., 2021. Detection of DDoS attacks with feed forward based deep neural network model. *Expert Systems with Applications*, *169*, p.114520.

[4] 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*, *8*, pp.53972-53983.

[5] Elsayed, M.S., Le-Khac, N.A., Dev, S. and Jurcut, A.D., 2020, August. Ddosnet: A deep-learning model for detecting network attacks. In *2020 IEEE 21st International*

Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 391-396). IEEE.

[6] Cui, Y., Qian, Q., Guo, C., Shen, G., Tian, Y., Xing, H. and Yan, L., 2021. Towards DDoS detection mechanisms in software-defined networking. *Journal of Network and Computer Applications*, *190*, p.103156.

[7] Devarajan, D. and Arora, K., 2021. Multiclass DDoS Detection using Machine Learning Ensemble. *Available at SSRN 3884632*.

[8] 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*, *75*(8), pp.4829-4874.