International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 12 | Dec 2019 www.irjet.net p-ISSN: 2395-0072

A Study of DDoS Attacks in Software Defined Networks

Chinmay Dharmadhikari[1], Salil Kulkarni[2], Swarali Temkar[3], Shailesh Bendale[4]

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

---

Abstract - *Virtualization has changed the ball game completely in all the technological aspect. One of such application of it is SDN. Software Defined Network (SDN) is currently the most popular network architecture in use. SDN separates the Data Plane from the Control Network. It introduces controllers, based on the OpenFlow protocol, to control the switches and routers in the data plane. Although SDN provides a simplified way to control the network, it gives rise to new security threats such as DoS attacks, Man in the Middle attacks etc. SDN being centralized it has a single point of failure which makes it vulnerable. One of the most common among them is DDoS. It affects the server which fails the whole network in addition to this it is easy to start this attack. Therefore, in order to detect and mitigate these vulnerabilities there have been several algorithms and approaches that has been enforced. In this paper a study various types of DDoS attack on SDN has been discussed, also the mitigation and detection of the attack has been studied.*

Key Words: Software Defined Networks (SDN), DDoS, Security.

1. INTRODUCTION

As SDN has dramatically changed the working of the network and made it more efficient by centralizing the control of the network with the help of controller, in addition to that it also separates the data plane from the control plane which helps in achieving the goal of centralization [1]. The architecture of the SDN is as follows.

SDN consists of 2 planes- Data Plane and Control Plane. Data plane is the actual network where the packets are forwarded. Switches and routers are the main components of data plane. Control plane consists of the controller as the main component. Controller is used to control the switches in the data plane. It provides central management and monitoring of the network. The control plane consists of controller and its 3 interfaces.

1. South-Bound Interface: Provides an interface between switches and controller.

2. North-Bound Interface: Provides an interface between controller and application layer program.

3. East-West Bound Interface: Provides an interface between the different controllers.

Following figure depicts basic architecture of SDN.

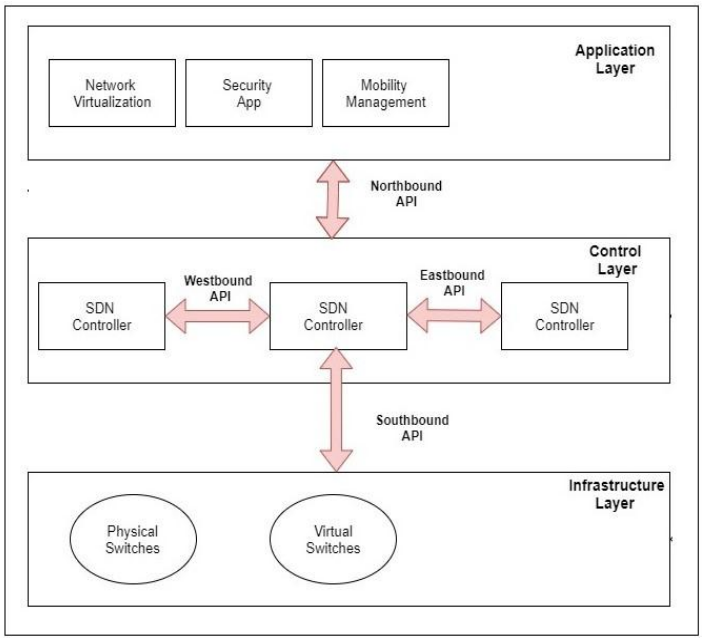

Fig -1: SDN Architecture

SDN has several advantages like centralized management, monitoring, centralized services and security.

Various Controllers are available in the market. Some of the Controllers are OpenDayLight, FloodLight, Pox, Ryu etc.

SDN currently does not have a security module. Security is the main concern of SDN. Although SDN architecture overcomes some the traditional attacks, it also gives rise to new attack strategies. Security concerns may arise due to some unintentional actions from the devices inside the network, or intentional attacks performed by malicious users [4].

Attacks on SDN can be classified as Spoofing, Tampering, Information Disclosure, Repudiation, Elevation of Privileges and DoS [3].

1. Spoofing: Spoofing is falsifying the information about the attacker. Spoofing is a part of a larger attack. Attacker can perform ARP Spoofing and IP Spoofing. Chances of Spoofing are reduced in SDN as

controller makes dynamic and regular changes in the network.

2. Tampering: Altering of network information is known as Tampering. Attackers might change the information in the flow tables of switches. They may alter the firewall policies to deny services to some users.

3. Repudiation: Denial of one of the host in 2-way communication is Repudiation. Encryption can be used to overcome repudiation.

4. Information Disclosure: Information Disclosure is an attack that is used to infiltrate the network. Infiltrators disclose information about the network to the attacker. Attackers can take control of a switch and can change the flow entries. Controllers can overcome this by regularly checking the switches and the network for suspicious activities.

5. DoS: DoS is a major attack that has a huge effect on the performance of a network. Dos might have immense effect in SDN. It can affect the flows between switches and controllers. DoS in SDN can be directed towards the controller. An attacker can take control of switch and keep the controller busy with various queries.

6. Elevation of Privilege: In this attack, the attacker tries to increase his/her access privilege level to gain access to privileged data. Attacker might try to gain access of data and application which need special privileges.

SDN is prone to a lot of vulnerabilities, one of them being DDoS. DDoS is common, most harmful and most easy to initiate.

The rest of the paper follows this structure. In Section 2, a brief literature survey is presented. In Section 3, DDoS attack has been briefly discussed. DDoS detection and mitigation in SDN is discussed in Section 4. In the end, the conclusion is presented in Section 5.

2. LITERATURE SURVEY

Some of the paper that we studied have been discussed below.

Author Jacob H. Cox et al. [1] throws light upon the architecture of the SDN. It also shows a concern and surveys the vulnerabilities of the same. Furthermore, it also discusses the further research aspects in the SDN. Overall it gives a clear vision about the pros and cons of the SDN architecture.

The authors Kübra Kalkan, Gürkan Gür, and Fatih Alagöz [2] have discussed and categorized the solutions against DDoS attacks in SDN. The solutions are categorized based on the dependability of the aspects.

Neelam Dayal and Shashank Shrivastava [6] about the DDoS attacks in their paper, in addition to the DDoS attack, it also talks about the severity and gives a systematic classification of the attack on the SDN architecture.

Roshni Mary Thomas and Divya James [7] have used the traffic monitoring approach to monitor the network traffic for the specific amount of time to detect DDoS attack. The iftop tool is used for monitoring and Firewall is placed in POX controller. Thus, if any attacker is found, the address will be forwarded to firewall and this will detect and block the packets.

Nhu-Ngoc Dao, Junho Park, Minho Park, and Sungrae Cho [9] have implemented an idea which helps to protect the network against DDoS. By IP filtering technique and using Openflow protocol the user traffic is analyzed to detect and prevent the attack. They have defined a temple table (T table) in the controller. This method can decrease the impact of DDoS effectively only when the amount of attack traffic is not very huge.

The authors Yandong Liu et al. [8] has discussed a secure framework for mitigation of the DDoS attack using the deep reinforcement learning which can learn the different attack policies under different attack scenarios and help in avoiding the DDoS flood attack. It basically analyses the attack pattern and throttle's the attacking traffic whereas it forwards the packet coming from the benign sources. The proposed framework has two modules first an Information collection modules which uses the OpenFlow protocol and sends message in the network requesting the information related to the network traffic which is analyzed here and second a DDoS mitigation module which uses the mitigation server and the agent where the agent is a separate host which is equipped with the deep reinforcement algorithm whereas the server runs as an application on SDN. DDPG is the learning algorithm used to train the agent.

2. DDOS ATTACK IN SDN

DoS is a major attack that has a huge effect on the performance of a network. Dos might have immense effect in SDN. It can affect the flows between switches and controllers. DoS in SDN can be directed towards the controller. An attacker can take control of switch and keep the controller busy with various queries [5].

Below figure (Fig 2) shows spoofing attack. In this attack the attacker targets the server by flooding the server by sending an overwhelming amount of requests which eventually breaks down the server. As a result, the requests from the legitimate users cannot be addressed by the server leading to a DDoS attack.

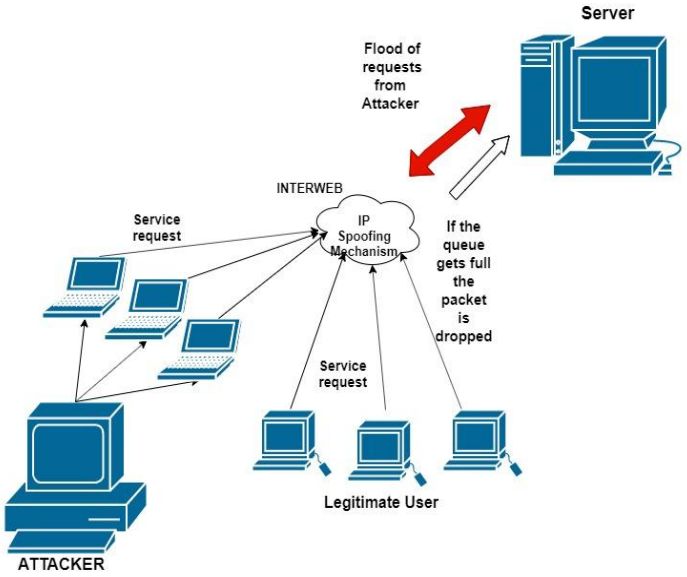

Fig -2: Spoofing Attack (DDoS)

Distributed Denial of Service (DDoS) attack is one of the severe security challenges faced by the SDN. It is a major attack, which has disastrous/catastrophic effect on the performance of the network. It disrupts the flow of the network by attacking the service nodes hence obstructing the legitimate users from getting service.

DDoS in SDN can be directed towards data plane as well as the control plane. In attack directed towards the control plane, results in keeping controller busy with requests resulting in wastage of computation time. Moreover, if the attack is on controller it can affect the whole network because controller being the heart of the network. Legitimate request might be discarded. DoS attack can be detected by the controller when a large amount of flow is detected from a single source. DoS is easy to identify. Spoofing is less effective in SDN due to continuous monitoring and updating policies. Man in the Middle (MiM) attack can be executed by taking control over a switch. Also, attacker can also enter a system by impersonating a switch. To overcome this SDN Controller should verify every switch before allowing it into the network.

DDoS attacks broadly classified into two categories DDoS attack on data plane and control plane [6].

Following figure classification of DDoS attacks.

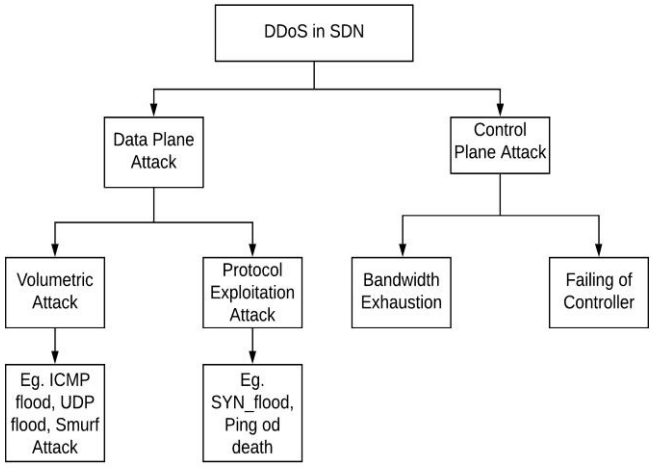

Fig -3: Classification of DDoS attacks

1.2 DDoS Plane DDoS

This category has 2 sub-categories viz, volumetric attack and protocol exploitation attack. In volumetric attack the attacker sends a huge amount of request to the victim. As a result, the victim tries to fulfil these requests eventually the victim overwhelmed by amount of packets received, hence crashes and fails to complete the requests. Basically, this attack overwhelms the victim with a large amount of request resulting in failing the server. Example of this attack is the ICMP flood, UDP flood, Smurf attack.

Whereas the protocol exploitation targets the device resources and application resources, that is it affects the main functioning of the victim by exhausting the resources such as memory, bandwidth, etc. An example of this attack is SYN_FLOOD attack where the attacker continuously sends SYN packets without waiting for the ACK from the receiver on the other hand the server keeps on allocating memory for the SYN requests eventually exhausting the memory, thus, leading to the failure of the network. Another example of this type is the ping of death.

On the other hand, the in the exhaustion application resources basically sends connection requests and eventually over burdens the victim resulting in failing to acknowledge any more connection requests

1.2 Control Plane DDoS

In this category of attack, the control plane is at a risk. The attacker sends an excessive random flow to the switch, which eventually leads to a scenario where the switch misses the attack and sends a Packet_In message, which symbolizes two things first, it cannot process the message, or it has miss a packet. The other type of attack is the one which affects the bandwidth of the OpenFlow protocol. In this case too, the Packet_In messages are sent as the controller is unable to process the request. This eventually leads to the exhaustion of the band width which brings the network down.

2. DDOS DETECTION AND MITIGATION IN SDN

Various SDN features can be used in stopping DDoS. SDN architecture offers centralized control of the network. A local controller always monitors and controls the network. The controller can take actions during abnormal network conditions. There are numerous applications used for packet capturing and traffic analysis in SDN. SDN allows us to set dynamic flow rules. Policy rules are applied to the whole network. SDN allows dynamic updating of Firewalls rules and forwarding rules.

1.2 DDoS Detection in SDN

DDoS attack floods the target with large number of packets. DDoS can be detected when the volume of packets in a network increase suddenly. There are various DDoS detection strategies based on different approaches.

A. Detection for Volumetric Attacks

Volumetric attacks include icmp flood, udp flood, smurf attack etc. In this type of large number of packets flow through the network. These types of attacks can be detected by setting a threshold. This threshold denotes the average number of packets flowing per second. If the number of packets flowing per second is more than the threshold, DDoS attack is being performed.

Chaitanya Buragohain and Nabajyoti Medhi [10] introduce FlowTrApp, a DDoS attack detection and mitigation mechanism. FlowTrApp is implemented using FloodLight Controller in mininet environment. It uses sFlow to collect flow information. Authors use flow rate and flow duration as parameters. They perform a UDP Flood DDoS attack. DDoS attack is detected by comparing the values of these parameters. Malicious devices are blocked.

Babatunde Hafis Lawal and Nuray AT [11] implement a real time detection and mitigation of DDoS attack. Authors use sFlow tool to monitor the network. They determine a threshold for packets per seconds. They perform an ICMP Flood attack. DDoS attack is detected if the number of packets flowing through the network is higher than the threshold.

B. Detection for Protocol Exploitation Attacks

Protocol exploitation attacks include SYN-Flood attack and HTTP attack. Volume of packets in this type of attack is usually less than Volumetric attack. They focus on resource exploitation of the target node. Although number of packets are less, these types of attacks are more severe on the node. Protocol Exploitation attacks can be detected by packet inspection. Packets are checked for abnormal values. In SYN-Flood attack, the MSS value in an abnormal packet is usually lower.

Authors Tushar Ubale and Ankit Kumar Jain [12] have implemented SRL, a system which provides security against TCP SYN Flood DDoS attack. This paper introduces 2 modules in SRL, Hashing module and Flow Aggregator module. Hashing module is used to remove fake values from flow table, while Flow Aggregator module is used to limit the number of requests to the server. Hence it successfully mitigates SYN FLOOD DDoS attack.

Seungwon Shin et al [13] propose AVANT-GUARD to mitigate SYN Flood DDoS. It relies on the fact that the attacker never tries to complete the TCP handshake. Attacker never sends a TCP-ACK packet. AVANT- GUARD is implemented on switches. It acts as a temporary server which accepts the TCP connection. If the connection is completed the module connects with the actual server. It then reports the failed/passed connections to the controller.

C. Detection using ML Algorithms

DDoS attacks can be detected using Machine Learning algorithms. ML is used to classify of packets. Algorithms are trained using classified dataset. After training it is capable to classify form normal to abnormal packets. Various ML algorithms are used for intrusion detection. Algorithms like Naïve Bayes, SVM, Decision Tree etc are used in packet inspection.

Saif Saad Mohammed et al. [14] propose a Machine Learning based DDoS mitigation system. Authors have used NSL-KDD dataset. An attack detection server is created to detect a DDoS attack. Naive-Bayes Algorithm is used in this paper. The classifier is trained and tested using the data provided by NSL-KDD dataset. Authentication module and Wrapper module are also included in ML Server. DDoS attacks are successfully mitigated using Machine Learning techniques.

Yao Yu et al. [15] implement a DDoS detection platform. The authors use machine learning algorithm. They depict a vehicular network in SDN. Algorithm used is SVM. Features are extracted from PACKET_IN, this data is used to train the algorithm. SVM training model is implemented in the controller. Suspicious packets are sent to the SVM model, which are classified by the model. Hence DDoS attack is detected using SVM algorithm.

1.2 DDoS Mitigation

A DDoS attack cannot be fully prevented, as sometimes legitimate clients could be mistaken as attackers. Once a DDoS attack is detected, is needs to be mitigated. DDoS can be mitigated by identifying the attacker and blocking it from making any further requests.

SDN enables us to add dynamic policies. Custom rules are added in the switches which allows us to block users. Firewalls are used to block IP/MAC addresses.

Various algorithms limit the number of requests a node can make to a server. For example, in a situation where a

client needs to have a TCP connection with the server, a limit can be decided for how many SYN packets it can send to the server in specific time period. The nodes which exceed these limits can be blocked by installing an IP/MAC based firewall rule. The node will then be blocked from making a request for a certain period.

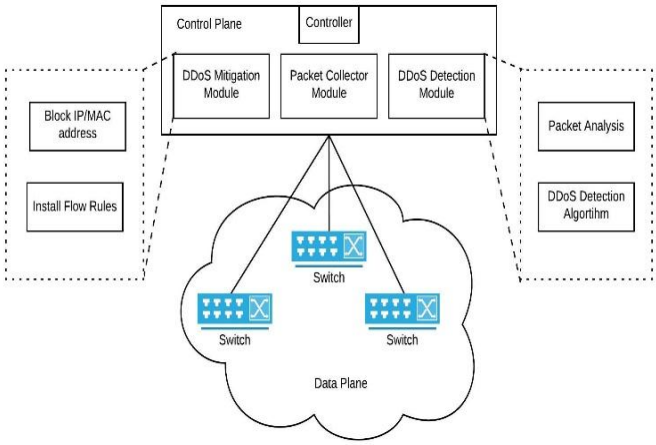

Fig -4: DDoS Mitigation architecture in SDN

Above figure shows a basic working of the mitigation architecture of the DDoS attack on control plane. There is a module in the control plane which collects the traffic flowing through the network. This data of the traffic is sent to the DDoS detection module where the packet analysis and a detection algorithm is applied to see if the network is under attack. If found that the network is under attack the mitigation module is informed about the attack and the module takes the required action against it. These actions include blocking the suspicious hosts.

2. CONCLUSION

Hence, we studied about the new and emerging technology, SDN and the threats that it comes with. In addition to this, we discussed about the DDoS attack on the SDN. Different types of DDoS attacks were reviewed. This paper reviews various DDoS detection approaches. It also throws light upon the mitigation measures taken against the DDoS on this architecture.

REFERENCES

[1] J. H. Cox et al., "Advancing Software-Defined Networks: A Survey," in IEEE Access, vol. 5, pp. 25487-25526, 2017.

[2] K. Kalkan, G. Gur and F. Alagoz, "Defense Mechanisms against DDoS Attacks in SDN Environment," in IEEE Communications Magazine, vol. 55, no. 9, pp. 175-179, Sept. 2017.

[3] Alsmadi, Izzat, and Xu, Dianxiang. (2015). "Security of Software Defined Networks: A Survey". Computers & Security, 53, 79-108.

[4] Siddhant Shah, Shailesh Bendale, "An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era.", ICCUBEA, 2019

[5] S. P. Bendale and J. Rajesh Prasad, "Security Threats and Challenges in Future Mobile Wireless Networks," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 146-150.

[6] N. Dayal and S. Srivastava, "Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN," 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bangalore, 2017, pp. 274-281.

[7] R. M. Thomas and D. James, "DDOS detection and denial using third party application in SDN," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 3892-3897.

[8] Y. Liu, M. Dong, K. Ota, J. Li and J. Wu, "Deep Reinforcement Learning based Smart Mitigation of DDoS Flooding in Software-Defined Networks," 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, 2018, pp. 1-6.

[9] Nhu-Ngoc Dao, Junho Park, Minho Park and Sungrae Cho, "A feasible method to combat against DDoS attack in SDN network," 2015 International Conference on Information Networking (ICOIN), Cambodia, 2015, pp. 309-311

[10] C. Buragohain and N. Medhi, "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers," 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, 2016, pp. 519-524.

[11] B. H. Lawal and A. T. Nuray, "Real-time detection and mitigation of distributed denial of service (DDoS) attacks in software defined networking (SDN)," 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, 2018, pp. 1-4.

[12] Ubale, Tushar & Jain, Ankit. (2018). SRL: An TCP SYNFLOOD DDoS Mitigation Approach in Software-Defined Networks. 956-962. 10.1109/ICECA.2018.8474561.

[13] Shin, Seungwon & Yegneswaran, Vinod & Porras, Phillip & Gu, Guofei. (2013). AVANT-GUARD: scalable and

vigilant switch flow management in software-defined networks. 10.1145/2508859.2516684.

[14] S. S. Mohammed et al., "A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network," 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, 2018, pp. 1-8.

[15] Y. Yu, L. Guo, Y. Liu, J. Zheng and Y. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks," in IEEE Access, vol. 6, pp. 44570-44579, 2018.