Mitigation of a combined DDoS attack on a Primary Server and SDN Controller Using Multi Layer Fair Queuing with priority on traffic variation

Sanjeetha.R, Rishab Pokharna, Shikhar Srivastava, Anita Kanavalli
Department of Computer Science and Engineering,
Ramaiah Institute of Technology
Bangalore, Karnataka, India
sanjeetha.r@msrit.edu

ABSTRACT

Distributed Denial of Service (DDoS) attacks on primary servers have various solutions today. However in a Software Defined Network (SDN) setting, a DDoS attack on a primary server could also bring down the SDN controller if the flow tables on the switches get compromised (Combined DDoS attack). All traffic from the compromised switches would flow to the controller which may repeatedly install the same rule into the compromised switch's flow table thereby spending all its resources on handling the traffic from the compromised switch.

In this paper we propose a solution to mitigate this combined DDoS attack by using Multi Layer Fair Queuing that prioritizes the switch queues based on the traffic variation so that normal packets are processed with high priority and attacker packets are processed with low priority thereby mitigating combined DDoS attack on primary server and SDN controller.

KEYWORDS

SDN, DDoS, Multi Layer Fair Queuing, Controller.

1 INTRODUCTION

SDN is a new network architecture that separates the data plane from the control plane. The SDN controller implements the control plane and is responsible for making forwarding decisions and installing rules in the flow table. The network devices like hubs, switches and routers implement the data plane. They simply forward the packets based on the rules installed in their flow table. SDN has a logically centralized controller which installs flow rules into the flow tables that are present in forwarding switches. When a switch receives a packet from a host, it refers to its flow table to decide the action to be performed viz., forward to a port or drop, in case it does not have any matching flow table entry, by default the switch forwards the packet to the controller. The controller receives the packet from switch and decides the action that has to be performed and installs this as a flow table rule into the switch which had forwarded the packet and also installs the same rule into all other switches in the network for consistency [1].

2 BACKGROUND

2.1 DDoS Attacks on Primary Server in SDN

In [2] *S. Lim et al.* discuss DDoS attack on a primary server in SDN that is performed using botnets that send unnecessary traffic to the victim primary server. When the primary server's resources get exhausted during such attack, it sends the notification to a DDoS blocking module (DBA) that is run on the controller and shuts down. The legitimate clients and botnets now send request to controller, to install rule containing destination IP address of the primary server. The DBA now provides the IP address of a redundant backup server such that only legitimate clients will be able to understand the new address for ex. using CAPTCHA. The botnets fail to interpret the IP address of the new primary server, but the legitimate clients will continue getting the service.

2.2 DDoS Attacks on SDN Controller

In [3] *Jeremy M. Dover* has demonstrated how a vulnerability of Open Floodlight controller allows an attacker in the same network to deny communication between a legitimate switch and the controller. The attack is performed by spoofing the datapath_id or dpid of a legitimate switch. Initially the switch initiates the TCP session to port 6633 on the controller, and maintains this session. The attacker switch spoofs the dpid of the legitimate switch and connects to the controller; the controller terminates the connection with the original switch, and establishes a new connection with this attacker switch. This degrades the performance of the network as the legitimate switch's flow table rules expire. Though the legitimate switch tries to re-establish its connection with the controller, the attacker switch also does the same with much less time interval.

2.3 Combined DDoS attack on the Primary Server and SDN Controller

As discussed in the introduction, when a switch receives a packet from a host and does not find any matching entry in its flow table, it forwards the packet to the controller. The controller then creates a flow rule for that packet and inserts it into the flow table of the requesting switch. This entry is given an idle and hard time out till which the entry is valid. Idle timeout indicates the time after which the entry is removed if there are no incoming packets matching the flow rule. Hard timeout indicates the time after which the entry is removed from the flow table irrespective of whether the incoming packets match the rule or not. The timeout range is anywhere between 0 and 65535.

To perform a combined DDoS attack on both primary server and controller, the attacker can compromise few switches in SDN by running a malicious code that alters the idle or hard time out of its flow table entries to zero thereby invalidating the flow table rules. This results in the switch sending all incoming packets to the controller as there is no matching valid flow entry. The controller now becomes busy in installing the flow rules of the compromised switches thereby exhausting its resources, which could otherwise be used to prevent DDoS attack on a primary server.

In this paper we propose a solution to mitigate this combined DDoS attack by using Multi Layer Fair Queuing that prioritizes the switch queues based on the traffic variation i.e. the packets having different destination IP addresses.

We assume that the attack traffic packets have low variation in destination IP addresses mainly because of two reasons

Multiple packets are sent to the same primary server being attacked by normal switches

Multiple requests will be sent by the compromised switch for the packets with the same destination IP address as the previously installed rule for the same is immediately invalidated. Generally any traffic flow will contain multiple packets being sent to the same destination host.

As opposed to this, normal traffic will have high variation in destination IP addresses.

3 PROPOSED SOLUTION

3.1 Mitigating Combined DDoS attack on primary server and SDN Controller

As discussed in section 2.3, in our paper we propose a solution for mitigating combined DDoS attack on primary server and SDN Controller based on the concept that the attack traffic will have low variation of IP address and normal traffic will have high variation. The solution is summarized as follows:

- Initially the requests coming from switches are put in its corresponding queue and are processed in round robin fashion giving equal priorities to all the switch queues.
- The traffic in each switch queue is observed for some period of time (one cycle) and the overall mean and standard deviation are calculated based on the destination IP address.
- The process is repeated for second cycle. The difference in variation of each switch queue and overall mean *dv* is calculated as *dv = abs(variation of traffic in switch − mean)* and compared with the standard deviation

  i. If *dv* is less than the standard deviation, its priority is decreased

  ii. If *dv* is greater than to the standard deviation, its priority is increased

  iii. If *dv* is equal to the standard deviation, its priority remains the same
- Using this method, the switch queues containing high variation (normal traffic) will eventually get high priority and the switch queues containing low variation (attack traffic) will get low priority. This way the combined DDoS attack on primary server and controller is mitigated.

REFERENCES

[1] Goransson, Paul, Chuck Black, and Timothy Culver. *Software Defined Networks: A Comprehensive Approach.* Morgan Kaufmann, 2016.

[2] Lim, Sharon, J. Ha, H. Kim, Y. Kim, and S. Yang. "A SDN-oriented DDoS blocking scheme for botnet-based attacks." In *Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on*, pp. 63-68. IEEE, 2014.

[3] Dover, Jeremy M. "A denial of service attack against the Open Floodlight SDN controller." Research Report, Dover Networks LLC. Mary Land, US. 2013