Anti DDoS Bloom Filter in SDN MiniNet POX Simulation

Yuhan Xu

Shanghai Jiao Tong University
ens@sjtu.edu.cn

Abstract

This report demonstrates what I have done in the Project-2 Secured Multicast in Datacenter Network (DCN) implemented with SDN in the Wireless Communication and Mobile Network Course. In this article, I use the basic idea of applying in-packet Bloom Filter into Software Defined Netwoking (SDN) to resolve the security issue in DCN. I use Python to simulate the basic model of Bloom Filter and compare Double "10" Bloom Filter to Single "1" Bloom Filter to demonstrate a method that could improve the accuracy of filtering DDoS attack from zombie network. What's more, I also use the MiniNet+POX platform to set up a 5-switcher-SDN topology, base on which future work of applying Bloom Filter on SDN to defend virtual network fom DDoS attack in MiniNet could be done.

I. Introduction

The Datacenter Network (DCN) is the fundamental infrastructure for cloud computing, where the one-to-many communication paradigm has been very popular in many DCN services. However, the recently proposed multicast mechanisms for DCN could be subject to Distributed Denial of Service (DDoS) attacks. To resolve the problem, we use in-packet Bloom Filter in Software Defined Network (SDN).

In the first section of this article briefly explained the basic concept of Software Defined Network, DDoS attack and Bloom Filter.

The second section introduced simulation of the Bloom Filter with Python and the compare result between Double "10" Bloom Filter and Single "1" Bloom Filter. The Bloom Filter was defined using MD-5 hash functions. Matlab was used to analyse the statistical result.

The third part presented how to set up a topology of 5-switcher-SDN topology in MiniNet. The last section gave the work that about to be done in future.

II. Basic Concept

I. Software Defined Network (SDN)

SDN is a type of network architecture that separates the network data plane. The separation of the network's data plane and control plane allows a network operator to control network behavior from a single high-level control program so that the switches in data plane can be directly programmable. Deployments of software define networking are often used to solve a variety of network management problems in real networks.[1]

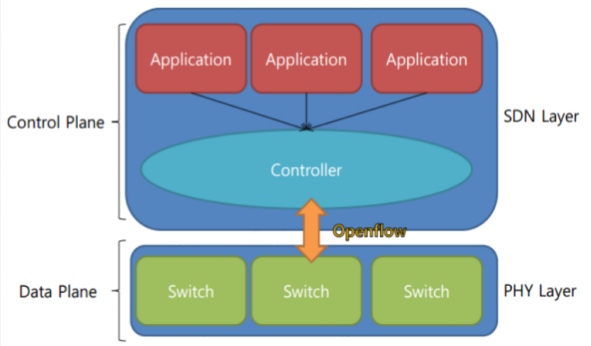

Fig.1 SDN sytem architecture[1]

II. Distributed Denial of Service (DDoS) attacks

DDoS attacks overwhelm the target system with data, such that the response from the target system is either slowed or stopped altogether. In order to create the necessary amount of traffic, a network of zombie or bot computers is most often used. Zombies or botnets are computers that have been compromised by attackers, generally through the use of Trojans, allowing these compromised systems to be remotely controlled. Collectively, these systems are manipulated to create the high traffic flow necessary to create a DDoS attack.[2]

III. In-packet Bloom Filter

A Bloom filter is a simple space-efficient randomized data structure for representing a set in order to support membership queries. Bloom Filters allow false positives but the space savings often outweigh this drawback when the probability of an error is controlled. Bloom Filters have been used in database applications since the 1970s, but only in recent years have they become popular in the networking literature.[3]

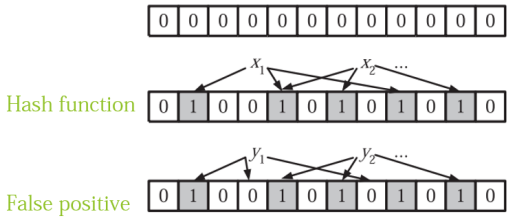

Fig.2 Bloom Filter[3]

In this article we use MD5 hash function to establish Bloom Filters. The Bloom Filters stored in the switches represent the IP of nodes and the Bloom Filters stored in the data packets represent the IP of source node and the destination nodes.

For Bloom Filter possesses following basic character:
A Bloom Filter of n element is described by an array of m bits, initially all set to 0. If it uses k independent hash functions and assume that hash functions map each item randomly.
The False positive rate is

$$F = \left(1 - e^{-\frac{kn}{m}}\right)^k$$

To achieve the minimize F, the number of independent hash functions k should be

$$k = \frac{m}{n} \ln 2$$

III. Simulation of Single and Double Bloom Filters with Python

I. Principle

In our experiment, Single Bloom Filter in the switch use one 128 bit array to do Bit-OR to all the IP of nodes, while in Double Bloom Filter we use two 128 bit array to document both Bit-OR and. Obviously, the Double Bloom Filter can add accuracy of filtering by decreasing the false positive rate, see Fig.3.

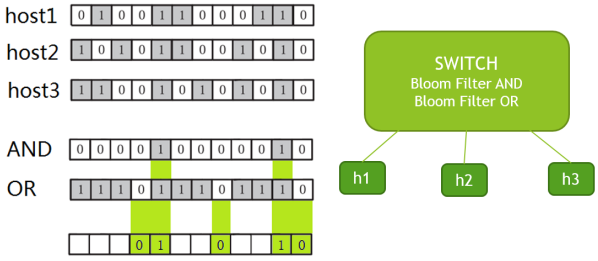

Fig.3 Double Bloom Filter Principle

II. Simulation Model and Parameters

We setup a single switch model to test the false positive rate of both 128 bit Single Bloom Filter and 256 bit Double Bloom Filter in the switch, see Fig.4. MD5 hash functions are used to setup Bloom Filters.
The host number linked by the switch range from 2 to 13. And we randomly choose the destination IP and test 800 times to check whether the DDoS attack can successfully affect the host through Bloom Filter in the switch.

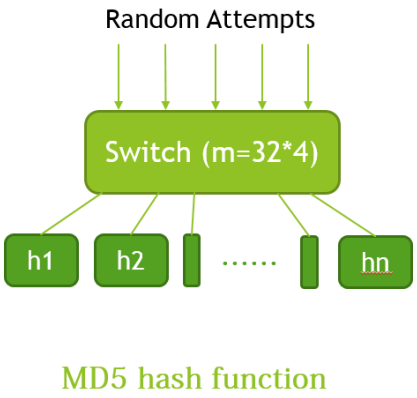

Fig.4 Experiment Model of Bloom Filter

III. Result and Analysis

The model was written in Python and the results are collected and drawn by Matlab, see Fig.5.

We can clearly see that the false positive rate of Double Bloom Filter(dark green) is lower than Single Bloom Filter(green) . And the 128-bit-MD5 Double Bloom Filter performs pretty well when the host number is under 6(the false positive rate is under 0.04). The false positive rate is close to 1, when host number is above 8 because the Bloom Filter array is almost straight '1' bit after doing Bit-OR for 8 IP address.

We also tried 'SHA1' and 'SHA224' instead of 'MD5', the upper bound of 128-bit Bloom Filter is 8 IP address as well.

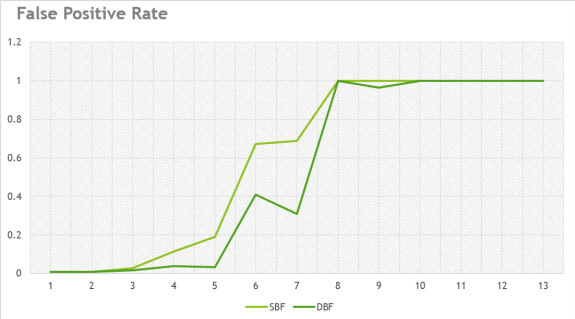

Fig.5 Simulation Result

IV. Mininet POX Experiment

I. Introduction of Mininet

Mininet is a network emulator. It runs a collection of end-hosts, switches, routers, and links on a single Linux kernel. It uses lightweight virtualization to make a single system look like a complete network, running the same kernel, system, and user code. [4]

Because you can easily interact with your network using the Mininet CLI (and API), customize it, share it with others, or deploy it on real hardware, Mininet is useful for development, teaching, and research.[5]

Mininet provides a simple?network testbed. In this article we use POX as the programming language based on Python.

II. Simulation Model

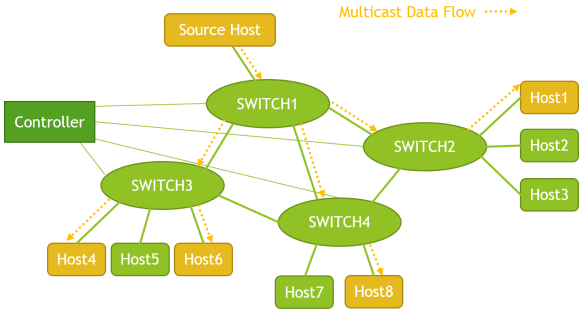

Fig.6 4-Switches-9-hosts topology

We setup a 4-Switches-9-hosts topology to test whether the Double Bloom Filter can work well on the virtual natwork and anti DDoS attack. The source host send multicast data flow to host1, host4, host6 and host8.

In the switches, Double Bloom Filter stores the IP addresses of directly-linked hosts and switches. Once the source send out data flow packed with destination IP address, the Bloom Filter filtering the data packet and send the data to the destination host.

III. Topology and Test

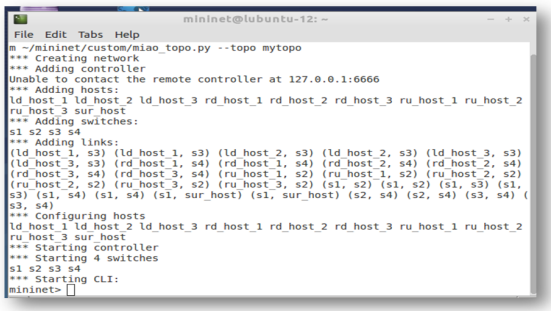

Fig.7 Topology simulation on Mininet

Fig.8 Programming on POX

IV. Future Work

- Programming on switches and control, such as changing destination address of data flow;
- The topology above is static, however, in the real world, the topology is dynamic. The control should figure out when a host leave or add in the topology, and changing the Bloom Filter in the switches. What's more, routing algorithm can be added to dynamically find the best routine to transfer packets.
- When malicious customers existing in the topology, DDoS attack should be take into consideration, see Fig.7. Control should be able to find the infected hosts and filter normal packets from infected malicious DDoS attack packets.

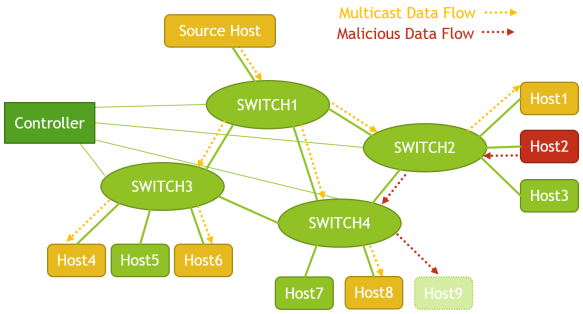

Fig.7 Topology with Malicious host

References

[1] Software Defined Networking, Dr. Nick Feamster from GECH, *Cousera*.

[2] What is a DDoS attack? Mary Landesman, *http://antivirus.about.com/od/whatisavirus/a/ddosattacks.htm*

[3] A. Broder and M. Mitzenmacher. Network applications of bloom filters: A survey. *Internet Mathematics*, 1(4):485-509, 2005.

[4] Introduction to Mininet: What is Mininet? Bob Lantz, Nikhil Handigol, Brandon Heller, and Vimal Jeyakumar *https://github.com/mininet/mininet/wiki/Introduction-to-Mininet#what*,1:1-5, 2 May 2014.

[5] Mininet: An Instant Virtual Network on your Laptop, *http://mininet.org/*