Detection of Distributed Denial of Service Attack in SDN using a Machine Learning Technique

Atul Sharma[1], Anand Gadekar[2], Sanket Kasbe[3], Urvashi Maheshwari[4], Prof. R. S. Apare[5]
UG Students, Department of Information Technology[1,2,3,4]
Professor, Department of Information Technology[5]
SKN Sinhgad Institute of Technology And Science, Lonavala, Maharashtra, India

Abstract: *Software-defined network (SDN) is a network architecture that is used to build, and design the hardware components virtually. We can dynamically change the settings of network connections. In the traditional network, it's not possible to change dynamically, because it's a fixed connection. SDN is a good approach but still is vulnerable to DDoS attacks. The DDoS attack is managed on the internet. To prevent 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 control layer is in the center that links with the application and infrastructure layer, where the devices in the infrastructure layer are controlled by the software. In this paper, we propose a machine learning technique namely a Decision Tree to detect malicious traffic. Our test outcome shows that the Decision Tree detects whether the attack is safe or not.*

Keywords: SDN, attacks, DDoS, Decision Tree

I. INTRODUCTION

DDoS detection is distinguishing distributed denial of service (DDoS) attacks from normal network traffic to perform effective attack mitigation. The primary goal of a DDoS attack is to either limit access to an application or network service, thereby denying legitimate users access to the services.

Many types of DDoS attack schemes are used today and they are steadily becoming more sophisticated. However, their common goal is to overwhelm targeted network resources with traffic or requests for service from many different sources — potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by identifying and blocking a single IP address. The sheer distribution of attacking sources also makes it very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

The first step in avoiding or stopping a DDoS attack is knowing that an attack is taking place. To detect an attack, one has to gather sufficient network traffic information, then perform analysis to figure out if the traffic is a friend or foe. This process can be performed manually or in an automated fashion. DDoS detection is the key to quickly stopping or mitigating attacks and for this to happen, two success criteria need to be met:

1. Speed of detection
2. Accuracy of detection

So, detection methods are a key consideration in formulating a strong DDoS defense

1.1. The DDoS Threat

There is no doubt, as evidenced by the alarming rise of DDoS attacks, that DDoS detection is an absolute necessity for businesses that rely on the internet traffic for them to avoid disruption of applications and services, revenue loss, and brand damage. Neustar, Inc., and others regularly publish reports on DDoS attacks and protection trends. A Neustar report highlights that DDoS attack volume has remained consistently high and that these attacks cause real damage to organizations. Some highlights from that report:

- **DDoS attacks are unrelenting and show no sign of abating**: The overwhelming majority of surveyed organizations (73 percent) suffered a DDoS attack. Eighty-five percent of attacked organizations were attacked more than once and 44 percent were attacked more than five times.
- **DDoS attacks are only the tip of the spear in complex assaults**: The majority of organizations that suffered

DOI: 10.48175/IJARSCT-7514

a DDoS attack (53 percent) also experienced some form of additional compromise. Forty-six percent of breached organizations discovered a virus, the malware was activated at 37 percent of breached organizations, and ransomware was encountered at 15 percent of breached organizations.

- **DDoS attacks are time-consuming and expensive**: It can take hours to detect and mitigate a DDoS attack at a significant cost to the organization. Seventy-one percent of organizations took an hour or more to detect a DDoS attack and 72 percent took an additional hour or more to respond to the attack. Forty-nine percent of surveyed organizations lose $100,000 or more per hour of downtime during these attacks.

II. LITERATURE SURVEY

The Distributed Denial of Service (DDoS) attack has seriously impaired network availability for decades and still, there is no effective defense mechanism against it. However, emerging Software Defined Networking (SDN) provides a new way to reconsider the defense against DDoS attacks. This paper proposes two methods to detect the DDoS attack in SDN. One method adopts the degree of DDoS attack to identify the DDoS attack. The other method uses the improved K-Nearest Neighbors (KNN) algorithm based on Machine Learning (ML) to discover the DDoS attack. The results of the theoretical analysis and the experimental results on datasets show that our proposed methods can better detect the DDoS attack compared with other methods.

Summary: Dong, S., & Sarem, M describes the results of the theoretical analysis and the experimental results on datasets to show that our proposed methods can better detect the DDoS attack compared with other methods.[1]

Recently, researchers and the industry have widely adopted software-defined networks (SDNs) and cloud computing. However, the widespread acceptance of these novel networking paradigms has hampered security threats. Advances in processing technologies have helped attackers in increasing the attacks too, for instance, the development of Denial of Service (DoS) attacks to distributed DoS (DDoS) attacks which are seldom identified by conventional firewalls. In this paper, we present the state of the art of the DDoS attacks in SDN and cloud computing scenarios especially, we focus in theanalysis of SDN and cloud computing architecture. Besides, we also overview the research works and open problems in identifying and tackling DDoS attacks.

Summary: Dong, S, and the team performed research work that opened open problems in identifying and tackling DDoS attacks.[2]

Distributed denial of service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. Therefore, it is necessary to propose an effective method to detect DDoS attack from massive data traffics. However, the existing schemes have some limitations, including that supervised learning methods, need large numbers of labeled data and unsupervised learning algorithms have relatively low detection rates and high false positive rates. To tackle these issues, this paper presents a semi-supervised weighted k-means detection method. Specifically, we firstly first a Hadoop-based hybrid feature selection algorithm to find the most effective feature sets and propose an improved density-based initial cluster centers selection algorithm to solve the problem of outliers and local optimal. Then, we provide the Semi-supervised K-means algorithm using hybrid feature selection (SKM-HFS) to detect attacks. Finally, we exploit DARPA DDoS dataset, CAIDA "DDoS attack 2007" dataset, CICIDS "DDoS attack 2017" dataset, and real-, world dataset to carry out the verification experiment. The experiment results have demonstrated that the proposed method outperforms the benchmark in the respect of detection performance and technique for order preference by similarity to an ideal solution (TOPSIS) evaluation factor.

Summary: The experimental results of the suggested approach surpass the benchmark in terms of detection performance and the strategy for order preference by similarity to an ideal solution (TOPSIS) evaluation factor.[3]

SDN (Software Defined Network) has attracted interest as a new paradigm in the network. Thus, the security of SDN is important. Distributed Denial Service (DDoS) attack has been the plague of the Internet. Now, it is a threat in some SSDN-applied scenarios, such as the campus network. It alleviates the DDoS attack in the campus

network, we propose an SDN framework to identify and defend against DDoS attacks based on machine learning. This framework consists of 3 parts white ich are the traffic collection the ion module, the DDoS attack identification module, and the flow table delivery module. The traffic collection module extracts traffic characteristics to prepare for traffic identification. Utilizing the flexible and multi-dimensional features of SDN network architecture in deploying a DDoS attack detection system, the controller extracts the network traffic characteristics through statistical flow table information and uses the support vector machines (SVM) method to identify the attack traffic.[4]

III. CONCLUSION

In Today's Days, Cyber attack has become common, many people do not even know that there is an attack called a cyber attack so, with help of our project, we can protect people from Dos and DDoS attack. we can even warn them so that no one can take advantage of them.

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 a hybrid feature selection algorithm. IEEE Access, 7, 64351- 64365.

[4]. 15th International Symposium on Pervasive Systems, Algorithms, and Networks IEEE DDoS Attack Identification and Defense using SDN based on Machine Learning Method, 2018

[5]. Miti, N., Narayan, D. G., & Balega, V. P. (2017, September). Detection of distributed denial of service attacks using machine learning algorithms in software-defined networks. In the 2017 international conference on advances in computing, communications, and informatics (ICACCI) (pp. 1366-1371). IEEE.

[6]. Muthamil Sudar, K., & Deepa Lakshmi, 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., & Deepa Lakshmi, 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.

DOI: 10.48175/IJARSCT-7514