DDoS attack solutions in SDN Network using OpenFlow

Introduction

SDN is a paradigm which allows us to view the network in two logically separate entities- the logic (control plane) and logistics (data plane). In this approach, the burden of computation which is normally distributed in conventional networks among the network devices is brought together in a single controller leaving the switches with minimal responsibility of forwarding the data packets across.

While this central view of network sounds promising in providing better configurability and management of network, it also stands the risk of being a 'Single Point of Failure (SPoF)'. Moreover, as the SDN architecture in itself does not provide any security feature, it is as vulnerable to all kinds of attacks as any conventional network. In our project, we focus on appropriate forwarding and mitigation mechanisms against DDoS (Distributed Denial of Services) attacks on switches, controllers. We will be looking for an appropriate mechanism for detecting UDP flooding, TCP-SYN flooding attack.

Problem Description

As discussed earlier, SDN does not inherently support security. Among the current security problems, one of the most urgent and hardest security issues is Distributed Denial of Service (DDoS).

There are several security issues to SDN due to DDoS attacks such as exhaustion of the memory of switch and controller, the control channel bandwidth and the computational power at data and control plane. Such attacks are made into effect by several DDoS techniques like SYN flooding, UDP flooding and botnets.

A SYN flood (half-open attack) is a type of denial-of-service (DDoS) attack which aims to make a server unavailable to legitimate traffic by repeatedly sending initial connection request (SYN) packets. UDP flooding occurs by sending enormous UDP packets with random port numbers for which the target system generates ICMP packets and eventually runs out of resources. DDoS attacks are also carried by botnets which are the collection of compromised zombies, and on the commands of the attacker it can send huge amounts of data to the target server.

There have been many studies about DDoS attack detection in SDN which need inspection of all the packets or collect all the flow entries in switches. In this project, we focus on mitigating aforementioned attacks using the features of SDN controllers in a better way which involves relatively less computational effort to detect the DDoS attacks.

Motivation and Challenges

Software Defined Networking (SDN) and OpenFlow have emerged as a new paradigm of networking. SDN gives network owners and operators more control of their infrastructure, allowing customization, optimization and overview of the network, thus reducing the overall capital and operational costs. Finding an efficient detecting and forwarding mechanism that makes best use of the capabilities of SDN is an open research avenue.

SDN being entirely a new architecture, research and implementation is still in its initial stages. It involves understanding the current design and programming the controller such that it helps to identify and mitigate the DDoS attack. The major challenge would be implementing the forwarding logic upon detecting the flooding of OpenFlow switches and controllers in the SDN network.

Proposed Idea

As discussed, the detection mechanism will make use of less computational overhead for a sudden change in the incoming flow of packets. We propose to exploit the global view of the network that SDN controller offers to detect a potential DDoS attack. The Packet_In event which is generated every time a new packet request arrives at a switch is the key here- instead of heavy analysis of all network parameters, we simply count the Packet_In events to derive the packet rate in any link. An abrupt increase in this event count, say more than 100 per second is an alarm- a possible DDoS attack. As this is detected, we will change the “action” field of the flow table entry in the concerned switch to drop those packets instead of forwarding. The proposed detection mechanism will be simulated in mininet using OpenFlow protocol.

Through the project we hope to shed some light on possible detection and prevention mechanisms to overcome problems created by flooding of network elements in the SDN environment. Future challenges are to trace the attack source, distinguish between a DDoS attack and legitimate requests (during peak business hours) and create a complete DDoS attack defense system using efficient algorithms.

References

[1] Nisha Ahuja, Gaurav Singal Department of CSE, Bennett University, Greater Noida, India “DDOS Attack Detection & Prevention in SDN using OpenFlow Statistics” 2019 *9th International Conference on Advanced Computing (IACC)*

[2] Nick McKeown et al., ”OpenFlow: enabling innovation in campus networks”. ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74 , April 2008.

[3] Xiang You, Yaokai Feng, Kouichi Sakurai, Kyushu University, Japan, “Packet In message based DDoS attack detection in SDN network using OpenFlow” 2017 *Fifth International Symposium on Computing and Networking*

Tools

Mininet, POX Controller