VOL. 13, NO. 10, MAY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

EXPERIMENTAL STUDY OF FLOOD TYPE DISTRIBUTED DENIAL-OF-SERVICE ATTACK IN SOFTWARE DEFINED NETWORKING (SDN) BASED ON FLOW BEHAVIORS

Andry Putra Fajar and Tito Waluyo Purboyo
Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia
E-Mail: an.driy@live.com

ABSTRACT

Distributed Denial of Services (DDoS) attacks are one of well-known and dangerous threats to the current network which always exists and evolves in line with the development of the network itself. Current network development has entered the Software Defined Networking (SDN) era which offers centralized control and programmability network by decoupling the network control and data plane that bring on us a dynamic, cost-effective, manageable and agile platform. On the down-side, this centralized platform can bring new security challenges such as DDoS attacks on the central controller which could compromise the entire network. The most common DDoS attack is Flood based DDoS attack. This attack is quite easy to do and very effective strikes the target. This paper offers some experimental study for detecting this kind of DDoS attack using flow behaviors to give an idea for researcher about the DDoS attack and the effect for the network.

Keywords: experimental, distributed denial of services, software defined networking.

INTRODUCTION

The emerged software-defined networking platform could change the trend of networking in the future with its promising feature that could strengthen the network security with its basic nature such as centralized network monitoring and provisioning and centralization of security and policy control which is not exist in the current network [1]. Although the SDN platform offers a great impact on security, this platform still has vulnerable side that can be exploited with malicious intent.

One of a reputable threat on the network is DDoS attacks. The generic characteristic of this attack drains the resources (bandwidth or connectivity) of network, server or application since the resources are limited in order to disrupt the service for legitimate users. Douligeris *et al.* [2] classifies the DDoS Attacks by exploited vulnerability in the following categories: flood attacks, amplification attacks, protocol exploit attacks and malformed packet attacks.

A. Flood attacks aim to deplete the victim's network resource such as network bandwidth by flooding it using User Datagram Protocol (UDP) Flood or Internet Control Message Protocol (ICMP) Flood until the victim can no longer receive the legitimate traffic. While UDP Flood [3] attack is an attack that used a huge number of UDP packets (random or same port) to overwhelming the victim (Figure-1), ICMP Flood uses the ICMP [4] (Ping) echo request packets for disrupt the legitimate traffic reach the victim (see Figure-2).
B. Amplifying the volume of attack traffic is characteristic of Amplification DDoS Attack. The attacker used other "trigger" machines to maximize the volume of attack traffic with only minimum traffic that sent to the triggered machine. Attack traffic volume from UDP based attack can be amplified, this attack is known as Smurf attacks (see Figure-3) and Fraggle attacks [6].

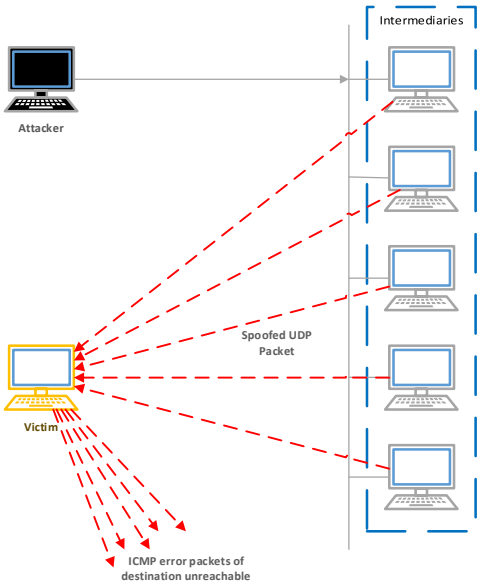

Figure-1. UDP flood attack [3].

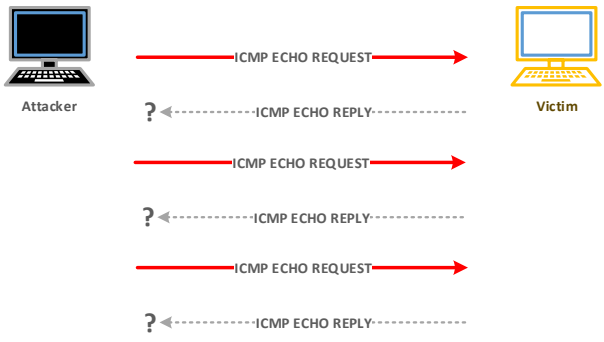

Figure-2. ICMP flood attack [4].

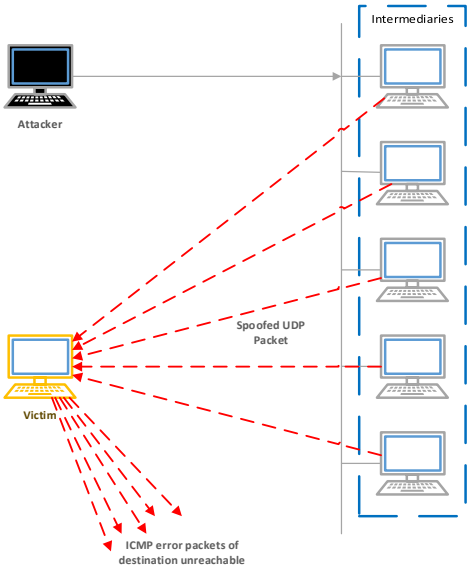

Figure-3. UDP flood attack [3].

C. Exploiting the specific feature of the protocol planted at the victim to deplete the server resource is characteristic of protocol exploits attack. One of the common attacks that exploit the protocol is TCP SYN attack (Figure 4) which exploits the three-way handshake in the TCP connection setup.
In TCP SYN attacks, an attacker sent a huge number of initial SYN request (spoofed) to the victim, then the victim replies it all with SYN/ACK to non-existent IP and waiting for the non-existent ACK. This waiting session will overload the queue buffer and make the victim unable to process other incoming connection.

D. Malformed packet attack is the type of attack that sending forged packets that will overload the victim with no use packet but must be processed and consuming the resources.

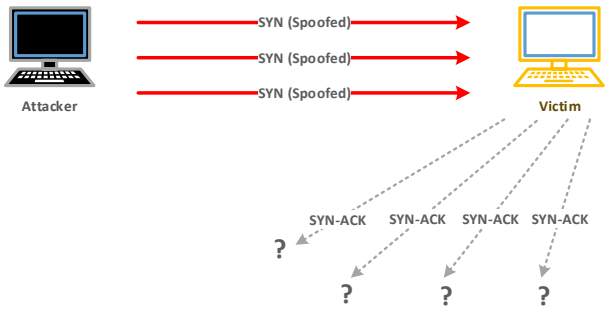

Figure-4. TCP SYN attack.

However, flood attack is the most common scenario that used by an attacker to execute the DDoS attack. In this paper, we present the detection simulation for flood type DDoS attack using flow behaviors analysis in order to ease another researcher to understand the behaviors of this attack type and its effect on the network.

METHOD

In this paper, we offer a method to detect flood type DDoS attack using industry standard flow analysis tools (sFlow) and iPerf. These tools provide some feature that can control and manage network usage especially sFlow. The method itself can be seen in figure 5. We add monitoring plane to complement the basic data plane and control plane on SDN platform. This monitoring plane that provides from sFlow used for measuring network traffic, collecting, storing and analyzing then, the result is sent to SDN controller for specifying the suitable rule policy.

EXPERIMENT SETUP

The simulation tool and another simulation environment can be seen in Table-1.

Table-1. Simulation setup.

Simulation tool	Mininet
Platform	Windows 10
OS	Ubuntu 16 VM
CPU	Intel core i7 2600k (3,4Ghz)
RAM	8Gb
SDN Controller	Floodlight
Supporting Tools	JDK 8, Ant, Atom, HPing3 Mausezahn, iPerf, sFlow

The network topology for this simulation is indicated in Figure-5. Denote the n-th host/user by hn (n = 1, 2, 3, …, 16) and s-th switch by sm (m = 1, 2, 3, 4). All of the switch monitored by sFlow and controlled by SDN controller. In order to facilitate the discussions, we restrict the topology as that shown in Figure-7.

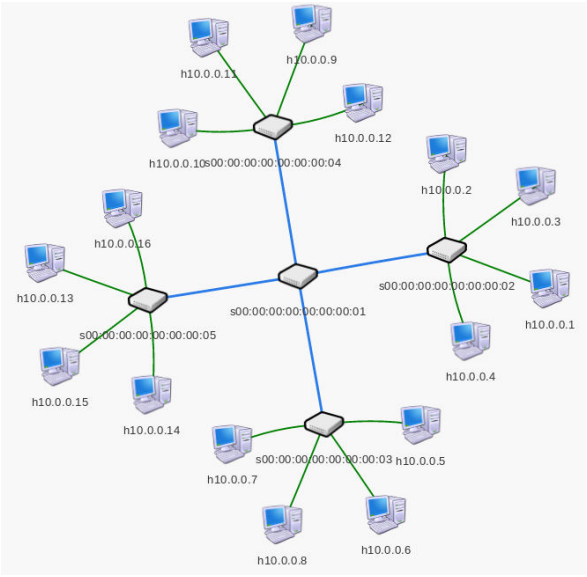

Figure-5. Network topology for simulation.

The h2 with IP 10.0.0.2 represent the attacker, h3 and h4 (10.0.0.3 and 10.0.0.4) as a legitimate user and the

victim is h1 with IP 10.0.0.1. The switch s1 monitored by sFlow in order to detect any malicious traffic.

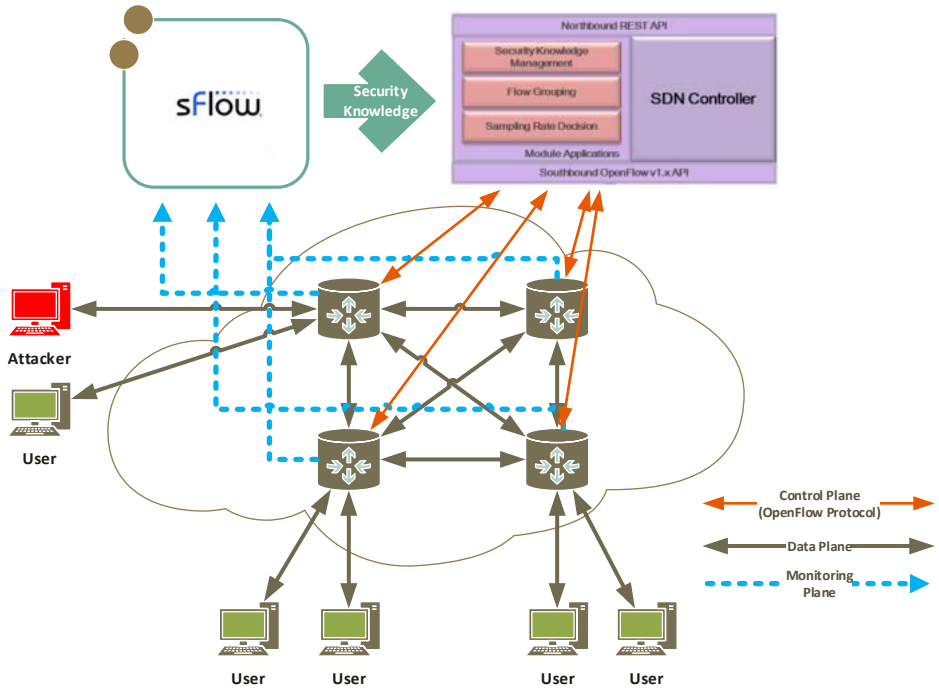

Figure-6. Simulation method.

The first simulation we will find out the TCP Throughput of the network using iPerf. After that, h2 (attacker) send malicious traffic to h1 and the maximal TCP throughput and latency will calculate again.

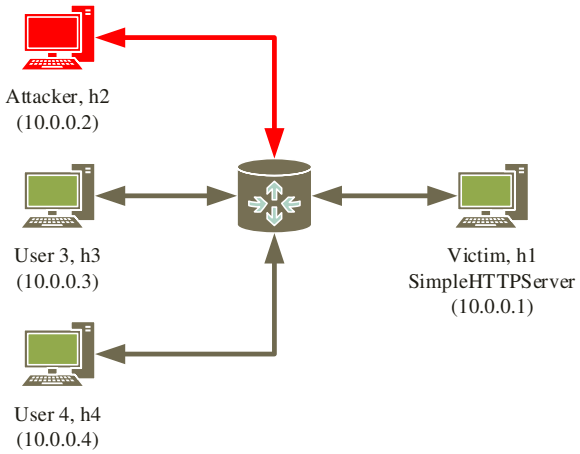

Figure-7. Restricted topology.

The h2 with IP 10.0.0.2 represent the attacker, h3 and h4 (10.0.0.3 and 10.0.0.4) as a legitimate user and the victim is h1 with IP 10.0.0.1. The switch s1 monitored by sFlow in order to detect any malicious traffic.

The first simulation we will find out the TCP Throughput of the network using iPerf. After that, h2 (attacker) send malicious traffic to h1 and the maximal TCP throughput and latency will calculate again.

RESULT

Simulation 1: TCP throughput each user

Based on topology on Figure-2, we find out the total TCP bandwidth between h1 and h2, h3, h4 using iPerf. The TCP server represented by h1 using the default port, default TCP window size (86, 3 KByte), and the interval is 1 second. H2, h3, and h4 test the consecutive TCP Throughput to h1 and the result can be seen in figure 8 below:

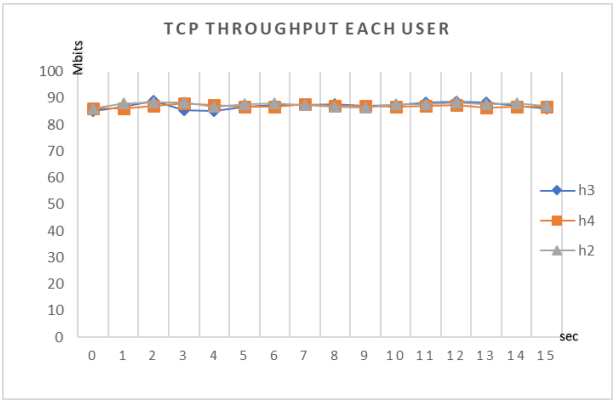

Figure-8. TCP throughput for each hn.

h2, h3, and h4 similarly have the same TCP Throughput which is 88 Mbits/sec because we set the bandwidth link at 100 Mbits/sec. This scenario match with RFC 6349 [7]

which is for 100 Mbits/sec has maximum achievable TCP throughput at 94,9 Mbits/sec.

Simulation 2: Legitimate Traffic vs TCP Flood attack.

In this step, h3 and h4 will send constant 10Mbits traffic to h1 for 50 s. After 20 s, h2 execute attack traffic to h1 and stop the attack at 40 s. The result of this simulation can see in Figure-9.

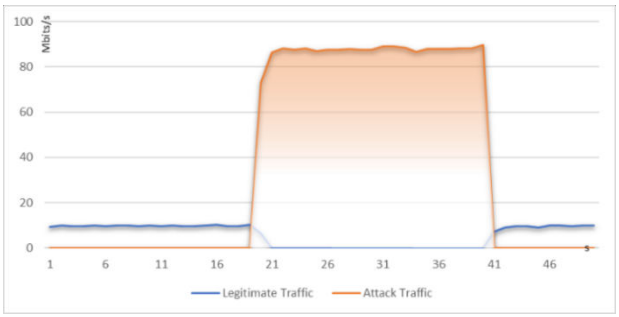

Figure 9. Legitimate vs attack traffic.

In Figure-9, we can see that the legitimate traffic constant at 10 Mbits/sec until 20 s. After an attack was executed at 20 s, the legitimate traffic drops to almost 0 Mbits/s until the attack was stopped. From this simulation, we can assume that the attack traffic consumed all of the TCP throughputs and inflict the link for h3 and h4 to h1 temporary down, see Figure-10. Both h3 and h4 could not get the ping reply from h1 during the attack (delay 20ms).

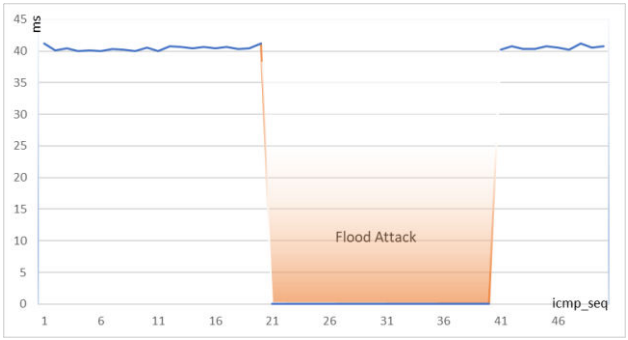

Figure-10. ICMP to h1.

Simulation 3: UDP throughput vs UDP flood attack

In this simulation, UDP Throughput will calculate using IPerf. This calculation will take before and during UDP Flood attack. In Figure-11 we can see the UDP Throughput have constant values without the attack. This throughput dropped during the attack at around 38 Mbps and may not reach 0 Mbps like TCP because UDP is connectionless protocol so the sender still sends the packets without acknowledgment from the receiver although the receiver does not receive the packet [8].

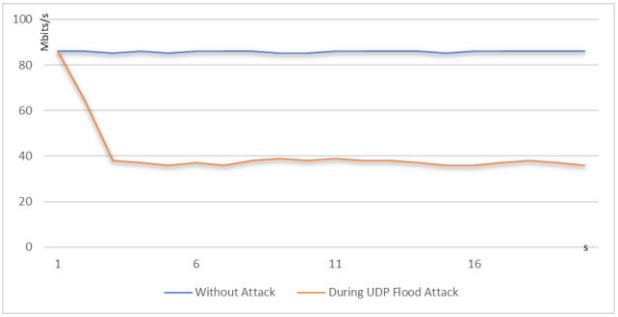

Figure-11. UDP throughput without and during UDP flood attack.

CONCLUSION AND FUTURE WORK

In this paper, we performed a flood type of DDoS attack on SDN platform simulation. The result of this simulation can be used as an overview to identify behaviors of flood type DDoS attack and the effect for the network. Actually, “distributed” DoS attack is performed by a lot of host/attacker, but in this simulation only performed by only one host (h2) however, it can represent the implication of the distributed DoS attack.

Flood type DDoS attack commonly drains the network resource so that other legitimate user could not get normal services from the network. With SDN feature, this type of attack is easy to detect and identify from its traffic which is have anomaly such as large bursty traffic.

For the future work, intrusion detection can be implemented for this kind type of attack based on traffic flow behaviors. Moreover, the defense mechanism could repeal all of type DDoS attack.

REFERENCES

[1] N. McKeown and T. Anderson. 2008. OpenFlow: Enabling Innovation in Campus Networks. ACM SIGCOMM Computer Communication Review.

[2] A. M. Christos Douligeris. 2004. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks. 44: 634-666.

[3] S. S. Kolahi, K. Treseangrat and B. Sarrafpour. 2015. Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13. In International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah.

[4] Harshita. 2017. Detection and Prevention of ICMP Flood DDOS Attack. International Journal of New Technology and Research (IJNTR). 3: 63-69.

[5] CERT/CC. Smurf IP Denial-of-Service Attacks. 13 March 2000. [Online]. Available: https://www.cert.org/historical/advisories/CA-1998-01.cfm?

[6] S. Kumar. 2007. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification on Internet. in Second International Conference on Internet Monitoring and Protection (ICIMP 2007), California.

[7] Constantine and e. al. August 2011. RFC 6349 Framework for TCP Throughput Testing. [Online]. Available: https://tools.ietf.org/html/rfc6349#section-3.2.2.

[8] S. S. Kolahi and P. Li. 2011. Evaluating IPv6 in Peer-to Peer 802.11n Wireless LANs. IEEE Internet Computing. 15(4): 72.