EasyChair Preprint

№ 8573

DDoS Attack Detection on SDN with Conv1D and LSTM

Alperen Örsdemir, Hamidullah Nazari and Devrim Akgün

August 3, 2022

3rd International Conference on Applied Engineering and Natural Sciences

https://www.icaens.com/

July 20-23, 2022, Konya, Turkey

DDoS Attack Detection on SDN with Conv1D and LSTM

Alperen Orsdemir[1*], Hamidullah Nazari[2] and Devrim Akgun[3]

[1]*Computer Engineering Department/Faculty of Computer and Information Sciences, Sakarya University, Turkey*
[2]*Computer and Information Engineering Department/ Institute of Natural Sciences, Sakarya University, Turkey*
[3]*Software Engineering Department/ Faculty of Computer and Information Sciences, Sakarya University, Turkey*

[*]*(alporsdemir@gmail.com) Email of the corresponding author*

***Abstract* –** Especially in the last decade, many companies have been digitalizing their architectures and using various kinds of software and hardware that reside in databases or virtual hosts within Local Area Networks. With the latest dynamic technologies, network data flow is monitored and controlled swiftly and in detail with SDN (Software Defined Networks). SDN packet traffic has a structure that can be easily projected compared to traditional networks. It provides broader control possibilities on the network and can be controlled faster. In this research, an SDN is used for identifying or increasing the quality of the identification of various network data and summarizes for further investigation. It is easier to record data flow from networks, analyze the network, and detect multiple types of malware, DoS, and DDoS (Distributed Denial of Services); SDN software is used to categorize network data for security and higher performance. Deep Learning methods have efficiently classified different types by their features. In this proposed model with CNN (Convolutional Neural Network), LSTM (Long Short-Term Memory), and DNN (Deep Neural Networks), the performance results were found to be satisfactory in categorizing malware or DDoS within healthy dataflow. Among the examined networks, the best performance has been obtained using CNN based model.

Keywords – Software Defined Network, DDoS, Deep Learning, Attack Detection, Convolutional Neural Networks

I. INTRODUCTION

SDN is different from traditional networks in controlling the network, handling data flow, and organizing it. SDN is way more manageable with a centralized system of software. Traditional networks are static and way harder to implement, configure, and run overall. SDN standardizes the functionality within the network. It is getting more complex to handle, analyze, and keep the network secure with increasing amounts of data flow in Local Area Networks. [1]. Thus, rather than standard physical networks, SDN makes examining portions of data more accessible [2],[3]. The centralized data flow structure in SDN allows researchers to handle and react against malware such as DDoS, Spoofing, and jamming, which harm institutions' digital and physical structures [4], [5]. Intelligent home systems and devices connected to each other are being controlled and secured with Software Defined Networking systems [6],[7]. Management of QoS (Quality of Services) is easier and more efficient with SDN structures [8]. The most common services of SDN are real-time inspection of packets and cognition of software. SDN software is most commonly used for monitoring traffic data flow for controllers to view usual processes and unexpected incidents that may occur in real-time. Research about network datasets is significantly crucial since processes that are being handled for services such as QoS, security of the network, incident response, and malware detection are being structured with models that are the results of SDN dataset research. Possibilities of dynamic rulemaking and forming in the network are supportive for researchers [9].

DDoS attacks are unparalleled in that most services are being attacked globally by making servers and structures out of service. When a DDoS attack occurs, services or clouds cannot be accessed. Tiring with overwhelmingly many requests, the controller cannot respond to new requests [10],[11] SDN analyzes network traffic possible with central control and observability on broad scales in the network [12].

Reaction and detection of DDoS attacks are being handled more simply. Neural network models present the ability to detect similar packets with harmful purposes. Researchers have been given a more convenient solution to respond to these incidents. Methods of neural networks offer a more productive solution to prevent DDoS attacks with visionary models.

II. Proposed Models

In this study, Deep Learning methods are used for DDoS detection in SDN with a comparison of different deep learning models such as DNN (Deep Neural Networks), CNN (Convolutional Neural Networks), and LSTM (Long Short Term Memory).

A. *DNN Model*

Deep neural networks are mathematical models inspired by the human brain. It generally consists of 3 layers, i.e., input, hidden, and output. These layers are interconnected with neurons, which form the basis of artificial neural networks, as shown in Figure 1. Each neuron takes input from several other neurons, multiplies them by their assigned weights, adds up, and transfers the sum to one or more neurons.

Thus, learning is accomplished. The layers created for training the DNN model consist of four dense layers with 32, 64, 128, and 128 nodes, respectively, two batch normalization layers, two dropout layers, and finally, an output layer using the sigmoid activation function for binary classification.

B. *CNN Model*

One of the most used models due to the achievements of the deep learning field is the CNN algorithm. CNN produces successful results in many fields, such as image and video classification, recommendation systems, natural language processing, and image analysis. CNN is one of the most preferred models in text classification and analysis. CNN consists of 1D convolution, pooling, flatten, and fully connected layers. CNN proposed model as Figure 2 for SDN classification was performed using two Conv1d with 16 and 32 filters, two BatchNormalization, two MaxPooling1D, one Flatten and Dense layers, and an output layer with a sigmoid activation function.

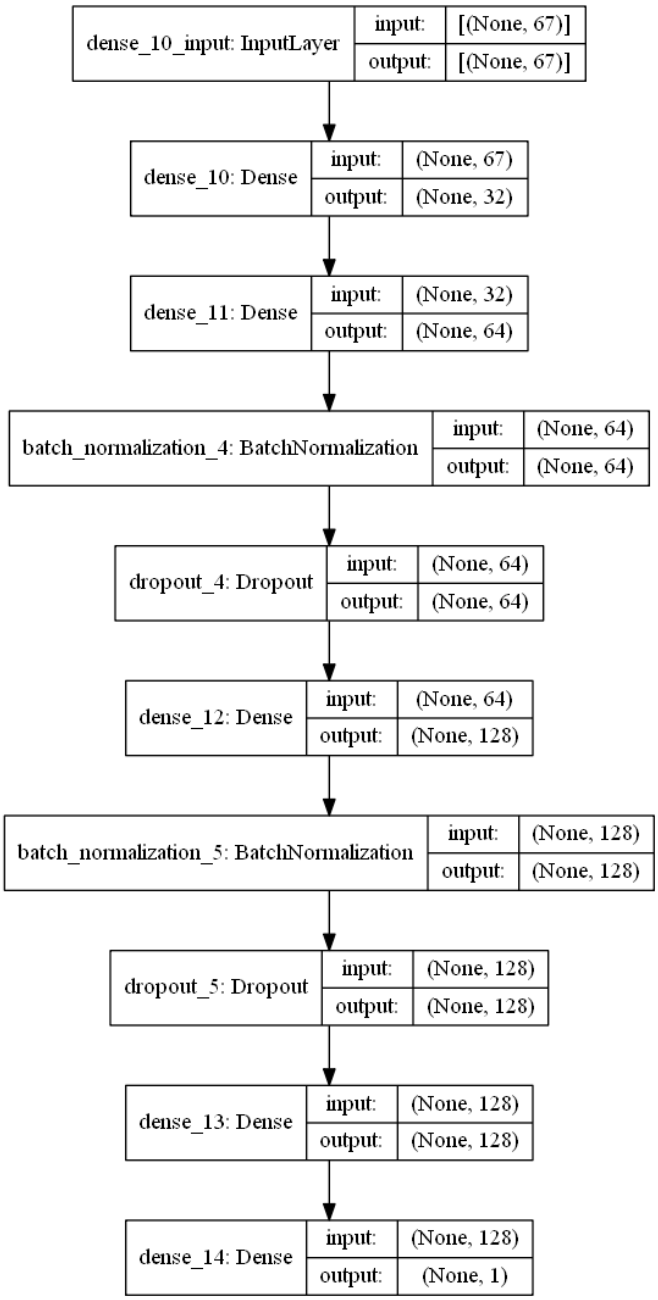

Fig. 1 DNN Based Model

C. *LSTM Model*

The long-short-term memory model, or LSTM, is a particular type of recurrent RNN network. Instead of a single neural network like a standard RNN, it consists of four interactive stages with a unique communication method. The first Forget Gate stage decides what information to keep or forget. That is, if the incoming input is unimportant, it is forgotten. If it is important, it is transferred to the next stage. The second input stage is used to update the cell

state. By applying the sigmoid function to the entered data, it is decided which information to keep; it is reduced, and the two results are multiplied. In the third cell state stage, the result from the Forget Gate is multiplied by the output of the previous layer, and then the glean value from the Input Gate is added. The fourth Output Gate decides the value to be sent to the next layer for prediction [13]. The SDN dataset is trained using an input layer, an LSTM with 64 filters, one dropout, flatten, fully connected layers (two Dense with 64 and 128 nodes), and an output layer shown in Figure 3.

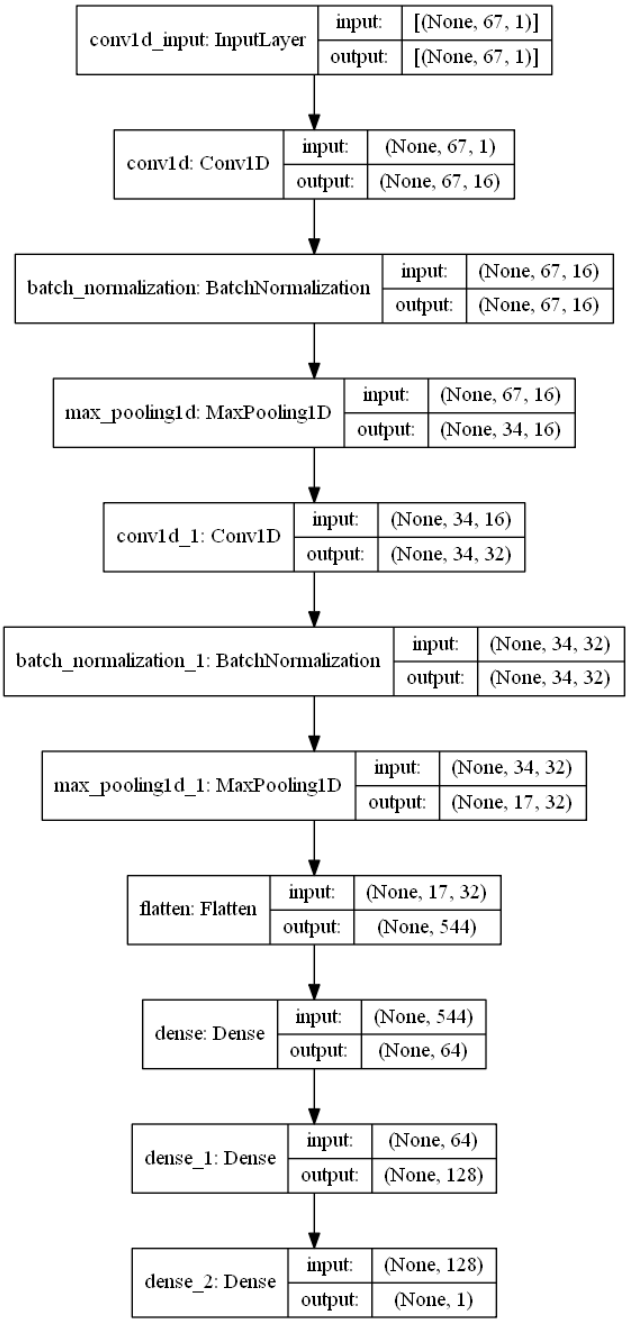

Fig. 2 CNN Based Model

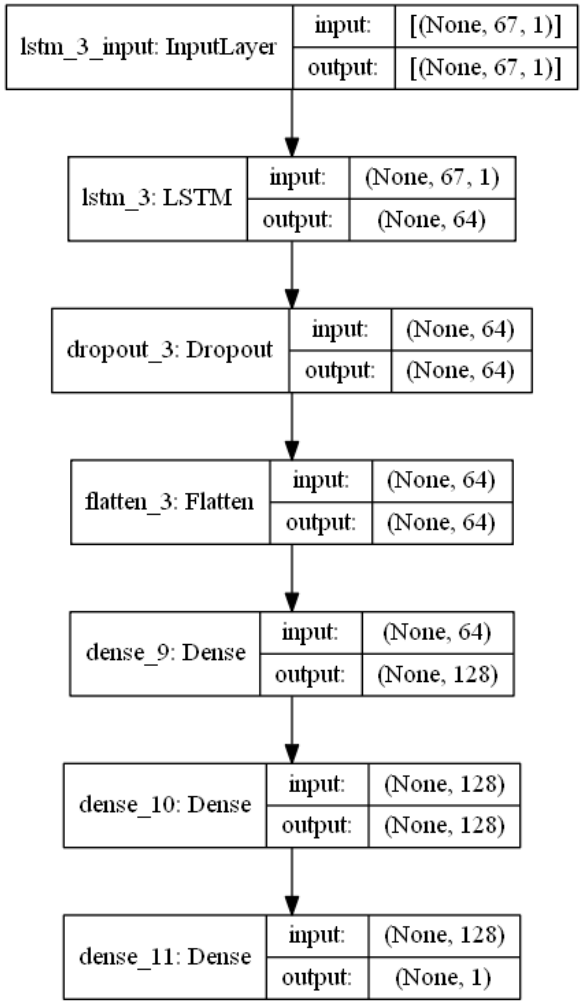

Fig. 3 LSTM Based Model

III. RESULTS

Deep Learning models have been realized with the Python programming language and the Tensorflow-Keras API. The public DDOS attack SDN Dataset [14] has been used for models to train. Dataset has been separated into three parts, train, test, and validation. Percentages are %70 train, %15 validation, and %15 test for the separations. Different feature engineering methods and pre-processing have been applied to the data before training. The input of models is defined as 68×1 array. DNN, CNN, and LSTM models have been trained with additional layers. The example values of train, validation accuracy, and loss values of the CNN model by epoch count within the proposed model with the best results have been shown in Figure 3. The CNN model has proven to be the most successful model among the three in this research.

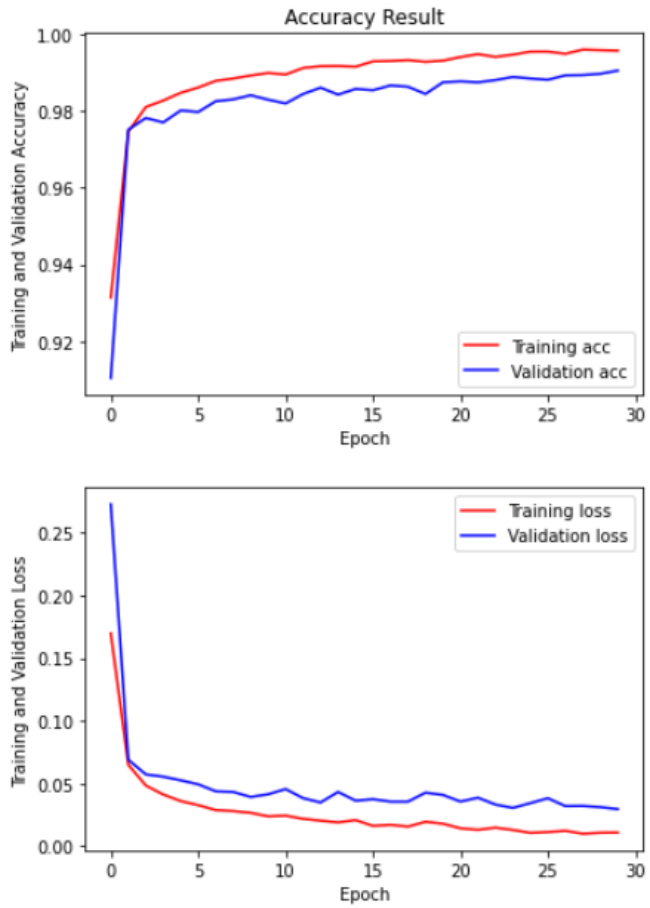

Fig 3. Training and validation accuracies and losses functions of the CNN proposed model

The model results show the Accuracy value as %99 and the Validation value as %98. For a better understanding of results, the confusion matrix of the proposed model is shown in Figure 4. Of 8130 DDoS's overall, 8031 of them has predicted successfully, and 99 DDoS packets have been missed. Similarly, with No_DdoS packets, 6998 have successfully been predicted, while 74 have been missed.

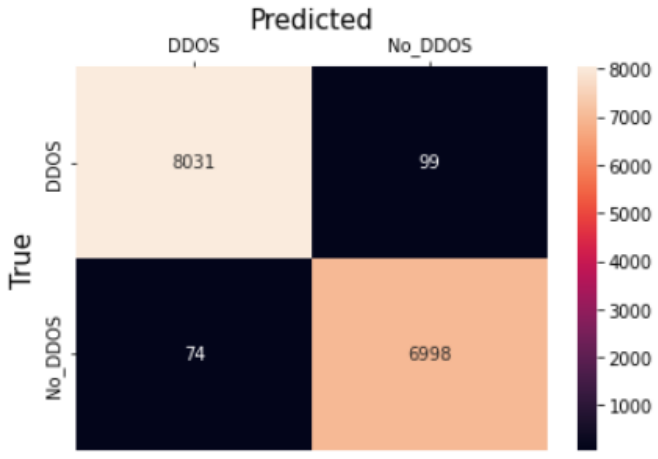

Fig 4. Confusion of CNN's proposed model

Table 1. Performance Measures.

Proposed Model	Precision	Recall	F1-Score
DNN	0.96	0.94	0.95
LSTM	0.97	0.95	0.96
CNN	0.99	0.99	0.99

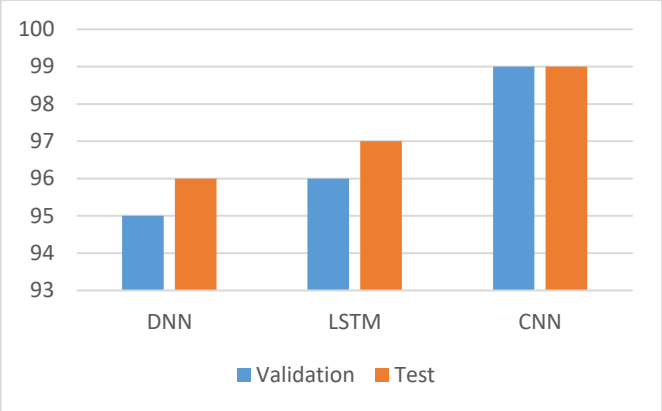

Fig 5. Comparison of validation and test accuracy values for the examined models

The proposed model's precision, recall, and F1-score metrics are shown in Table 1 by using the True and False values [15]. Figure 5 shows the test and validation accuracy comparisons of examined models where CNN performs the best classification accuracy.

IV. CONCLUSION

Deep Learning methods perform incomparably well among the other techniques with SDN. In this research, DNN, LSTM, and CNN deep learning models have been trained using DDOS attack SDN dataset. Even if the model hasn't been used in a real environment rather than in the dataset, we obtained good scores in the percentage of detecting DDoS attacks. For future studies, we plan further research into detecting malware and DDoS with higher performance.

REFERENCES

[1] M. M. Raikar, S. M. Meena, M. M. Mulla, N. S. Shetti, and M. Karanandi, "Data Traffic Classification in Software Defined Networks (SDN) using supervised-learning," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 2750–2759, 2020, doi: 10.1016/j.procs.2020.04.299.

[2] C. Li *et al.*, "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN," *Int. J. Commun. Syst.*, vol. 31, no. 5, pp. 1–15, 2018, doi: 10.1002/dac.3497.

[3] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey," *IEEE Access*, vol. 7, pp. 107346–107379, 2019, doi:

10.1109/ACCESS.2019.2932422.

[4] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft Comput.*, 2022, doi: 10.1007/s00500-021-06608-1.

[5] Q. Niyaz, W. Sun, and A. Y. Javaid, "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," *ICST Trans. Secur. Saf.*, vol. 4, no. 12, p. 153515, 2017, doi: 10.4108/eai.28-12-2017.153515.

[6] D. K. Dake, J. D. Gadze, G. S. Klogo, and H. Nunoo-Mensah, "Multi-Agent Reinforcement Learning Framework in SDN-IoT for Transient Load Detection and Prevention," *Technologies*, vol. 9, no. 3, p. 44, 2021, doi: 10.3390/technologies9030044.

[7] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert, and C. Kemp, "User behavior anomaly detection for application layer ddos attacks," *Proc. - 2017 IEEE Int. Conf. Inf. Reuse Integr. IRI 2017*, vol. 2017-January, pp. 154–161, 2017, doi: 10.1109/IRI.2017.44.

[8] P. Wang, F. Ye, X. Chen, and Y. Qian, "Datanet: Deep learning based encrypted network traffic classification in SDN home gateway," *IEEE Access*, vol. 6, pp. 55380–55391, 2018, doi: 10.1109/ACCESS.2018.2872430.

[9] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," *SDN4FNS 2013 - 2013 Work. Softw. Defin. Networks Futur. Networks Serv.*, 2013, doi: 10.1109/SDN4FNS.2013.6702553.

[10] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," *2015 Int. Conf. Comput. Netw. Commun. ICNC 2015*, pp. 77–81, 2015, doi: 10.1109/ICCNC.2015.7069319.

[11] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 602–622, 2016, doi: 10.1109/COMST.2015.2487361.

[12] S. Sezer *et al.*, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, pp. 36–43, 2013, doi: 10.1109/MCOM.2013.6553676.

[13] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997, doi: 10.1162/neco.1997.9.8.1735.

[14] D. Ahuja, Nisha; Singal, Gaurav; Mukhopadhyay, "DDOS attack SDN Dataset," https://data.mendeley.com/datasets/jxpfjc64kr/1. doi: 10.17632/jxpfjc64kr.1.

[15] H. Nazari and D. Akgun, "A Deep learning model for image retargetting level detection," *4th Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2020 - Proc.*, no. 3, pp. 2020–2023, 2020, doi: 10.1109/ISMSIT50672.2020.9254845.

[16] C. Zhang, P. Patras, and H. Haddadi, "Deep Learning in Mobile and Wireless Networking: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2224–2287, 2019, doi: 10.1109/COMST.2019.2904897.

[17] O. Hannache and M. C. Batouche, "Neural network-based approach for detection and mitigation of DDoS attacks in SDN environments," *Int. J. Inf. Secur. Priv.*, vol. 14, no. 3, pp. 50–71, 2020, doi: 10.4018/IJISP.2020070104.

[18] A. Banitalebi Dehkordi, M. R. Soltanaghaei, and F. Z. Boroujeni, *The DDoS attacks detection through machine learning and statistical methods in SDN*, vol. 77, no. 3. Springer US, 2021. doi: 10.1007/s11227-020-03323-w.

[19] S. Hizal, U. Cavusoglu, and D. Akgun, "A new Deep Learning Based Intrusion Detection System for Cloud Security," *HORA 2021 - 3rd Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc.*, 2021, doi: 10.1109/HORA52670.2021.9461285.

[20] S. Askar, "Deep learning Utilization in SDN Networks: A Review," *Available SSRN 3962994*, pp. 174–182, 2021, doi: 10.5281/zenodo.5222205.