iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** X **Month of publication:** October 2023

DOI: https://doi.org/10.22214/ijraset.2023.56350

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue X Oct 2023- Available at www.ijraset.com

DDoS Attack Detection in SDN using ML Techniques

N. Narasimha Reddy[1], G.M. Vema Reddy[2]
[1, 2]*Students, Department of Computer Science and Engineering, JNTUA College of Engineering (AUTONOMOUS) Pulivendula, Andhra Pradesh, India*

Abstract: ***The increasing prevalence of DDoS attacks poses a serious threat to modern network infrastructures. SDN has been proposed as a promising solution for enhancing network security. However, detecting and mitigating DDoS attack in software definednetwork remains a challenging task. In this research paper, suggest an innovative approach in order to identify DDoS assaults in software-defined networks using (ML) techniques. Ourmethod entails gathering and analyzing network data. Traffic data using SDN controllers. We use variety of ML techniques analyze the traffic information to discover unexpected traffic patterns that might point to the presence of a DDoS attack. Random Forest, DecisionTree, K-Means clustering are among the algorithms used. We evaluate our approach using a real-world dataset and compare it to existing DDoS detection techniques in SDN. Our results show that our approach achieves high accuracy, precision, and recall rates indetecting DDoS attacks. We also demonstrate that our technique can detect either known and unexpected DDoS assaults with low false-positive rates. Overall, our study indicates thepotency of applying machine learning methods to SDN DDoS attack detection. Our methodoffers a promising remedy for boosting network security in contemporary infrastructures.***

Keywords: DDoS, ML, SDN, Random Forest, KNN, SVM

I. INTRODUCTION

The paradigm of "Software Defined Networking" is new. The data plane and application plane that make up sdn are the tools in the control and data planes to get over the restrictions of commonnetwork architecture. Based on the controller's Control Applications such asapplication balancers,firewalls, and quality of service apps are handled by application plane, and application plane computes the information plane routing tables to determine the traffic flow burden. Software defined architecture improves network usability by segregating network control operations.Many routers throughout will be in charge of any ongoing programs a conceptually controller centralized.Applications only have a single point of access to the SDN-provided network data. The controlleris instructed to carry out load distribution and intrusion detection for the application when there isa lot of traffic by the integration of numerous apps. If an anomaly is discovered, to alter the data plane in order to fix it. Routers on the network that can be managed by software and have an open interface. The control layer of network devices in software defined architectures can be adjusted through the application layer, which is made up ofthe same controller, the SDN-architecture's-brain. API is used to communicate between the two layers. A centralized protocol is used by the infrastructure for communication between network devices and controllers. The architecture oftheSDN is explained in Figure 1. High security systems are necessary to detect and analyse suspicious activities because the controller handles a large amount of communication. By analyzing the traffic features, we suggest an ml-based mechanism to find the SDN's detrimentalbehavior.

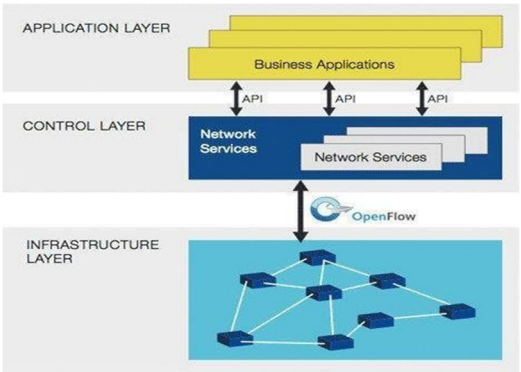


Fig-1.: SDN Architecture

II. RELATED WORK

Many people worked on finding the Ddos attacks on the Software Defined Network. There are numerous methods in finding the attacks using the traditional methods. In [1], author creates DDoSin a host. They discovered a DDoS assault using enhanced KNN algorithms. These algorithms have good prediction rates, each at 0.912. In [2], writers provided information about how ddos attack can be done using cloud computing, to counter the attacks done by using cloud computing we need to select the best feature from the dataset. In [3] it suggests that using semi supervised k means algorithm wit hybrid selection feature we can find the ddos attacks. They asserted that the suggested method provides an effective performance level of 80%.In [5], The SVM technique canbe used to find ddos attacks in an SDN. Accuracy of the experiment is 0.98. In [6], Authors used analytical machine learning, to recognise DDoS attacks. Additionally, they asserted that machinelearning-based methodologies frequently seek to identify zero-day attacks. In [7], the study shows hybrid machine learning approach can recognize DDoS attacks effectively. When operating in an SDN environment, we use SVM, Self-organized Map (SOM) to identify harmful activity. In [8], authors present an ensemble model, combining effective classification algorithm for better performance to detect the ddos attacks.

By studying the numerous works we conclude that the classification algorithms like SVM, NaïveBayes, Random Forest, KNN are used extensively for finding the ddos attacks.

III. PROPOSED WORK

In this section, we go over our suggested method for leveraging ml in sdn to detect ddos assaults.Due to its precise categorization and low complexity, we employed the support vector and random forest technique to detect attacks. By examining the crucial aspects of traffic, the svm and random forest method is utilised to identify ddos assaults. DDoS attacks are categorized into three types they are (i)volume-based assaults, which primarily utilised to flood the target server's internet pipe with UDP andICMP traffic. (ii)SYN flood, fragmented packet, ping of death, and smurf DDoS are examples of protocol attacks that primarily target stealing server resources. (iii) GET/POST floods are an example of an application layer attack that targets webapplications with the intention of bringing down the webserver.

A. Algorithms of ML

SVM is a machine learning algorithm based on the hyperplane feature which can be used for either classification or regression. In this article, it is intended to identify the packets as harmful or natural. To be subjected to a Ddos attack Support vector machine, random forest are used instead of other ml approaches. SVM is more trustworthy. DDoS attacks target numerous hosts, and the ML technique aids in the identification of malicious attacks in an SDN context. For the purpose of training models using both Support vector and Random Forest, the dataset is split into training and testing data. The ml module is used to collect and analyse the flow of traffic and the flow table entries in order to find the malicious packet.

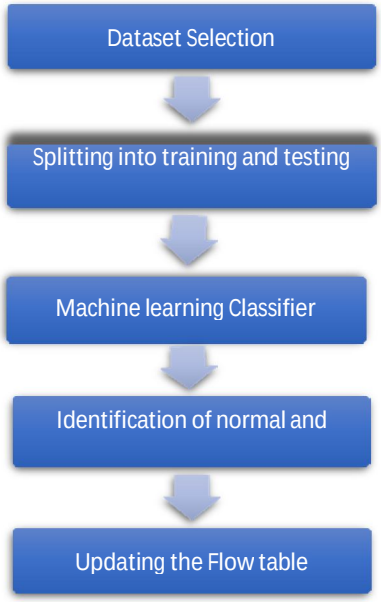


Fig-2: System Diagram

B. Identifying the Attack

Dataset is initially split into a training dataset part and a test dataset part. Essential features are found andchosen for further classification during the feature extraction step. The dataset is then run through a random forest and a support vector machine classifier. Based on the flag value (0 or1), the data is divided into two categories: attack and normal. Attack type (flag=1) warns the controllers to remove the specific flow of traffic from the flow table in that circumstance. If not, the controllerwill create the routing path for the packets of typical traffic.

Based on the given data the model is built using svm and a random forest algorithm the accuraciesof the model are calculated and the best model is selected. When it is tested against the real worldscenario when there is malicious intent in the packet flow to the network. It creates a payload to control the malicious packets if overloaded the transmission of packets is stopped.

IV. SETUP FOR EXPERIMENTATION

We utilised Mininet, a widely utilised simulation tool, to model the SDN environment [9, 11– 14]. It isused to build a link in the SDN network topology. We can theoretically add switches, controllers and hosts using mininet, as well as alter or update the network connection.

Environment for DDoS attack detection is shown in Figure 3. Using 3 controllers, 9 switches, and 100 hosts. One host is designated as the victim in a SYN flooding attack, while four hosts act as the attackers. Each time, flow will be generated in the direction of the data plane devices, and each switch will manually capture traffic flow data. We used KDD99 dataset [10] in order to train and test the suggested model.

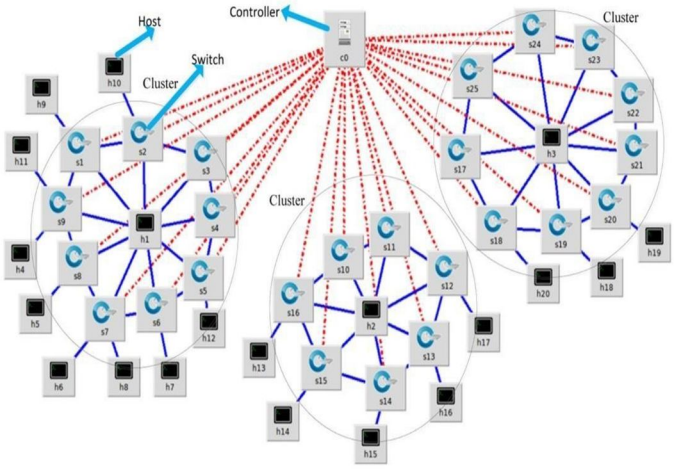


Fig-3: Network Topology

V. PERFORMANCE METRICS

Performance of the task we've proposed is determined using the classification metrics we generally use for performance analysis are used.The success rate of the ML classifier is evaluated using accuracy. The correctly classified attacks over all traffic that is classified as attack is calculated with precision. The correctly classified attacks over traffic that is wrongly classified as attack are calculated using recall. To get the weighted mean of recall and precision, utilize the F-measure. The decision tree marginally differs in both precision and recall while the SVM has an 85 percent accuracy and recall rate better than it. Random forest is more precise than the SVM.

VI. CONCLUSION AND FUTURE WORK

In the end, using ML approaches for the finding of DDoS assaults in the SDN architecture has shownto be successful for correctly classifying the attacks and lowering the number of wrongly classified attacks for existing detection strategies. The use of different (ML) methods, including decision trees, SVMs, and neural networks, has allowed researchers to recognise aberrant traffic patterns that are indicative of DDoS attacks withhigh accuracy.

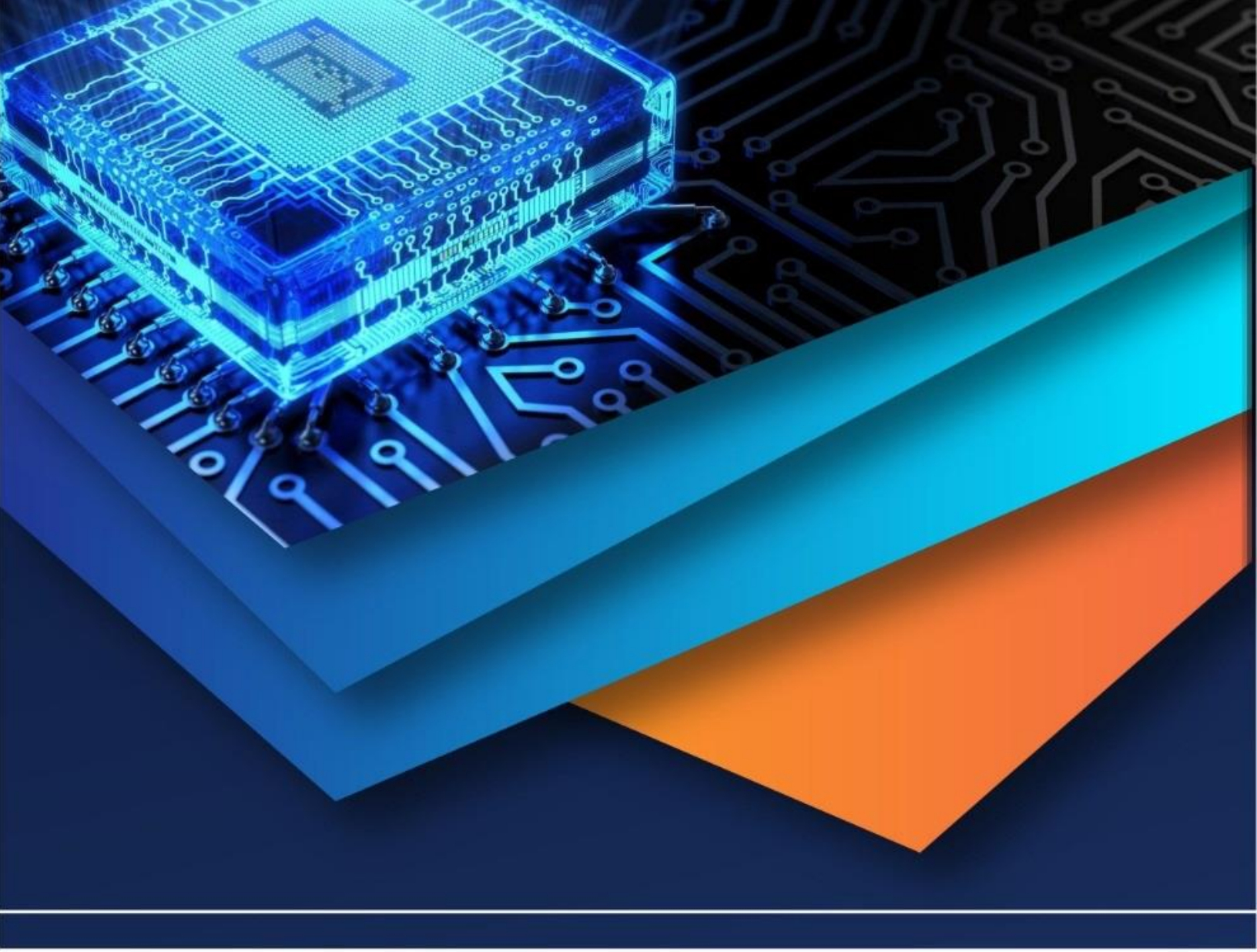
Future work in this area is still possible, though. Investigating the efficacy of merging several ML algorithms to raise the overall accuracy of DDoS detection systems is one possible line ofresearch. Additionally, it will be crucial to create ML models that can adjust and learn in real-time to new types of attacks as attackers continue to advance their strategies and methods.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Future study should also examine how various network topologies and traffic patterns affect the effectiveness of ML-based DDoS detection systems. This will be especially crucial as SDN usage increases and it is implemented in more intricate network environments. Finally, it is important to take into account the usability and scalability of ML-based DDoS detection systems as the amount of network traffic keeps growing, making it crucial to develop ML models that can effectively process large amounts of data in real-time without placing an undue computational burden on network infrastructure.

REFERENCES

[1] Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN Withthe Degree of DDoS Attack in Software-Defined Networks. IEEE Access, 8, 5039-5048.
[2] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS)attacksin SDN and cloud computing environments. IEEE Access, 7, 80813- 80828.
[3] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semisupervised K-means DDoS detectionmethodusing hybrid feature selection algorithm. IEEE Access, 7, 64351-64365.
[4] Meti, N., Narayan, D. G., & Baligar, V. P. (2017, September). Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. In 2017 internationalconference on advances in computing, communications and informatics (ICACCI) (pp. 1366-1371). IEEE.
[5] 15th International Symposium on Pervasive Systems, Algorithms and Networks IEEE DDoSAttack Identification and Defense using SDN based on Machine Learning Method,2018
[6] Muthamil Sudar, K., & Deepalakshmi, P. (2020). A two level security mechanism to detecta DDoS flooding attack in software-defined networks using entropy-based and C4. 5 technique. Journalof High Speed Networks, (Preprint), 1- 22.
[7] Deepa, V., Sudar, K. M., & Deepalakshmi, P. (2018, December). Detection of DDoS attack on SDN control plane using Hybrid Machine Learning Techniques. In 2018 International Conference onSmart Systems and Inventive Technology (ICSSIT) (pp. 299- 303). IEEE.
[8] Deepa, V., K. Muthamil Sudar, and P. Deepalakshmi. "Design of Ensemble Learning Methods forDDoS Detection in SDN Environment." 2019 International Conference on VisionTowards Emerging Trends in Communication and Networking (ViTECoN). IEEE, 2019.
[9] J. Cui, M. Wang, and Y. Luo, ``DDoS detection and defense mechanism based on cognitive- inspired computing in SDN," Future Gener. Comput. Syst., vol. 97, pp. 275_283, Aug. 2019.
[10] N. I. G. Dharma, M. F. Muthohar, J. D. A. Prayuda, K. Priagung, and D. Choi, ``Time- based DDoS detection and mitigation for SDN controller," in Proc. 17th Asia_Paci_c Netw. Oper. Manage.Symp. (APNOMS), Aug. 2015, pp. 550_553.
[11] S. Wilson Prakash and P. Deepalakshmi, DServ-LB: Dynamic server load balancing algorithm,International Journal of Communication Systems, 32 (1) (2019), 1-11.
[12] S. Wilson Prakash and P. Deepalakshmi, Flow-based Dynamic Load balancing algorithm for theCloud networks using Software Defined Networks, International Journal of Cloud Computing, 8(4) (2019), 299-318.
[13] S. Wilson Prakash and P. Deepalakshmi, Server-based Dynamic Load Balancing, Proceedings ofthe IEEE International Conference on Networks & Advances in Computational Technologies, Thiruvanthapuram, India, 2017.
[14] S. Wilson Prakash and P. Deepalakshmi, Artificial Neural Network based Load Balancing on Software Defined Networking, IEEE International Conference on Intelligent Techniques in Control,Optimization and Signal Processing, (2019), 1-4.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)