International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 12 | Dec 2018 www.irjet.net p-ISSN: 2395-0072

Detection of Distributed Denial-of-Service (DDoS) Attack on Software Defined Network (SDN)

Mr. Ajinkya Patil[1], Mr. Pratik Jain[2], Mr. Ravi Ram[3], Mr. Venkatesh Vayachal[4], Prof. S. P. Bendale[5]

[1,2,3,4]B. E. Student, Dept. of Computer Engineering, NBN Sinhgad School of Engineering, Ambegaon, Pune – 411041, Maharashtra, India

[5]Professor, Dept. of Computer. Engineering, NBN Sinhgad School of Engineering, Ambegaon, Pune – 411041, Maharashtra, India

---

Abstract - *Software Defined Network (SDN for short) enables better network flow, managing network traffic, and optimizing the network to work better than traditional network. Software-defined networking technology is a cloud computing approach that facilitates network management and enables efficient network configuration programmatically to improve the performance of the network and to facilitate monitoring. SDN addresses the fact that the traditional networks have a static architecture which is decentralized and highly complex. The need of current networks is flexibility and easy and efficient troubleshooting. SDN uses the concept of centralization of network intelligence in a single main network component. This is achieved by dissociation of the forwarding process of network packets from the routing process.*

The rate of development of internet technology is higher than ever. Due to this rapid development, the network flow rates are now higher than ever. In addition, the Distributed Denial-of-Service (DDoS) attacks which poses a major threat to network security are now prevalent. In computer networks, a Denial-of-Service (DoS) attack is a cyber-attack where, the attacker or the mastermind's goal is to make the network resources or a machine (such as Servers, Network Controllers, Access Points, etc.) unable to process the requests of the intended users. The attacker achieves this by disrupting the services of a machine (host) connected to the network. If any host in the network is unable to process or function the requests from users, the network fails.

Using functionalities of Mininet such as OpenFlow Switches, Ryu Controllers, Collection Modules and feature extractions we are trying to simulate an SDN (Software Defined Network). A DDoS attack on this network will be simulated. We will try to detect this attack on the network using detection methods based on data mining techniques.

Key Words: Software Defined Network (SDN), Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS).

1. INTRODUCTION

Software Defined Network (SDN in short), is an architecture that is dynamic, it can adapt to different functionalities such as high-bandwidth, profitable, and can be managed easily compared to traditional network model. [1] Software Defined Networking provides number of benefits, centralized network provisioning, better enterprise management, better security, low operational costs, isolation and traffic control, managing packet forwarding. The SDN suggests a Centralized Network by dividing the architecture into Network Control Plane and Forwarding Plane. The network control plane is directly programmable and consists of one or more controllers which is also considered as Brain of SDN.

With the separation of Control Plane, the administrators are able to dynamically adjust traffic flow in the whole network, according to network needs. [2] Administrators can also configure and optimize the network security and secure the network resources with the help of SDN programs.

The network implementation, configuration and troubleshooting require high skilled network and system engineers. The system managers can control different components or "layers" (i.e., application, control and data plane), they can allocate resources to network users through application layer, manage the network entities through control plane, and network devices on data plane.

The OpenFlow protocol was one of the important elements for building a SDN, it can also be called as OpenFlow framework, first SDN standard. Most of the software defined network have some version of SDN Controller, as well as Southbound APIs and Northbound APIs as shown in Figure 1. The controllers and switches follow OpenFlow standards, and OpenFlow runs between them acting as a communication medium. There are different controller platforms which are open source such as Beacon, OpenDayLight, Floodlight, Open vSwitch.

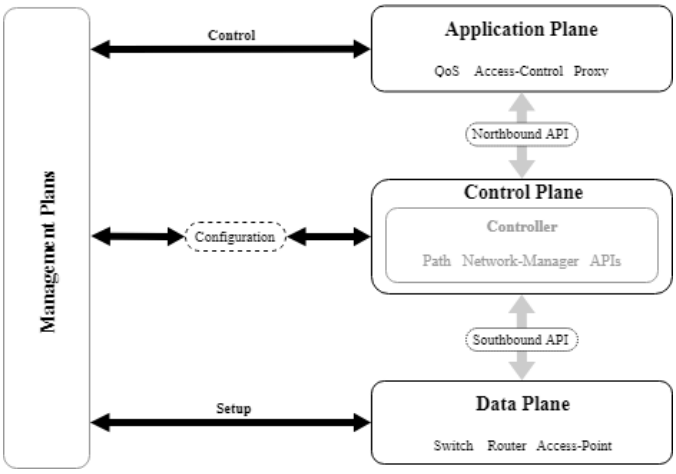

Fig - 1: Software Defined Architecture

The Traditional network are static and can be programmed at the time of installation, while the Software Defined Network (SDN) are programmable at deployment time as well at later stages. Traditional networks have distributed control plane and SDN have centralized control plane. The Traditional network are hardware appliances and works using protocols. The SDN are configured using open software and use APIs to configure the network as per the needs.

As the Software Defined Network is based on centralized control there is high-value target exposed in the network. The attackers can have total control over the network by taking control over it, and a single vulnerability could cause lot of damage, so security must be primary concern when deploying the SDN, it also increases the workload of the administrator as security must be deployed manually. Attacks such as Network Manipulation, Traffic diversion, App manipulation, API exploitation Traffic sniffing, Denial-of-Service (DOS) and Brute force. We are focusing on Distributed Denial-of-Service (DDoS) attack in particular.

The Distributed Denial-of-Service (DDoS) are most threatening challenges to Internet Security nowadays. As shown in Figure 2, [3] The DDoS attacker first takes control over the network devices (computers or other devices) called as hosts in the network to carry out the attacks, the goal of the attacker is to overload the data packets being sent to target (server's) and making the legitimate packet flow from accessing available services. [4] The attacker uses many hosts they can send multiple new packets at the same time, the incoming new packets will search for its destination information which is stored in switch forwarding table, as the legitimate packets cannot be differentiated by harmful packets hence the attack becomes successful.

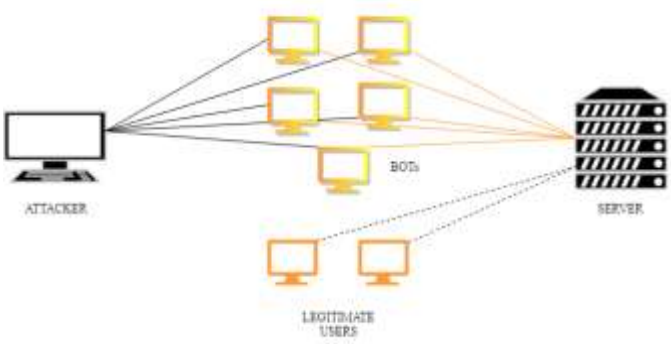

Fig -2: Distributed Denial-of-Service (DDoS) Attack

Detecting these DDoS attacks can be very hard done by conventional detection methods. The attackers may be distributed and located under different switches, the detection process may not benefit by performing detection process into the switches because switches may not detect attacks completely.

2. OBJECTIVES

As the requirements are dynamic in the today's world it becomes a necessity for the system configuration to evolve as per the requirement. The networking systems have a drastic role in the system communication. As the requirements change it is need to configure a network which could be modified with the help of the software remotely instead of configuring hardware as and when required. The Software Defined Network (SDN) is a way through which this could be attained easily. Using the Software Defined Network. With the help of SDN it is easy to configure the network as per the traffic and as per the user demands increase, the topologies of the network could be easily changed, the network traffic flow could be monitored and also it is possible to re-distribute the traffic to avoid the bottlenecks.

The SDN allows us a vast field of network management to ease the networking solutions. The SDN is vulnerable to attacks from outside sources and the data needs to be protected. The attacks from parasites could cause a huge data loss leading to loss in data integrity as well as data consistency. The familiar types of attacks in the SDN are the Denial-of-Services attack and Distributed Denial-of-Service attack.

DoS and DDoS attacks are the types of attack in which the system is flooded with number of un-legit requests, thus keeping the servers busy serving the fakes and denying service to the legit requests. This causes system breakdown and leads to mass communication failure in the cases of heavy traffic servers of social media platforms.

Our study mainly focuses on the detection of DDoS attacks in the software defined network, this would allow us to protect the system from denying services to the users and protecting the service integrity. Once the attack on the system is recognized it is easy to control the attack by disabling the particular sets of internet protocol addresses and thus securing the systems.

3. RELATED RESEARCH

Currently, there are various methods available to detect the DDoS attack. Some of the methods are mentioned below.

In a research paper, D. Kotani [5] proposed packet-in filtering mechanism which makes the SDN control panel secure. The mechanism works by recording the values of packet headers, before passing the packets then filtering the packets which aren't recorded. This method works until the attacker doesn't generate new flows.

S. Mousavi [6] introduced a detection method before a DDoS attack is initiated on the network. It is based on entropy variation of data flow on IP address. It assumes that the IP addresses (destination) are evenly distributed. If any attack flow is present then the IP addresses must be in small quantity to generate low-traffic flow.

P. Dong [7] proposes detection method for DDoS attack against controllers. The switches contain the information of

incoming flow and reports it to the controller. The attack detection module runs on the northbound interface of the controller distinguishing between flow statistics.

Yang Li [8] proposes feature selection and feature weight mechanisms to reduce the computational cost and boost performance. The method is based upon Transductive Confidence Machines for K-Nearest Neighbors (TCM-KNN) algorithm.

S. Jaiswal [9] uses K-Nearest Neighbor (KNN) classifier and Ant Colony Optimization (ACO) techniques. It is applied on multiple classifiers, which aims on misclassified features taking more amount of time to calculate and classify, the ACO optimizes the category until the features are accurately classified. It employs ID3 (decision tree) algorithm for feature reduction.

H. Peng [10] focuses on the anomalous flow, and presents anomaly flow detection method, it collects the information (such as flow details, flow type, all features by which we can distinct between multiple flows) from switches or controllers and then Detection mechanism is responsible for classifying the features and network flow with Double P-value of Transductive Confidence Machines for K-Nearest Neighbors (DPTCM-KNN) algorithm.

4. RESULT ANALYSIS

Based on the experimental results performed on KDD'99 Dataset which is most used data set for anomaly detection methods and research. [11] KDD99 is feature extracted version of DARPA which is the base raw dataset. In the 1998 DARPA Intrusion Detection System Evaluation Program was prepared, consisting of an attack scenario to Air-Force base. It consists of host and network dataset files; Host dataset file is small dataset containing system calls. Network Dataset is mostly used because it consists of seven weeks of network traffic (TCP/IP dump).

Table -1: Conversion Matrix

Predicted Values	Actual Values	
	Positive (1)	Negative (0)
Positive (1)	TP	FP
Negative (0)	FN	TN

Confusion Matrix is used to measure the performance of the classification algorithm or classifier. We can derive many ratios from confusion matrix:

- **True Positive (TP):** These are cases in which we predict 'Yes' and the actual result shows 'Yes'.
- **True Negatives (TN):** These are cases in which we predict 'Yes' but the actual result shows 'No'
- **False Positive (FP):** Here we predict 'Yes', and actual result is 'No'. This is also called Type I error.
- **False Negative (FN):** Here we predict 'No' and actual result is 'Yes'. This is also called Type II error.

The findings are shown in Table 2 which use Mininet Emulator for simulating virtual software-defined network, for TCM-KNN algorithm which improves feature selection, KNN-ACO algorithm which combines K-Nearest Neighbor and Ant Colony Optimization, and DPTCM-KNN algorithm which improves the precision even further.

Table -2: Results based on KDD99 Dataset

Method	True Positive Rate	False Positive Rate
TCM-KNN	Low (89%)	Medium (11%)
KNN-ACO	Medium (92%)	Medium (11%)
DPTCM-KNN	High (97%)	Low (6.25 %)

- **True Positive Rate** (TPR) = TP/(TP + FN)
- **False Positive Rate** (FPR) = FP/(TP + FN)

5. CONCLUSION

In this paper, we have studied various methodologies which are used for detection of Distributed Denial-of-Service (DDoS) Attacks on Software Defined Network (SDN), based on the findings and results we have concluded that the Double P-value of Transductive Confidence Machines for K-Nearest Neighbors (DPTCM-KNN) method is more feasible and efficient to find out anomalous flow in Software Defined Network.

REFERENCES

[1] Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. Security and communication networks, 9(18), 5803-5833.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] Khan MFI (2017) Software-Defined Networking Reviewed Model. Int J Adv Technol 8: 177. doi:10.4172/0976-4860.1000177

[3] S. P. Bendale, J. R. Prasad, "Security threats and challenges in Future Mobile Wireless Networks", IEEE International Conference proceeding GCWCN, 2018-19.

[4] Al-Mafrachi, B. H. A. (2017). Detection of DDoS Attacks against the SDN Controller using Statistical Approaches (Doctoral dissertation, Wright State University).

[5] Kotani, D., & Okabe, Y. (2014, October). A packet-in message filtering mechanism for protection of control plane in openflow networks. In Proceedings of the tenth

ACM/IEEE symposium on Architectures for networking and communications systems (pp. 29-40). ACM.

[6] Mousavi, S. M. (2014). Early detection of DDoS attacks in software defined networks controller (Doctoral dissertation, Carleton University).

[7] Dong, P., Du, X., Zhang, H., & Xu, T. (2016, May). A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows. In Communications (ICC), 2016 IEEE International Conference on (pp. 1-6). IEEE.

[8] Li, Y., & Guo, L. (2008, March). TCM-KNN scheme for network anomaly detection using feature-based optimizations. In Proceedings of the 2008 ACM symposium on Applied computing (pp. 2103-2109). ACM.

[9] Jaiswal, S., Saxena, K., Mishra, A., & Sahu, S. K. (2016, March). A KNN-ACO approach for intrusion detection using KDDCUP'99 dataset. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on (pp. 628-633). IEEE.

[10] Peng, H., Sun, Z., Zhao, X., Tan, S., & Sun, Z. (2018). A detection method for anomaly flow in software defined network. IEEE Access.

[11] Özgür, A., & Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ PrePrints, 4, e1954v1.