Detection of TCP, UDP and ICMP DDOS attacks in SDN Using Machine Learning approach

R. Anusuya[1],
Professor, Department of CSE,
Modern Institute of technology and research Centre,
Alwar, Rajasthan. E-mail: anusuccess@yahoo.com

M. Ramkumar Prabhu[2]
Professor, Department of ECE,
PERI Institute of Technology, Chennai.
E-mail: ramkumarprabhu@gmail.com

Ch. Prathima[3]
Assistant Professor, School of Computing,
Mohan Babu University, Tirupati.
E-mail: Prathima.ch@vidyanikethan.edu

J. R. Arun Kumar[4]
Professor, Department of CSE,
Modern Institute of technology and research Centre,
Alwar, Rajasthan. E-mail: arunnote@yahoo.com

Abstract: Software Defined Networking (SDN) is an architecture for the network to control centrally through programmed software applications. SDN enables the programming behaviour of the network centrally over software programs with the help of open Application interfaces. We can change the parameters of network connections in a dynamic manner. In conventional network, it is impossible to change the settings in a dynamic way, as it is a fixed connection. In SDN, the Control plane is controlled by software is at the center which links the application layer and infrastructure layer. Software-Defined Networking (SDN) has proved its efficiency in countering attacks by providing network surveillance and online configuration of the network. DDoS attack is a malicious attack in which the attacker floods the target server from various sources. This project uses SDN intrusion dataset for training. This project focuses on the implementation of a compatible way for finding the DDoS detriment in SDN employing multiple Machine Learning (ML) approaches.

Keywords: DDoS attack, Machine Learning, Software-Defined Networking.

I. INTRODUCTION

Software Defined Networking (SDN) is widely used interconnected criterion that is dynamic, less cost, extensible, by preparing it better suited to various devices or different network projects. The network or interconnection control and advancing activities are segregated in this architecture, by permitting network control straightforwardly programmable and the framework components are preoccupied for applications and organization administrations. It is critical to construct a Intrusion Detection System (IDS) based on network that detect DDoS detriment using information from network traffic flows (SDN). In SDN, the control planes (CP) are separated by network devices. This technology different from traditional network design in its operation. Because the traditional network is a fixed link, it is not possible to adjust dynamically.

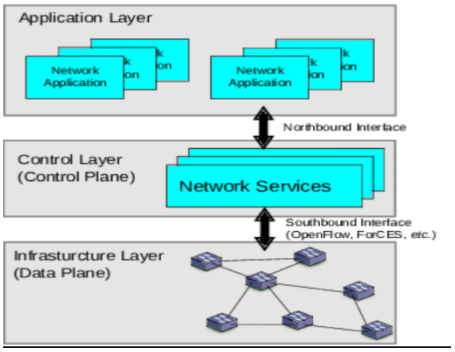


Fig 1: Architecture of SDN.

In SDN, we can modify the specifications of network connections on the fly. On the basis of controller's decisions, the data plane transports network traffic. The control plane determines traffic flow by enumerate routing tables. The application plane controls other applications such like load balancers, firewall, & Quality of Service (QoS) apps. Creating an Intrusion Detection System (IDS) is based on a network and utilizes modern networking technologies like SDN is of utmost importance. This

system should be able to find DDoS attacks by analysing data from network traffic flows that are managed by SDN. DDoS attacks are dangerous attacks from various OSI layers. DDoS attacks continue to cause countless issues in today's network infrastructures. These are usually high-volume and expensive attacks. Artificial intelligence approaches such as machine learning can, however, identify them. Control programmes in a logically centralized controller will manage numerous routers across the network. DDoS attacks have grown in frequency and severity over time, as well as in sophistication. The modularity aspect allows us to adapt and improve any component of the architecture separately, such as the flow collector, and detection.

Using artificial intelligence methodologies, this study provides a scalable and extensible SDN-based architecture for detecting DDoS attacks. The modularity aspect allows us to improve each component separately, namely pre-processing, the flow collector, detection, and flow management modules.

This approach allows experimenting with alternatives ML detection techniques to counter different DDoS attacks. And also, this research looked into the most common and harmful transport layer to do damage by DDoS, UDP Flood and SYN Flood. Because a large quantity of traffic passes through the controller in the SDN control layer, a good security system is required to analyse and identify suspicious traffic. Furthermore, the approaches KNN, RF, DT, and SVM were successful for various sorts of attacks.

II. RELATED WORKS

S.No	AUTHOR NAME	TITLE	PROPOSED SYSTEM	LIMITATIONS
1.	Mario Lemes Proença, Jr. (proenca@ uel.br)	Long Short Term Memory and Fuzzy Logic for finding Anomaly and Mitigation in Software-Defined Network.	The system proposed in this paper aims to characterise network traffic, detect DDoS attacks, and mitigate Port scan in an SDN environment.	However, this work was subjected to few high-volume damages. Up-to-date datasets are not used.
2.	N. N. Tuan	A DDoS detriment mitigation scheme in ISP networks using ML by SDN	This work proposed a DDoS attack mitigation strategy for TCP-SYN and ICMP flood attacks in SDN-based (ISP) networks using an ML approach, namely, K_Nearest_Neighbor and X_G_Boost.	The datasets used in this paper are not up to date and explored only few types of DDoS attacks.

3.	T. V. Phan	Q-MIND: Loosing stealthy DoS detriment in SDN with a machine-learning based defense framework	This research published Q-MIND, a machine ML defence application, to find and mitigate DoS damage in SDN.	This work explored only few classification Methods and this work only detects whether attack is DDoS attack or not. This work does not explored types of DDoS attacks**.**
4.	M. Idhammad	Semi-supervised ML approach for finding DDoS	Writers presented an online ordered semi-supervised ML process in finding DDoS by network Entropy estimation, Co-clustering, Data Gain Ratio, and Extra-Trees algorithm.	This study did not use up-to-date datasets and a smaller number of methods are explored.
5.	X. Liang	A long short-term memory framework for finding DDoS detection	To address this paper a guided DDoS, find scheme by LSTM is published.	This work explored only slow rate DDoS attacks. Only explored a single classifier.
6.	Amit Praseed	DDoS detriment at the application layer: Problems and research perspectives for safeguarding web applications	DDoS detriment on the application or framework layer have begun. They make legitimate application layer requests, making existing defence mechanisms difficult to detect.	This paper presents a detailed explanation and classifications of application layer DDoS to help researchers better understand of attacks.
7.	M. Elsayed	A Deep-Learning Model for Detecting Network Attacks	The authors published DDoSNet, an intrusion detecting system against DDoS damage in SDN framework, in this paper.	This work does not focus on testing the proposed model's performance on other datasets.

III. PROPOSED SYSTEM

This section discusses about proposed work for finding of DDoS damage using ML approaches in SDN. The presented work makes uses machine learning techniques which are SVM, Decision tree, k Nearest Neighbours, Random Forest. The advantage of using this ML algorithms is their less complexity.

This work focuses on the following DDoS attack:

1) TCP-SYN FLOOD ATTACK: It is a type of DDoS attacks where intruder rapidly initialises a connection without finalizing it to web server. The server must use resources to wait for poorly opened connections, which might cause the system to become unresponsive to routine traffic.

2) UDP FLOOD ATTACK: It is a classification of DDoS damage (attack) where intruder attacks the ports of host with IP packets comprising User Datagram protocol packets.

3) ICMP FLOOD ATTACK: Usual method in which a DDOS attack occurs is when attacker floods the target device with ICMP echo requests, causing it to be overwhelmed.

A. MACHINE LEARNING:

The methodology employed in this study involves utilizing ML techniques to identify DDOS attacks in SDN. Dataset that will be used for both training and testing the algorithms is SDN DDOS. Prior to the analysis, essential pre-processing steps have been carried out on the dataset. Necessary pre-processing steps have been applied to the dataset.In the pre-processing process, Data cleaning, variable standardization and feature selection were performed. Preprocessed data has been splitted into trainee and testing sets to train and testing ML algorithms.

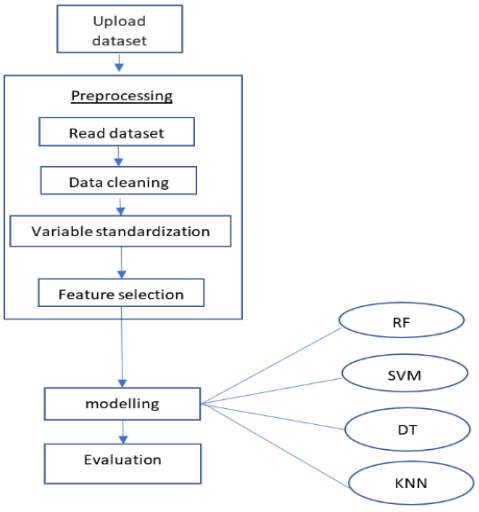


Fig 2: Illustration of machine learning process.

In Data cleaning process, all the Null values from dataset were identified and removed. In variable standardization process all the features with standard variation equals to 0 were removed from the dataset. In feature selection process, necessary has been extracted from the dataset. Then algorithms were trained using pre-processed data and evaluated based on performance metrics.

B. MODELLING MACHINE LEARNING ALGORITHMS:

The ML algorithms utilized in this study for the identification of DDoS attacks include Random Forest, SVM, DT, KNN.

SVM: SVM is supervised ML based process that is used in both classification and regression challenges. Important aspect of this algorithm is to classify input points by finding hyperplane in N-dimensional space.

KNN: This algorithm is used for both classification and regression issues. This algorithm assumes that similar objects are put into same category.

RANDOM FOREST: It is for classification and predicting issues. It constructs decision trees from heterogeneous data and classifies and predicts using the average of their votes.

DECISION TREE: It is a tool to solve classification and prediction problems**.** Internal nodes symbolise to test attribute, every branch symbolises a test outcome, and leaf nodes stores a class label**.**

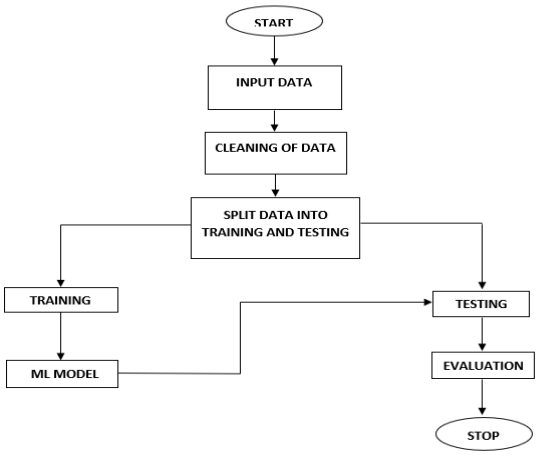


Fig 3: Block diagram for modelling ML algorithms.

Training and testing sets have been created from the pre-processed dataset. and training set was used for training machine learning and a model will be created from training. The model was tested with the testing set. From the results of testing, accuracies of machine learning algorithms were generated.

C. EXPERIMENTAL ANALYSIS:

The Efficiency of the ML algorithms used in the suggested system was assessed in a Mininet and Ryu controllers-based SDN test environment.

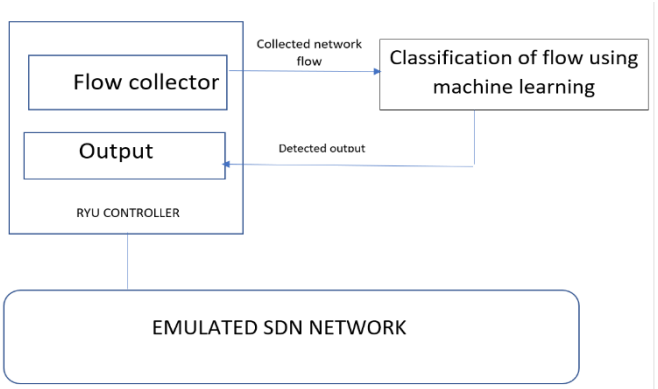


Fig 4: Architecture of SDN Testbed.

A simple SDN network consisting of 18 hosts, 6 switches and a controller has emulated using Mininet and Ryu controller. Mininet is a standard tool used to emulate SDN networks and Ryu controller is a python based programmable controller used in research works regarding SDN networks. Despite the fact that, in various virtual machines installed all of these applications, the proposed work only uses one physical computer to emulate the MNE and RYU controller. Following is how the proposed architecture works. Flow Collector is an application programme that runs in the controller. Network traffic flow is collected by flow collector and delivers the collected flow to a trained ML model, which detects if the flow represents an attack or normal traffic and presents the results to the controller.

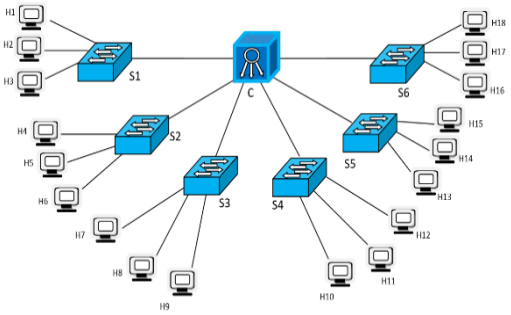


Fig 5: Emulated SDN network topology

A simple web server (SimpleHTTPServer) will be running on any of hosts and DDoS attacks will be performed on that webserver. To perform attacks a standard tool hping3 is used. Hping3 can be used to perform TCP-SYN, UDP, ICMP attacks. During DDoS attacks webserver is hosted on one host and attack will be generated from another host and one more host is employed to notice the reachability of web-server while attack in progress. Each trained ML algorithm is evaluated in SDN testbed in similar manner

IV. RESULT ANALYSIS

Performance of Machine Learning algorithms in the proposed work is analysed using recall, accuracy and f1-score. Accuracy describes the success of ML algorithm. The recall metric is employed to differentiate between true positives and false negatives as well as to identify true negatives. In addition, the F1-score is a calculation of the weighted mean between precision and recall.

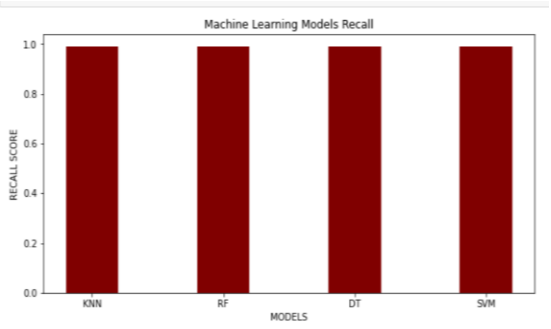
A. Accuracies of Machine Learning Models:

Machine learning models	ACCURACY of detection (%)
Decision Tree	99.95
Random Forest	99.99
KNN	97.99
SVM	66.07

Table 1: Accuracy of ML models.

B. Recall Comparison of Machine Learning Models:

All the ML models in the proposed work have achieved same recall value which is 99.99



S-switch

Fig 6: Recall comparison ML Models

F1-score comparison of Machine Learning Models:

All the ML models in the proposed work have achieved the same F1-score which is 99.99.

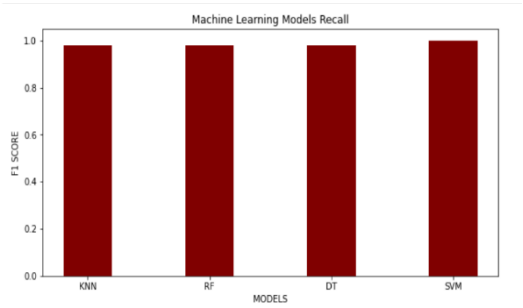


Fig 7: F1-score comparison of Machine learning models

V. CONCLUSION AND FUTURE WORK

DDoS attacks has become very sophisticated in latest time, as well as more enormous. This work we present a flexible solution using ML techniques for finding of DDoS attacks in SDN. Large Volumes of data is pre-processed and trained with ML algorithms, namely KNN, SVM, DT, and RF. These trained algorithms were evaluated in simulated SDN network. out of these algorithms Random Forest and Decision Tree algorithm has shown the best results. In future, the work will be focused on increasing the scalability of network and also the mitigation of attacks in SDN network. Thus, the Suggested system can be useful for identifing DDoS attacks in SDN.

REFERENCES

[1]. "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning" by NOE MARCELO YUNGAICELA-NAULA, CESAR VARGAS-ROSALES, (Senior Member, IEEE), AND JESUS ARTURO PEREZ-DIAZ. (Base Paper)

[2]. M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proenca, ''Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment,'' IEEE Access, vol. 8, pp. 83765–83781, 2020.

[3]. M. Idhammad, K. Afdel, and M. Belouch, ''Semi-supervised machine learning approach for DDoS detection,'' Appl. Intell., vol. 48, no. 10, pp. 3193–3208, 2018.

[4]. N. N. Tuan, P. H. Hung, N. D. Nghia, N. V. Tho, T. V. Phan, and N. H. Thanh, ''A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN,'' Electronics, vol. 9, no. 3, p. 413, Feb. 2020.

[5]. T. V. Phan, T. M. R. Gias, S. T. Islam, T. T. Huong, N. H. Thanh, and T. Bauschert, ''Q-MIND: Defeating stealthy DoS attacks in SDN with a machine-learning based defense framework,'' in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2019, pp. 1–6.

[6]. X. Liang and T. Znati, ''A long short-term memory enabled framework for DDoS detection,'' in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2019, pp. 1–6.

[7]. M. M. Salim, S. Rathore, and J. H. Park, ''Distributed denial of service attacks and its defenses in IoT: A survey,'' J. Supercomput., vol. 76, pp. 5320–5363, Jul. 2019.

[8]. K. Srinivasan, A. Mubarakali, A. S. Alqahtani, and A. D. Kumar, ''A survey on the impact of DDoS attacks in cloud computing: Prevention, detection and mitigation techniques,'' in Intelligent Communication Technologies and Virtual Mobile Networks. Cham, Switzerland: Springer, 2019, pp. 252–270.

[9]. D. Gurusamy, M. Deva Priya, B. Yibgeta, and A. Bekalu, ''DDoS risk in 5G enabled IoT and solutions,'' Int. J. Eng. Adv. Technol., vol. 8, no. 5, pp. 1574–1578, 2019.

[10]. Kaspersky. (2021). Kaspersky Q4 2020 DDoS Attacks Report. [Online]. Available: https://securelist.com/ddos-attacks-in-q4-2020/100650/

[11]. A. Praseed and P. S. Thilagam, ''DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications,'' IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661–685, 1st Quart., 2019.

[12]. J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, ''Security in SDN: A comprehensive survey,'' J. Netw. Comput. Appl., vol. 159, Jun. 2020, Art. no. 102595.

[13]. N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ''Survey on SDN based network intrusion

detection system using machine learning approaches,'' Peer-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Jan. 2019.

[14]. Dr.Anusuya Ramasamya, Dr.M.Sundar Rajanb, Dr.J.R.Arunkumar "Segmentation of Spatial and Geometric Information from Floorplans using CNN Model" Turkish Journal of Computer and Mathematics Education Vol.12 No.9 (2021), 1909-1920

[15]. R. Swami, M. Dave, and V. Ranga, ''Software-defined networking-based DDoS defense mechanisms,'' ACM Comput. Surv., vol. 52, no. 2, p. 28, 2019.

[16]. C. Birkinshaw, E. Rouka, and V. G. Vassilakis, ''Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks,'' J. Netw. Comput. Appl., vol. 136, pp. 71–85, Jun. 2019.

[17]. P. Wang, L. T. Yang, X. Nie, Z. Ren, J. Li, and L. Kuang, ''Data-driven software defined network attack detection: State-of-the-art and perspectives,'' Inf. Sci., vol. 513, pp. 65–83, Mar. 2020.

[18]. M. Idhammad, K. Afdel, and M. Belouch, ''Semi-supervised machine learning approach for DDoS detection,'' Appl. Intell., vol. 48, no. 10, pp. 3193–3208, 2018.

[19]. Rajan, M.S., Arunkumar, J.R., Anusuya, R., Mesfin, A. (2021). Earliest-Arrival Route: A Global Optimized Communication for Networked Control Systems. vol 384. Springer, Cham. https://doi.org/10.1007/978-3-030-80621-7_10.

[20]. Arunkumar, J. R., Anusuya, R., Rajan, M. S., & Prabhu, M. R. (2020). Underwater wireless information transfer with compressive sensing for energy efficiency. Wireless Personal Communications, 113(2), 715–725

[21]. Priyadarshini and R. K. Barik, ''A deep learning based intelligent framework to mitigate DDoS attack in fog environment,'' J. King Saud Univ.-Comput. Inf. Sci., pp. 1–7, Apr. 2019.

[22]. V. Punitha, C. Mala, and N. Rajagopalan, ''A novel deep learning model for detection of denial of service attacks in HTTP traffic over internet,'' Int. J. Ad Hoc Ubiquitous Comput., vol. 33, no. 4, pp. 240–256, 2020.

[23]. P. Nirmala, T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, Raja Raju, "A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model", Wireless Communications and Mobile Computing, vol. 2022, Article ID 1955009, 13 pages, 2022. https://doi.org/10.1155/2022/1955009.

[24]. M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, ''DDoSNet: A deep-learning model for detecting network attacks,'' in Proc. IEEE 21st Int. Symp. 'A World Wireless, Mobile Multimedia Netw.' (WoWMoM), Aug. 2020, pp. 391–396.

[25]. Prathima, C., Muppalaneni, N.B., Kharade, K.G. (2022). Deduplication of IoT Data in Cloud Storage. In: Satyanarayana, C., Gao, XZ., Ting, CY., Muppalaneni, N.B. (eds) Machine Learning and Internet of Things for Societal Issues. Advanced Technologies and Societal Change. Springer, Singapore. https://doi.org/10.1007/978-981-16-5090-1_13

[26]. Muppalaneni, N.B., Prathima, C. (2021). A Secure Smart Shopping Cart Using RFID Tag in IoT. In: Shakya, S., Balas, V.E., Haoxiang, W., Baig, Z. (eds) Proceedings of International Conference on Sustainable Expert Systems. Lecture Notes in Networks and Systems, vol 176. Springer, Singapore. https://doi.org/10.1007/978-981-33-4355-9_52

[27]. Dr. Sivakumar .C (2023), "Design of Acceptance Sampling based Network Intrusion Detection system using Deep Learning Techniques", Journal of Survey in Fisheries Sciences, 10(1S) 3817-3821.

[28]. C. Silpa , Dr.I. Suneetha , Dr.G. Reddy Hemantha , Ram Prakash Reddy Arava, Y. Bhumika, "Medication Alarm: A Proficient IoT-Enabled Medication Alarm for Age Old People to the Betterment of their Medication Practice", Journal of Pharmaceutical Negative Results, vol. 13, no. 4, pp. 1041–1046, Nov. 2022.

[29] Infectious diseases of Rice plants classified using a deep learning-powered Least Squares Support Vector Machine Model,Goluguri,N.V.R.,Suganya Devi, K., Prathima,C.H.Indian Journal of Computer Science and

Engineering this link is disabled, 2022, 13(5), pp. 1640–1659.

[30] Auto Encoders and Decoders Techniques of Convolutional Neural Network Approach for Image Denoising In Deep Learning Chilukuri, JRA Kumar, R Anusuya, MR Prabhu, Journal of Pharmaceutical Negative Results 13 (4), 1036-1040,2022