Literature Review on DDOS Attacks Detection Using SVM algorithm.

Manasvi Suryavanshi [1], Nikita Pawar[2], Sanathkumar Pillai[3]

[1,2,3] *Student and Department of Computer Engineering, ISB&M School of Technology, SPPU, India.*

---***---

Abstract - *Software-defined network (SDN) is a network architecture that is used to build, and design the hardware components virtually. In the traditional network, it's not possible to change dynamically, because it's a fixed connection. SDN is a good way but still is weak to DDoS attacks. The DDoS attack is a problem for the internet. To avert the DDoS attack, the machine learning algorithm can be used. The DDoS attack is the multiple collaborated systems that are used to target a particular server at the same time. In SDN The Data plane takes care of the network traffic based on the decision made by the controller. The Control plane chooses the course of traffic by computing the routing tables. We have used a machine learning technique namely Support Vector Machine (SVM) to detect malicious traffic using two datasets namely KDD99 and CIS-CIC-IDS 2018. Our test outcome shows that the Support Vector Machine (SVM) algorithm provides better accuracy and detection rate.*

Key Words: Machine learning, DDoS, SVM, SDN, KDD99, CIS-CIC-IDS

1. INTRODUCTION

Software-Defined Networking is an emerging paradigm that overcomes the limitations of conventional network architecture by separating the control from data plane devices. SDN consists of planes such as the data plane, control plane, and application plane. The Data plane takes care of the network traffic based on the decision made by the controller. The Control plane chooses the course of traffic by computing the routing tables. SDN architecture boosts the network performance by breaking up the network control and forward function. The control programs managing a logically centralized controller will control multiple routers across the network.

1.1 Machine Learning

Machine Learning is a subfield of Artificial Intelligence, that teaches computers to do what comes naturally to humans and animals: learn from experience. It has various types: Supervised learning, which trains a model on known input and output data and predicts future outputs. Unsupervised Learning, which finds hidden patterns in input data. Reinforcement Learning is a reinforcement learning agent that can perceive and interpret its environment, take actions and learn through trial and error.

1.2 Supervised Learning

A supervised learning algorithm takes a known set of input data to the data(output) and trains a model to generate predictions for the response to new data. It comprises two techniques classification and regression to develop machine learning models. Classification models identify input data. The data can then be filtered into specific groups.

SVM: In Machine Learning one of the most important tasks is when you have a bunch of objects that you want to classify, for that you are required to use SVM. Support Vector Machines (SVM) are some of the simplest and arguably the most elegant methods for classification. Each object you want to classify is represented as a point in an n-dimensional space and the coordinates of this point are usually called features. SVMs perform the classification test by drawing a hyperplane that is a line in 2D or a plane in 3D in such a way that all points of one class are on one side of the hyperplane and all points of the other class are on the other side and while there could be multiple such hyperplanes SVM tries to find the one that best separates the two classes.

2. Literature Survey:

Sr. no.	Literature Name	Research Gap Identified
1	WORKSHOP ON SUPPORT VECTOR MACHINES: THEORY AND APPLICATIONS	This paper presents several of the issues discussed during the one-day workshop on "Support Vector Machines" organized as part of the (ACAI 99) in Chania, Greece. The paper's goal is twofold: to present a summary of the theory and current understanding of SVM, and to discuss the issues that arose during the workshop.
2	CNN-Based Network Intrusion Detection against Denial-of-Service Attacks.	The project was developed based on a Convolutional Neural Network (CNN) and evaluated its performance through comparison with a Recurrent Neural Network (RNN). Furthermore, we suggest the optimal CNN design for better performance through numerous experiments. The number of clusters must be specified in advance by the system. Clusters having non-convex forms are not suited for detection If the training data is not linearly separable, determining optimal parameters in SVM might be difficult.
3	Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques.	The paper proposes a machine learning technique namely Decision Tree and Support Vector Machine (SVM) to detect malicious traffic. The test shows the outcome that the Decision Tree and Support Vector Machine algorithm provides better accuracy and detection rate.
4	The Design of SDN-based Detection for Distributed Denial of Service (DDoS) attack.	SDN can give an attractive solution for network security. There are different kinds of DDoS detection techniques; signature-based and anomaly-based detection. When the signature-based detection technique had made use of network behaviors, the anomaly-based detection then used the machine learning techniques. The paper proposes the design of SDN-based detection for DDoS attacks. From the advantage of ASVM, it can significantly reduce the training time as well as testing time compared with the SVM algorithm.
5	A Comprehensive and Effective Mechanism for DDoS Detection in SDN	Apart from a single point of failure of the controller, an attacker can target SDN at various levels by DDoS attacks. Existing solutions focus on a particular attack type or require alterations in SDN infrastructure. This paper proposes a detailed, yet effective and lightweight approach to detect various fundamentally different DDoS attacks in SDN that rely on sequential analysis and employs a non-parametric change point detection technique called Cumulative Sum accuracy, detection rate, and low false alarm rate compared to the simple machine learning. Using CAIDA, we evaluated the effectiveness of our solution Internet traces as well as the DARPA intrusion detection evaluation dataset.
6	A two-level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 technique	The paper has proposed a security mechanism that detects the attack on two levels to create an efficient DDoS detection system. In level one, they have used an entropy-based mechanism that detects the attack in an earlier stage by analyzing the number of packets and IP addresses. And in level two they have used a machine learning technique called the C4.5 technique which tries to improve the accuracy by analyzing more than six features. Their experiment concludes with the result showing entropy-based technique is useful for early detection of DDoS attacks and the C4.5 technique improves the accuracy and low false alarm rate.
7	Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques	The paper has proposed a hybrid machine learning model which helps in the detection of DDoS attacks in an SDN environment. They have used a combination of two machine learning-based models i.e. Support Vector Machine (SVM) and Self Organized Map (SOM) and have achieved more precision, distinguishing rate, and small false alarm rate compared to the simple machine learning model.
8	Time-based DDoS Detection and Mitigation for SDN Controller	The paper has reported on the detection and mitigation method of DDoS attacks on SDN controllers. They have described the basic operation of SDN controllers and have analyzed the potential vulnerabilities in SDN controllers that can be exploited for DDoS attacks. They have also investigated the pattern of time of DDoS attacks for preventing DDoS attacks in the future.

9	Implementation of SDN-based IDS to protect Virtualization Server against HTTP DoS attacks	The paper has proposed an SDN-based IDS which protects the Virtualization Server from HTTP Denial Of Service attacks. They have concluded their experiment by showing success in detecting HTTP Denial Of Service attacks and interrupting communication between the attacker and the server by dropping all packets from the attacker. Their system has also been able to detect other forms of attack and respond to malicious activities.
10	DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks	The paper has analyzed four features when the SDN controller is attacked by a DDoS attack. They have proposed a new concept called the degree of attack and based on the concept they have derived a detection algorithm called the DDA algorithm. And to improve their detection efficiency, they have proposed one more algorithm named DDAML algorithm. Their experiment shows that their proposed algorithms can identify the DDoS attack better, and they have achieved higher detection rates compared with the existing data.

Table Fig -1: Literature Review

3. CONCLUSIONS

As there is increasing evolution in cyber-attacks in the modern era it is a difficult task to detect DDoS attacks that requires a fundamental grasp of cyber security as well as modern threats, networking, and platforms to prevent them from happening. We will be using the KDD99 dataset and CSC CIC IDS 2018 to train and test our proposed model we will be using the Support Vector Machine algorithm to detect the DDoS attack on the classification module which is deployed on the SDN environment the SVM techniques are used to distinguish between normal and malicious traffic data our experimental shows that SVM works better in our simulated environment shortly to gain better accuracy we plan to implement advanced support vector machine A-SVM to detect DDoS attacks by analyzing the kernel vector.

REFERENCES

[1]. Dong, S., & Sarem, M. (2019). DDoS Attack Detection Method Based on Improved KNN With the 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) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813-80828.

[3]. Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-supervised K-means DDoS detection method using 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 international conference on advances in computing, communications, and informatics (ICACCI) (pp. 1366-1371). IEEE.

[5]. 15th International Symposium on Pervasive Systems, Algorithms and Networks IEEE DDoS Attack Identification and Defense using SDN based on Machine Learning Method, 2018

[6]. Muthamil Sudar, K., & Deepalakshmi, P. (2020). A two-level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 techniques. Journal of 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 on Smart Systems and Inventive Technology (ICSSIT) (pp. 299-303). IEEE.

[8]. Deepa, V., K. Muthamil Sudar, and P. Deepalakshmi." Design of Ensemble Learning Methods for DDoS Detection in SDN Environment." 2019 International Conference on Vision Towards 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 Genre. Compute. 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 the Cloud 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 of the 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.

[15].Santos, R., Souza, D., Santo, W., Ribeiro, A., & Moreno, E. (2020). Machine learning algorithms to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, 32(16), e5402. Authorized licensed use is limited to Tencent.