International Journal of Future Generation Communication and Networking
Vol. 12, No. 5, (2019), pp. 253 - 258

A survey of effects and detection of attacks with preventive measures to reduce DoS attacks on SDN

[1]Taskeen Fathima, [2]Dr.(Mrs.) S. Mary Vennila,
[1]Assistant Professor, Justice Basheer Ahamed Sayeed College for Women (Research Scholar, PG & Research Department of Computer Science, Presidency College) TamilNadu, India.
[2]Dr.(Mrs.) S. Mary Vennila, Associate Professor and Head, PG & Research Department of Computer Science, Presidency College, Chennai, TamilNadu, India.

Abstract: *The emergence of cloud services has challenged the advent of a digital automated society where almost everything is connected and accessible from everywhere. The traditional networks are complicated and very hard to maintain as the control plane and the data plane are put together. The SDN (Software Defined Networks) is an evolving technology that commits to transform this by separating the network's control logic from the underlying routers and switches, making the entire network centralized and creates the talent to program the network. SDN market is expanding continuously at a rapid pace. There is a demand for SDN from various evolving industries such as health care, military, manufacturing, retail and custom goods and telecommunications among many others. The separation of control plane and data plane brings new security challenges like the DoS attacks specific to OpenFlow SDN networks. The major threat faced by these services is security management. As there are numerous non-recognizable attacks against the cloud environment faced by cloud users, special attention is required for SDN control plane security. DoS attacks are considered a major threat to network, overloading the controller resulting in critical degradation of the overall network performance. This paper is focused on DoS attacks associated with SDN and proposes to work with Moving target defence (MTD) algorithm for security applications.*

Keywords: *SDN, Open Flow, Security issues, DoS attacks.*

I. INTRODUCTION

There are number of security issues that SDN faces and threats at the data plane and application plane can be controlled by network providers or network operators or application service providers. Special attention is needed for attacks on SDN control plane particularly DoS attacks [1]. SDN has advantages of central management and programmability, agility and vendor neutrality, but still has a risk of DoS. The centralized control in SDN is a risk factor because the attacker may attack the control plane with malicious packets which results in single point of failure of the control plane. The entire network will collapse if the control plane fails, SDN includes centralized control logic and separates the data plane from the control plane. Controller is the brain of SDN. It becomes easy for the network engineers to monitor the traffic and diagnose threats, insert and modify the security policies, but creates security challenges which did not exist before. A DoS attack is defined [2] as an attempt by an attacker to prevent access to online information or services to legitimate users. Coventional approaches handle DoS attacks in SDN either by dropping malicious packets or by aggregating flow rules, resulting in legitimate packet drop or loss of control over network traffic. SDN is vulnerable to various kinds of security threats such as spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege [3]. Among the other threats, DoS is the most devastating effect as it degrades the performance of SDN by increasing latency and dropping legitimate packets [4, 5]. An attacker can easily launch a DoS attack by sending useless packets with different source addresses so that the switch forwards each packet towards the controller in the form of packet-in-message [6]. This attack will overload the controller and the flow table [7]. There are many challenges when it comes to security, the reason being centralized network intelligence of SDN is vulnerable for various attacks. DDoS is a weapon of choice for hackers which cause huge revenue loss. It paralysis the networks and services by overwhelming servers and network devices with illegitimate traffic.

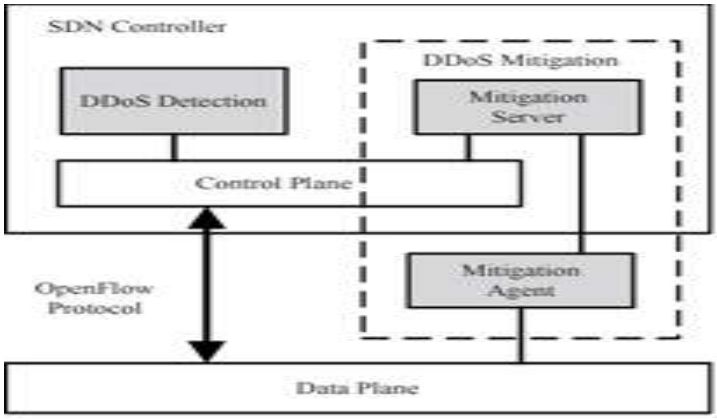

Fig. 1: SDN attack Environment

II. LITERATURE SURVEY ON THE TYPES OF ATTACKS ON SDN AND THEIR MITIGATIONS

In [18] authors have proposed such a model that is able to trace the attack source. Each device's information with its location is recorded with a controller that is used to identify the correct source of packet. At regular time interval, port statistics from each switch are retrieved, if there is any suspicious flow, it is removed from that switch's table. This proposal is good for tracking the source, but detection of exact attack traffic is not clearly specified in this proposal.

Authors in [19] used maximum entropy estimation to estimate the benign traffic distribution in order to detect network security problems in home and office networks using SDN. Traffic is divided into packet classes and maximum entropy estimation is then used to develop a baseline benign distribution for each class. Packet classes are based on protocols and destination port numbers. However, the authors only used the low rate network traffic to do the experiments as they were focused on a home environment.

Authors in [20] proposed an algorithm to realize information security management. They used algorithm based on soft computing, which was implemented for intrusion detection in SDN. Its prototype implementation consists of statistic collection, processing module and decision-making module. These modules are based on the Beacon controller in Java. The algorithm first collects and aggregates network statistical data. Then, it processes these statistical data and makes operation decisions. Finally, they train the decision-making module by applying machine learning techniques to adapt to a constantly changing environment.Authors in [21] proposed a DDoS blocking application (DBA) using SDN to efficiently block legitimate looking DDoS attacks in collaboration with the targeted servers for attack detection. The model was demonstrated to detect HTTP flooding attack. Authors in [22] proposed a system to detect DDoS attacks in the controller using entropy calculation. Their implementation depends on a threshold value for entropy to detect attacks which they selected after performing several experiments. The approach may not be reliable since threshold value would vary in different scenarios.In [23] authors proposed an entropy based light-weight DDoS detection system by exporting the flow statistics process to switches. This approach reduces the overhead of flow statistics collection in the controller, but it attempts to bring back the intelligence in network devices.

III. EFFECTS AND DETECTION OF DOS ATTACKS ON SDN

The major effect is on the control layer of the SDN architecture is the exhaustion of the control plane bandwidth by flooding the network with packets that switch had sent to the controller. For Instance, if the switch has received large number of packets in a short time and these have to be sent to the controller. This leads to heavy burden of bandwidth on the control plane which leads to delay the new flow table entries installation and the switch will not be able to forward the traffic from the new flows [8, 9].

Dos attacks on SDN Layers

SDN is actually one of the intelligent network with diverse applications which can be a target of DDoS. It consists of three functional layers, the application layer, control layer and the infrastructure layer. Potential malicious attacks can be launched on these layers.
At the Control layer, the controller is the centralized network of the SDN architecture so it is more attractive for attacks as a single point of failure for the network. The reason for this is there are many conflicting flow rules from different applications may cause the DoS attacks.
At the application layer, attacks on the application plane can affect other applications and also on the northbound API's.

Table I DDoS Attacks on SDN layers.

Plane	**Possible attacks**
Data plane	TCAM exhaustion, switch DDoS, other traditional DDoS (ICMP flood, TCP flood, TCP_SYN flood, etc.)
Control plane	Resource depletion, OpenFlow bandwidth exhaustion, amplification attacks
Application plane	Exhausting northbound API, application layer DDoS (HTTP flooding,etc)

At the data layer, attacks are possible on the switches as well as the southbound API's; the attacker can overload switch memory by producing many useless fake flow rules on the data plane. Table I presents few DDoS attacks [10] possible on various SDN layers.

IV. PREVENTIVE MEASURES FOR SDN RELATED DOS ATTACKS

There are several research works on SDN for investigating security applications to be built upon SDN controller with different aims, basically the idea here is to collect network statistics from the data plane of the network in a standardized way (using OpenFlow) and apply classification algorithm on the statistics to detect the network anomalies. If there is presence of anomaly, the application will instruct the controller to reprogram the data plane in order to mitigate. Table II. presents comparative study [11] on Mitigation of DDos Attacks on SDN.

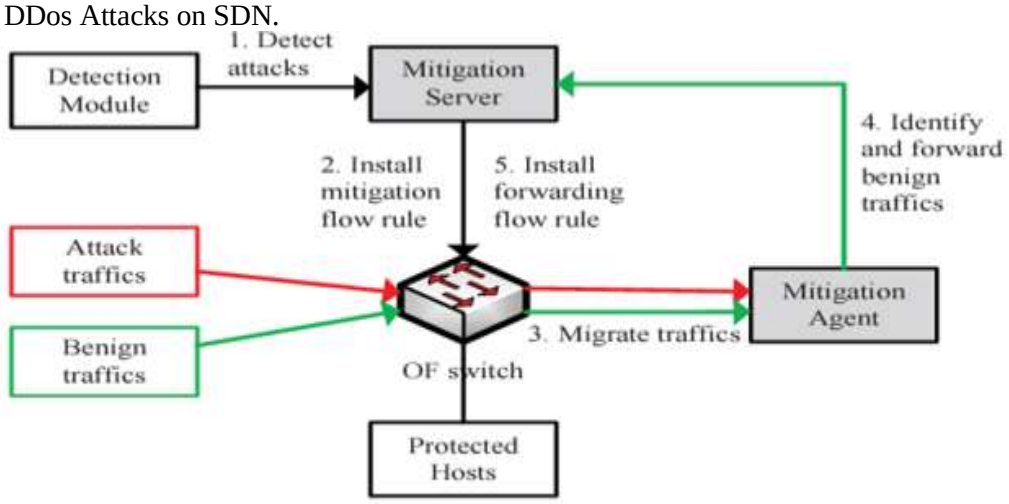

Fig. 2: Working process of DDoS mitigation module

Table II. Comparative study on Mitigation of DDos Attacks on SDN

Attack Mitigation techniques	
Drop packets [34, 59, 71] The network traffic conforming to defined rules is transmitted and	The network traffic conforming to defined rules is transmitted and remaining is dropped

remaining is dropped Block port [58, 72] The network traffic from attacking port is completely blocked Redirection [58, 66, 72] The legitimate traffic is redirected to new IP address Control bandwidth [74] The controller limits the flow transmission rate by allocating average bandwidth to each interface Network reconfiguration and topology change [58] The network controller changes the flow table on each switch to change the network topology Deep Packet Inspection [58, 72] Deep packet inspection is a process that may completely examine both header and data part of packet. Deep packet inspection enables security functions and makes it possible to detect several types of attacks including buffer overflow attacks, denial-of-service attacks, and worms and virus attacks MAC address change and/or IP address change [58, 72] When the attack is detected MAC address or IP address of the victim is changed. Legitimate traffic is routed to new address and malicious traffic it blocked Quarantine or Traffic isolation [58, 72] This mitigation technique prevents the network resource Drop packets [12,14,15]	
Block port [13,16]	The network traffic from attacking port is completely blocked
Redirection [13,16]	The legitimate traffic is redirected to new IP address
Control bandwidth [17]	The controller limits the flow transmission rate by allocating average bandwidth to each interface
Network reconfiguration and topology change [13]	The network controller changes the flow table on each switch to change the network topology
Deep Packet Inspection [13,16]	Deep packet inspection is a process that may completely examine both header and data part of packet. Deep packet inspection enables security functions and makes it possible to detect several types of attacks including buffer overflow attacks, denial-of-service attacks, and worms and virus attacks

MAC address change and/or IP address change [13,17]	When the attack is detected MAC address or IP address of the victim is changed. Legitimate traffic is routed to new address and malicious traffic it blocked
Quarantine or Traffic isolation [13,17]	This mitigation technique prevents the network resources from being overwhelmed by the volume-based attack by isolating the malicious traffic

V. CONCLUSION

The analysis identifies the centralized nature of SDN which makes it vulnerable to DoS attacks that disables the whole network or degrades the network performance. The techniques to counter DoS attacks in SDN may require complex methods, modified switches, have chances of more delay in routing process and can add more traffic to the controller for verification purpose. Another type of security application is proposed by implementing moving target defense (MTD) algorithms. MTD can be used to create an attack on the network which is more difficult than hiding or changing the key properties of the system or the network. This work is in progress. In SDN network, this is possible due to the intelligence of the centralized network.

REFERENCES

[1] Vinnarasi, Janet and Sudha, N., Security solution for SDN using Host-based IDS over DDoS Attack (September 7, 2018) International Journal of Emerging Technology and Innovative Engineering, Vol. 5, Issue 9, September 2019.
[2]US-CERT. Security Tip (ST04-015): Understanding Denial-of-Service Attacks. http://www.us-cert/ncas/tips/ST04-015.
[3] Ahamed I, Namal S, Ylianttila M, Gurtov A(2015) Security in Software defined networks : a survey. IEEE Communications Survey Tutorials 17:2317-2346.
[4] Alsmadi Izzat, DianXiang Xu(2015). Secutity of software defined networks: a survey. Computer Security 53:79-108.
[5] Imran M, Durad MH, Khan FA, Derhab A (2019) Towards an optimal solution against Denial of service attacks in software defined networks. Future Generat Computational Systems 92:444-453.
[6] Muhammad Imran, Muhammed Hanif Durad, Farruch Aslam Khan and Abdelonahid Derhab, (2019) Reducing the effects of DoS attacks in software defined networks using parallel flow installation. http://doi.org/10.1186/s13673-019-0176-7.
[7] Anand N, Babu S, Manoj B(2018) On detecting compromised controller in software defined networks. Computer Networks 137: 107-118.
[8] R. Kandoi, M. Antikainen, "Denial-of-service attacks in OpenFlow SDN networks", IFIP/IEEE International Symposium on Integrated Network Management, Ottawa, Canada, May 11-15, 2015
[9] A. Ramanathan, J. Mitchell, A. Scedrov, V. Teague, "Probabilistic bisimulation and equivalence for security analysis of network protocols", International Conference on Foundations of Software Science and Computation Structures, FoSSaCS 2004. Lecture Notes in Computer Science, Vol, 2987, Springer, Berlin, Heidelberg, pp. 468-483, 2004.
[10] Dingwen Hu, Peilin Hong, Yixin Chending, " FADM: DDoS Flooding Attack Detection and Mitigation system in software-Defined Networking:, Computer Science Published in GLOBAECOM-IEEE Global, doi: 10.1109/Glocom.2017.8254023.
[11]Narmeen Zakaria Bawany1 · Jawwad A. Shamsi1 · Khaled Salah2, "DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions ",Computer Engineering And Computer Science, Arab J Sci Eng doi: 10.1007/s13369-017-2414.
[12] 4. Giotis, K.; Argyropoulos, C.; Androulidakis, G.; Kalogeras, D.; Maglaris, V.: Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput. Netw. 62, 122–136 (2014)

[13] Chung, C.-J.; Khatkar, P.; Xing, T.; Lee, J.; Huang, D.: NICE: Network intrusion detection and countermeasure. IEEE Trans. Dependable Secure Comput. 10(4), 198–211 (2013)
[14] Dillon, C.; Berkelaar, M.: OpenFlow (D) DoS Mitigation. Technical Report (Feb 2014). http://www.delaat.net/rp/2013-2014/p42/ report.pdf (2014)
[15] Chin, T.; Mountrouidou, X.; Li, X.; Xiong, K.: Selective packet inspection to detect DoS flooding using software defined networking (SDN). In: 2015 IEEE 35th International Conference on distributed Computing Systems Workshops (ICDCSW), pp. 95–99. IEEE (2015)
[16] Xing, T.; Huang, D.; Xu, L.; Chung, C.J.; Khatkar, P.: SnortFlow: a OpenFlow-based intrusion prevention system in cloud environment. In: Proceedings—2013 2nd GENI Research and Educational Experiment Workshop, GREE 2013, pp. 89–92 (2013)
[17] Afaq, M.; Rehman, S.; Song, W.-C.: Large flows detection, marking, and mitigation based on sFlow standard in SDN. J. Korea Multimedia Soc. 18(2), 189–198 (2015)
[18] S. Luo, J. Wu, J. Li, B. Pei, "A defense mechanism for distributed denial
of service attack in software-defined networks", Ninth International Conference on Frontier of Computer Science and Technology, Dalian, China, August 26-28, 2015
[19] S. A. Mehdi, J. Khalid, S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking", International Workshop on Recent Advances in Intrusion Detection, RAID 2011. Lecture Notes in Computer Science, Vol. 6961, pp. 161-180, Springer, Berlin, Heidelberg, 2011
[20] S. Dotcenko, A. Vladyko, I. Letenko, "A fuzzy logic-based information security management for software-defined networks", 16th International Conference on Advanced Communication Technology, Pyeongchang, South Korea, February 16-19, 2014
[21] S. Lim, J. Ha, H. Kim, Y. Kim, S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks", Sixth International Conference on Ubiquitous and Future Networks, Shanghai, China, July 8-11, 2014
[22] S. M. Mousavi, M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers", International Conference on Computing, Networking and Communications, Garden Grove, USA, February 16-19, 2015
[23] R. Wang, Z. Jia, L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking", in IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, August 20-22, 2015