2019 IEEE Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)

DDoS attack detection and classification via Convolutional Neural Network (CNN)

Ahmed Ramzy Shaaban
Communication Department
Military Technical college
Cairo,Egypt
ramboramzy@yahoo.com

Essam Abd-Elwanis
Communication Department
Military Technical college
Cairo,Egypt
mohwanees@yahoo.com

Mohamed Hussein
Communication Department
Military Technical college
Cairo, Egypt
mhussein39273@gmail.com

Abstract— **Distributed Denial of Service (DDoS) attacks became the most widely spread attack because it is easily designed and executed but it is very difficult to detect and mitigate. Several artificial neural network (ANN) techniques were considered to detect and classify DDoS attacks. Mission control center (MCC) is responsible for controlling the spacecraft, so MCC network should maintain the availability i.e. should be protected from any kind of malicious traffic affect its availability such as DDoS attack. In this paper, convolutional neural network (CNN) technique is presented to detect and classify the DDoS traffic into normal and malicious information with an accuracy of 99 % using two different datasets. One is captured from simulated MCC network by Wireshark and the other one was a predefined open source dataset. The results are compared with other classification algorithms like decision tree (D-Tree), support vector machine (SVM), K-nearest neighbors (K-NN), and neural network (NN).**

Keywords—DDoS; availability; MCC; ANN; CNN; D-Tree; SVM; K-NN; NN.

I. Introduction

Any spacecraft needs to be controlled from the ground during communication sessions via mission control center (MCC), this MCC network might be exposed to Distributed Denial of Service (DDoS) attack so, MCC will be unavailable and will not do its function - no any commands will be sent to the satellite or receiving health state telemetry-in this section we explained the meaning of DDoS, the used mechanisms and techniques to detect and block or mitigate the various types of DDoS attack and focused on artificial neural network (ANN) techniques to classify or differentiate between normal and malicious traffic. DDoS attack could be defined with different definitions, but all these definitions have the same meaning. In general, DDoS attacker search over the network for vulnerabilities- in network devices- that could be exploited to hack or compromise these devices so, the attacker can manage and control these hacked machines remotely and launch his script on infected devices. At specific time – decided by the attacker – DDoS attacker run his script so all hacked devices start to flood the target server with high traffic at the same time to consume the bandwidth or resources of the server consequently, the victim server couldn't provide its services to the normal clients – service was denied, the main target behind a DDoS attack is to deny legitimate users from using system services/resources and decrease system availability. DDoS attack can be categorized [1] into two types: 1- Direct attacks, 2- indirect attacks some researchers named it reflector attacks. These 2 categories use the same techniques of attack but in different ways. The difference between direct and indirect will be explained in the next few words:

<u>1- Direct attacks: </u>Attacker denied or blocked the target server by sending flood of packets directly to the victim server but directly here didn't mean the traffic was sent from attacker itself but from infected or compromised machines in the network. These attacks use TCP SYN flood technique by sending large number of SYN packets to the target server and the attacker uses spoofing technique so target server replied with SYN-ACK packets to the spoofed address – replied to none – till victim server can't handle with any new requests.

<u>2- Indirect attacks: </u>the attack was carried out by using intermediary devices named reflectors such as routers so, compromised computers send the high traffic to the intermediate devices then traffic directed to the target server therefore it was named indirect attacks. In addition, indirect attacks use TCP SYN flood technique but in different way. SYN packets were sent to the intermediate devices by the attacker but using IP of target server as a source address in the packets that were sent to reflectors so it replied with SYN-ACK packets to the target server, which cannot handle all requests. There are many techniques and mechanism to detect DDoS attacks or to classify malicious traffic from normal traffic.

We used machine learning (ML) technique in this paper, so a short brief about machine learning was introduced in the next paragraph. ML is one form of artificial intelligence (AI) which give the systems the ability to learn automatically from the data itself without any programming or involvement from human. Learning process starts with information or data – in our case data was network traffic – in order to search for any patterns in the collected data to make right decision in future data. Therefore, the developed model from learning act as human brain. ML can be categorized into 3 main techniques according to Learning from data [2] book as follow :

<u>1-Unsupervised learning: </u>the model build itself by learning relationships between the data using only the input data as a training data i.e. no output data were used in learning. This type of learning used in clustering mechanisms.

<u>2-Supervised Learning:</u> in this technique, the model was built by learning from input and output data. This type of

978-1-7281-3995-119$31.00 ©2019 IEEE

learning used in 2 main categories: **a-Regression**: you have to own input data and corresponding output data. .

b-Classification: you have to own the input data and valid output labels.

3-Reinforcement Learning: input data and output labels/data are not needed to be presented to the model on pairs. This technique is still under research.

Deep learning is a form of ML that produce a great effect in computer and data processing, using various nonlinear-processing layers for extracting the valid features from the data directly. These data might be text, image or network traffic. Now deep learning is considered the new way to develop high precise model for data classification. Because at this time the availability of the huge amount of data which are needed for deep learning. Any deep neural network consists of three layers: input layer, hidden layers and output layer. Significantly, a convolutional neural network (CNN) is a form of deep neural networks and it is applied in classification of images and the Most frequently techniques [3] [4] that are used in network traffic classification are:

1- Bayes Classifier: used classification relied on Bayes theorem application.

2- Artificial Neural Network: consists of neurons that can be communicate with each other.

3- Support Vector Machine: it is one kind of supervised learning and can carry out linear and nonlinear classification effectively. The novelty in this paper is using CNN technique separately which is not considered in literature review .This paper was divided into the following sections: 1-literature survey on the applied MM algorithms which was used in DDoS classification.2- Illustrate the simulated network and the proposed algorithms used in DDoS classification .3- the results from the used algorithms.

II. Related Works

The use of deep learning mechanisms and techniques is considered new in the last decade in network field. It is difficult to detect DDoS, because it is very hard to differentiate between the malicious traffic and normal traffic. Deep learning classification methods can be used to differentiate normal and malicious traffic. Some artificial intelligence techniques like machine learning algorithms have been used to classify DDoS attack traffic and detect DDoS attacks [5] such as Naive Bayes, Random forest tree etc.

Several papers discussed detection of DDoS using Artificial Neural Network (ANN) .Model [6] detect three types of DDoS attacks by analyzing captured traffic and extract the used features but this model has shown lower accuracy in the classification of UDP attack . DDoS attack detection relied on analysis of network traffic patterns was shown in paper [7] by identifying certain parameters such as Time to Live (TTL), protocol , source port number and IP addresses. Based on these parameters, model is proposed for detecting DDoS attack by using correlation coefficients but the used data set in this paper was obsolete (since 1998).

In [8] the authors used Least Squares-Support Vector Machine (LS-SVM) , Naïve Bayes and K-Nearest techniques to make classification of the network traffic and used data set of size 6000 packet as maximum but this value was very small with respect to the network traffic in case of carrying out DDoS attack. In addition, machine learning techniques used to secure data and information which is stored in clouds from being attacked by DDoS. In [9] detection of DDoS attacks in cloud computing simulation was done by using K-means , decision tree and naïve Bayes techniques. The best detection accuracy was taken from decision tree but authors in [10] showed that the best accuracy was taken from SVM model . In [11] also, about five classifier algorithms were used to detect DDoS attack in Internet of Things (IoT) networks all of these classification algorithms showed accuracy higher than 99% and this great accuracy encourage researchers to resume search in this field . neural network (NN) technique were used in [12] and big data set was used to train the neural network it was great but the authors stated that sometimes the captured packets showed unexpected features that the model did not learn it before. Also, ANN was used in [13] to detect and classify DDoS traffic .this model was able to classify 3 types of attack but with different accuracies because authors extracted about only five features from the network traffic to be trained by the model and the number of extracted features were little. Survey was done [14] on shortages, advantages and effective factors of the ML techniques that could detect DDoS attacks and this research showed that there was no technique – from tested techniques – could overpass the other techniques but the authors didn't illustrate the extracted features from TCP header or ICMP header that all techniques used it for learning. Authors in [15] presented comparison between three different types SVM, KNN and multilayer perceptron (MLP) and the accuracy was above 98% in all used models but the models were fed with obsolete data sets and these data sets contain too much features . Another authors applied ML classification algorithms but in software defined network (SDN) environment [16] and they stated an important point that any classifier system give a better accuracy on offline training data set than on live traffic .

III. System overview

Any satellite needs to be controlled after launching it so, ground control station is needed for controlling and it is named Mission Control Center (MCC). MCC network must be secured from any attacks specially DDoS attacks. MCC network was shown in "Fig.1".

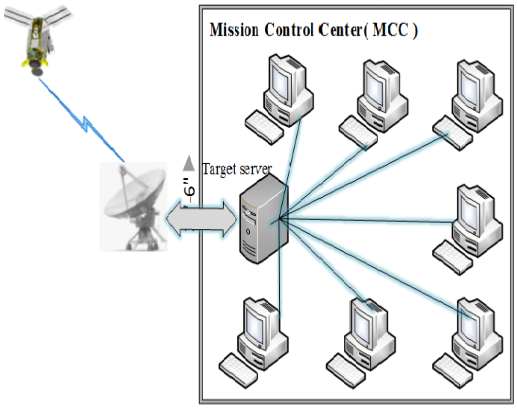
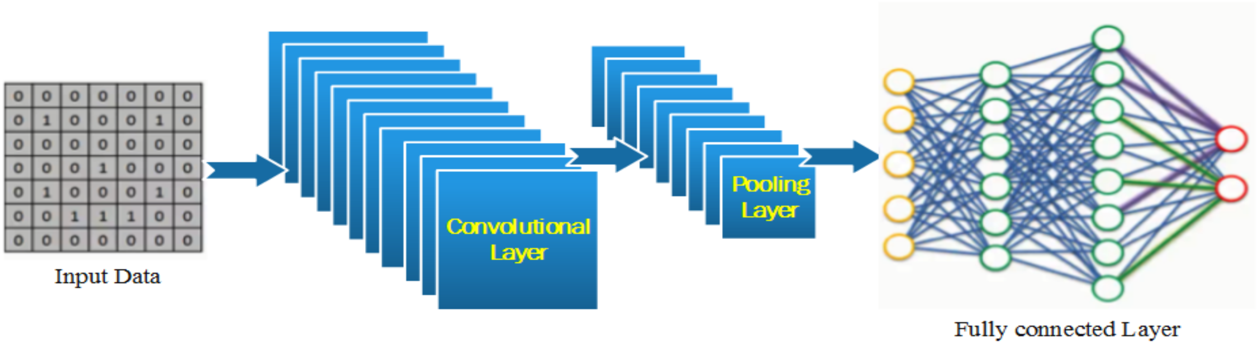


Fig. 1. MCC network



0	0	0	0	0	0	0
0	1	0	0	0	1	0
0	0	0	0	0	0	0
0	0	0	1	0	0	0
0	1	0	0	0	1	0
0	0	1	1	1	0	0
0	0	0	0	0	0	0

Fig. 2. CNN architecture

The target server simulated the spacecraft telemetry and all MCC devices received this telemetry through illustrated network. These assumptions according to [17] TCP and HTTP Flood DDoS Attack was launched at certain time . The attack started with the script, which installed previously on the network devices to attack the target server and make it unavailable to legitimate clients. In this paper, five classification algorithms were used to differentiate between malicious traffic from the normal: NN, CNN, SVM, D-tree and K-NN .As far as the authors knowledge it will be the first time to use CNN separately in classification and detection of DDoS attack.CNN was described in details later. About the datasets which were used to train all classifiers, two datasets were used one was captured from simulated MCC network and the other one downloaded offline from [18] .

Convolutional Neural Network:

Deep learning is a form of machine learning and CNN is a type of deep neural network. CNN has proven to be effective in many various studies and applications specifically in image classification field. Any CNN algorithm simply shown in “Fig.2”, it consists of multiples layers: input layer, convolutional layers, pooling layers, fully connected layer and output layer, the deepness of the CNN dependence on the number of layers used, the more layers used the more deepness we have. The explanation of these layers will be stated in detail in the next section. The classification process stages, which introduced in paper, was shown in “Fig.3” and described in the following paragraph:

1-Dataset collection stage: as mentioned before 2 datasets were used to train the models: a- online dataset which was captured by using Wireshark sniffing program, the traffic was captured normally and during DDoS attack then these traffics exported to excel file and it was known by dataset1. b- Predefined offline dataset -NSL-KDD dataset- [18] which is called DDoS attack dataset. These datasets were fed to the classification models. Certain parameters were extracted as follow: the extracted 8 parameters from dataset one are Time of capturing, time difference between the captured packet and the previous packet, source address, destination address, source port, destination port, protocol and TCP flag and represented as 8 columns and in case of proposed CNN algorithm each row converted to matrix 3*3 to be considered as 2D image. So, padding was used to complete the matrix elements padding was only one column. In dataset two the parameters were 41, matrix was 6*7 and padding was one.

2-Feature extraction stage: it is embedded within the convolution layers via each layer’s filters, such that each filter parameters shall be learned and optimized through the backpropagation process.

3-Classification process stage: the model was trained in this stage. Keras library as a backend for Tenser-flow library -which designed by Google and has excellent reputation in the field of deep-learning – in Python was used to build and train the deep learning model then make the classification process.

4-Comparison Stage: the results from CNN were compared with the results from other classifies.

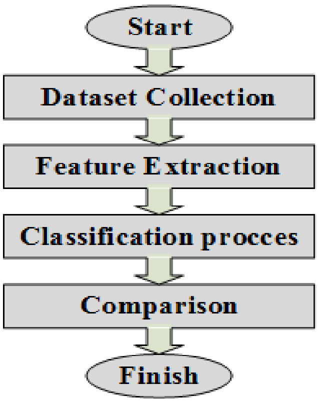


Fig. 3. CNN Stages

CNN layers of the presented algorithm were shown in “Fig.4”. It consists of input layer, (convolutional, activation function, pooling, fully connected) layers and output layer. Convolutional and activation function layers extracted the features from the data that coming from input layer using some filters based on certain activation function.

Pooling layer was responsible for reduction of the matrix size by using one of the following techniques: max pooling or average pooling to increase the speed of learning process and prevent overfitting problem.

Fully connected layer received the data from the final pooling layer after arranging it in 1D array then produce 1D array which represented the classes (normal, DDoS attack).

The summary of the presented CNN algorithm, it contains 3 stages the first stage consists of input layer, 2 convolutional layers then the output from these layers is fed to pooling layer.

Second stage consists of the same previous layers except input layer and the third stage consists of fully connected network and output layer.

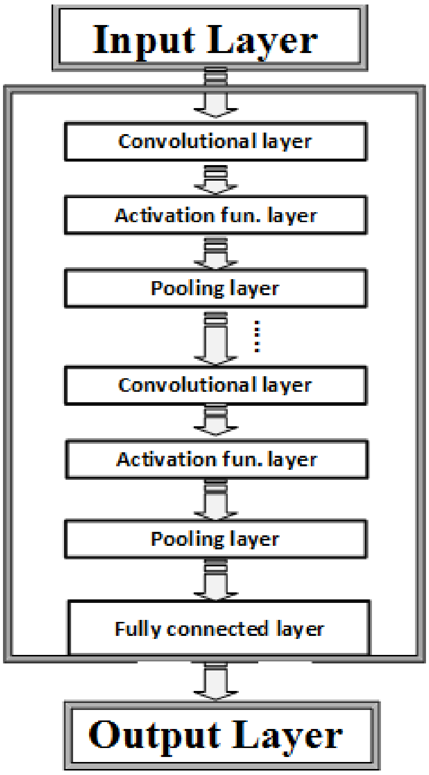


Fig. 4. Proposed CNN layers.

IV. Analysis and Results

Each dataset contains hybrid of normal and malicious traffic with different number of samples as shown in Table.I

TABLE I. DATASETS DESCRIPTION

No.	No. of samples	Notes
Dataset-1	28311 sample	Simulated network traffic
Dataset-2	125973 sample	NSL-KDD – offline data -

We said before that dataset-1 data were captured by Wireshark sniffer and saved in .Pcap format then exported to .CSV format. Dataset-2 was downloaded as a text file also converted to csv file. CNN model and all other classifiers was fed by the exported csv files. CNN model divided the input samples to train data and test data using Adadelta optimizer, test data = 0.2 of the trained data. Relu function was used as an activation function for the convolutional and the fully connected layers and the softmax was used for output layer. After training the model for 30 epochs with first dataset .The accuracy of the model was 99% and the results of CNN model were shown in “Fig.5”, “Fig.6”, and Table II explains in detail the output from each layer used in the model.

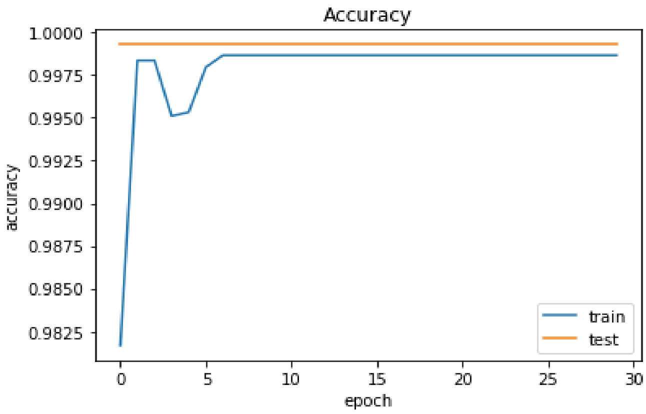


Fig. 5. CNN accuracy for dataset-1

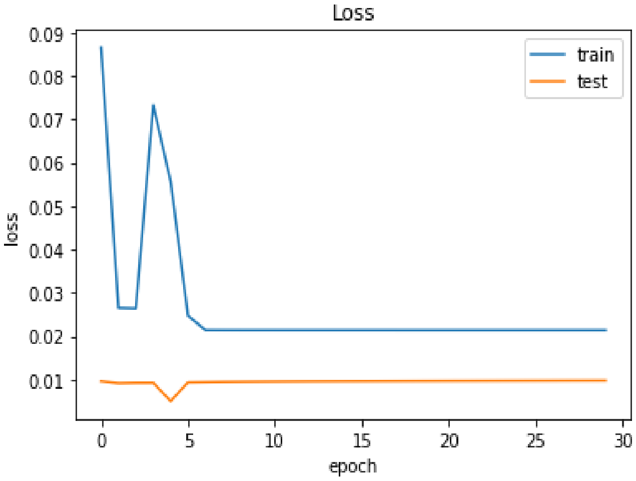


Fig. 6. CNN loss for dataset-1

TABLE II. CNN SUMMARY

Layer (type)	Output Shape	Param #
conv2d_1 (Conv2D)	(None, 32, 3, 3)	320
activation_1 (Activation)	(None, 32, 3, 3)	0
conv2d_2 (Conv2D)	(None, 32, 3, 3)	9248
activation_2 (Activation)	(None, 32, 3, 3)	0
max_pooling2d_1 (MaxPooling2)	(None, 32, 2, 2)	0
conv2d_3 (Conv2D)	(None, 64, 2, 2)	18496
activation_3 (Activation)	(None, 64, 2, 2)	0
conv2d_4 (Conv2D)	(None, 64, 2, 2)	36928
activation_4 (Activation)	(None, 64, 2, 2)	0
max_pooling2d_2 (MaxPooling2)	(None, 64, 1, 1)	0
flatten_1 (Flatten)	(None, 64)	0
dense_1 (Dense)	(None, 64)	4160
activation_5 (Activation)	(None, 64)	0
dense_2 (Dense)	(None, 2)	130
activation_6 (Activation)	(None, 2)	0

And with the second dataset the results show that the accuracy was 99% as in "Fig.7", and "Fig.8" shows the loss. Summary of results were shown in Table III, which shows that the accuracy was above 99% for the two datasets.

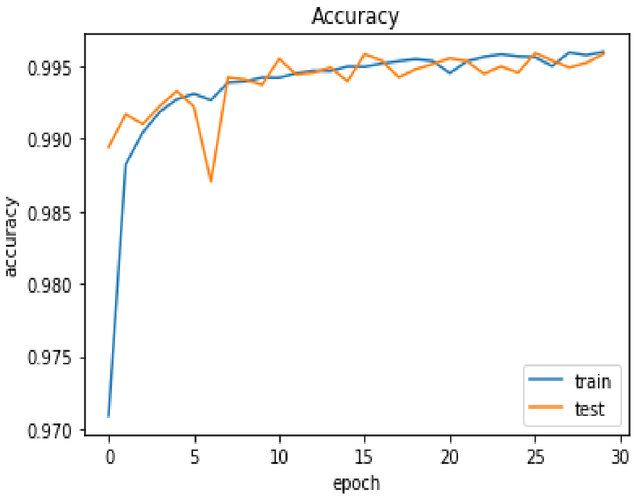


Fig. 7. CNN accuracy for dataset2

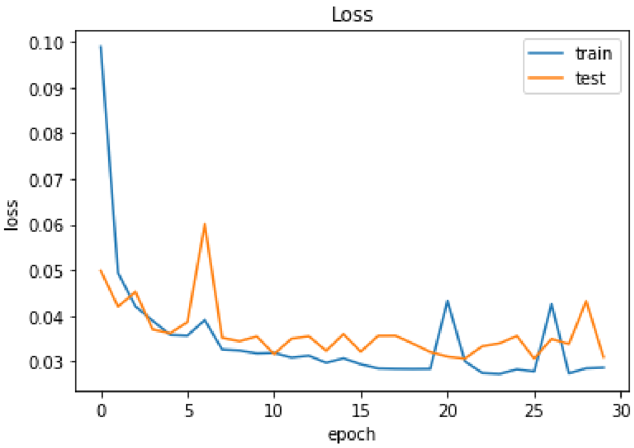


Fig. 8. CNN loss for dataset-2

TABLE III. CNN RESULTS SUMMARY

	Accuracy	Loss
Dataset-1	0.9933	0.0067
Dataset-2	0.9924	0.0076

The results from other classifiers- Dtree, SVM, KNN and NN- were shown in "Fig.9", "Fig.10" and Table IV using the same datasets. As shown from all previous results the presented CNN algorithm could classify and detect DDoS attacks with better accuracy than other used classification algorithms.

TABLE IV. ACCURACY OF OTHER CLASSIFIERS

Technique	Dataset-1	Dataset-2
D-tree	0.94995	0.92992
SVM	0.96362	0.94026
KNN	0.93965	0.92755
NN	0.98028	0.97922

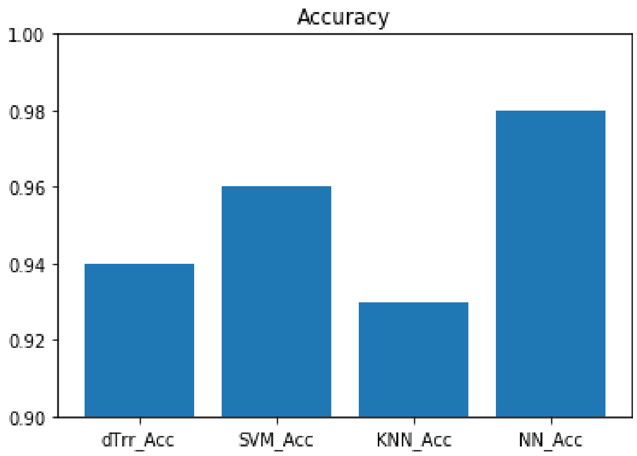


Fig. 9. Accuracy of other classifiers for dataset-1

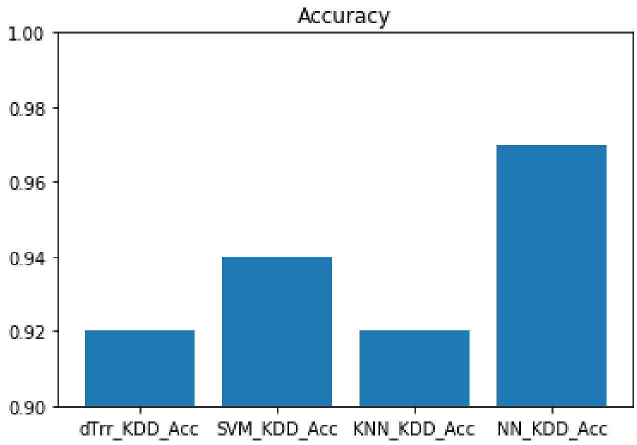


Fig. 10. Accuracy of other classifiers for dataset-2

V. CONCLUSION

Now Distributed Denial of Service is considered one of the most serious and widespread threats that faced by those responsible for securing networks. In this paper, five different classification algorithms were proposed and implemented to detect and classify DDoS attack. All models are built and trained by using two different datasets. Convolutional Neural Network (CNN) is commonly used in image processing and classification field. CNN is introduced to classify normal traffic from DDoS attack. According to analysis and results, we found that CNN performed better than other classifiers with accuracy of 99 %.

For the future work, we are planning to build a new model to block or mitigate DDoS attack based on the output from CNN classification algorithm used in this paper.

REFERENCES

[1] B. Nagpal, P. Sharma, N. Chauhan, and A. Panesar, "DDoS tools: Classification, analysis and comparison," in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 342-346, 2015.

[2] Y. S. Abu-Mostafa, M. Magdon-Ismail, and H.-T. Lin, *Learning from data*. AMLBook New York, NY, USA:, 2012.

[3] B. Zhang, T. Zhang, and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 1276-1280, 2017.

[4] A. Alsirhani, S. Sampalli, and P. Bodorik, *DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark* (2019 IEEE Transactions on Network and Service Management). IEEE, pp. 1932-4537, 2019.

[5] A. Yudhana, I. Riadi, F. J. I. J. O. A. C. S. Ridho, and APPLICATIONS, "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics," vol. 9, no. 11, pp. 177-183, 2018.

[6] D. Peraković, M. Periša, I. Cvitić, and S. J. T. J. Husnjak, "Model for detection and classification of DDoS traffic based on artificial neural network," vol. 9, no. 1, p. 26, 2017.

[7] T. Thapngam, S. Yu, W. Zhou, S. K. J. P.-t.-p. n. Makki, and applications, "Distributed Denial of Service (DDoS) detection by traffic pattern analysis," vol. 7, no. 4, pp. 346-358, 2014.

[8] A. Sahi, D. Lai, Y. Li, and M. J. I. A. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," vol. 5, pp. 6036-6048, 2017.

[9] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, pp. 1-7, 2017.

[10] A. R. Wani, Q. Rana, U. Saxena, and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pp. 870-875, 2019.

[11] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, pp. 29-35, 2018.

[12] C.-J. Hsieh and T.-Y. Chan, "Detection DDoS attacks based on neural-network using Apache Spark," in *2016 International Conference on Applied System Innovation (ICASI)*, pp. 1-4, 2016.

[13] D. Peraković, M. Periša, I. Cvitić, and S. Husnjak, "Artificial neuron network implementation in detection and classification of DDoS traffic," in *2016 24th Telecommunications Forum (TELFOR)*, pp. 1-4, 2016.

[14] X. Liang and T. Znati, "An empirical study of intelligent approaches to DDoS detection in large scale networks," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 821-827, 2019.

[15] T. Roempluk and O. Surinta, "A Machine Learning Approach for Detecting Distributed Denial of Service Attacks," in *2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON)*, pp. 146-149, 2019.

[16] J. Bakker, B. Ng, W. K. Seah, and A. Pekar, "Traffic Classification with Machine Learning in a Live Network," in *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 488-493, 2019.

[17] A.Ramzy, E.Abdelwanees, and M.Hussien, "TCP and HTTP Flood DDOS Attack Analysis and Detection for space ground Network," , Unpublished 2019.

[18] NSL-KDD "https://iscxdownloads.cs.unb.ca/iscxdownloads/CIC-IDS-2017/#CI-IDS-2017," ed, 2017.