Software-Defined Networking - DDoS attack detection using Entropy Method

Dr. Chao-Li Tarng, Pranusha Boinpally, Amit Chaudhary

Department of Electrical Engineering, San Jose State university, San Jose, California 95192.

Introduction

SDN is an approach to networking in which data plane and control plane works separately. It has a centralized control console and easily programmable & manageable.

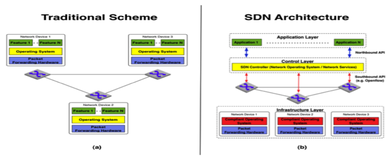


Figure 1: Architecture of Traditional Network vs. SDN

Though Software Defined Networking is a innovative way of managing modern networks, security is the big concern. DDoS, Man in the middle and ARP spoofing attacks are few of the attacks that can compromise the network security. Controller, the brain of the network should be protected from the attacks before it brings down the whole network. So research is being done to protect network controller, the main component in the architecture.

This project work shall contain the information of the security behavior of different topologies in the network and also emphasizes the observation and prevention of DDoS attacks using entropy method..

Methodology

Custom Topologies

As real networks are more complex mininet is used to create topologies using python code.

Cost is reduced with virtual networks and accommodate feasibility. For the maximum throughput controller performance can be enhanced by the calculating the network parameters in various modes.

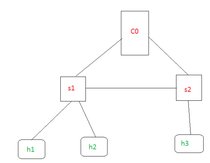


Figure 2: 3 Host- 2 Switch Topology

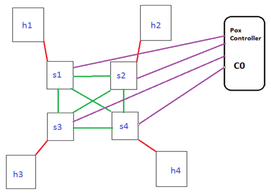


Figure 3: 3 Loop Topology

Methodology

Spanning Tree Algorithm is used to avoid multiple loops in mesh topology.

POX remote controller is used in following two modes

- Hub mode
- Learning switch mode

These topologies are used to test the network attack behavior.

DDoS Detection:

A DDOS attack uses many computers or internet connection to exhaust any server/host and it is very critical than DOS attacks. DDOS could be performed by making Zombies, Zombies are made by DDOS Attacker and group of Zombies are called Robot network or Botnet. DDOS attack could also be performed by using different tools i.e. LOIC, XOIC, HULK, TOR's Hammer etc.

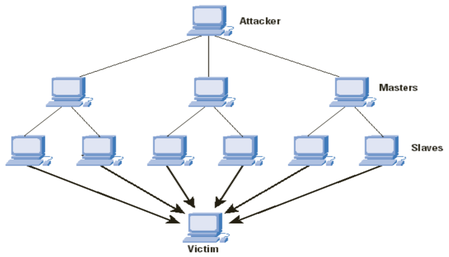


Figure 4: A DDoS Attack [13]

ENTROPY FOR DDoS DETECTION:

The main motive to use the entropy is to detect the DDoS attack at early stages. How early the attack should be detected is depends on the capacity and tolerance of the system. Using Entropy the attack can be detected in few hundred packets and can perform mitigation techniques to make the attack less effective. This is a lightweight technique to detect the attacks and that is too at early stages.

Using entropy randomness in a network can be measured. Let W is the data with n elements, H is the entropy and probability of event x is shown below:

$$W = \{x_1, x_2, x_3, \ldots, x_n\} \qquad p_i = \frac{x_i}{n} \qquad H = -\sum_{i=1}^{n} p_i \log p_i$$

In this project two hash tables are maintained, one contains the count of DPIDs and other one contains count of destination IP addresses. Every time it gets any entry it updates from which switch it is getting this packet and what is the destination of the packet. On the basis of these two entries the entropy can be calculated and can set a threshold entropy value, if the value of entropy goes lower than the minimum entropy value, it could be assumed an attack.

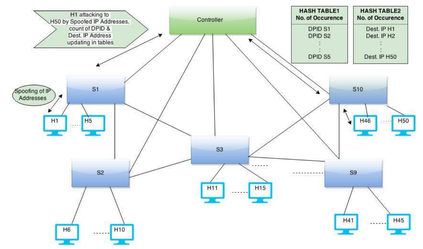
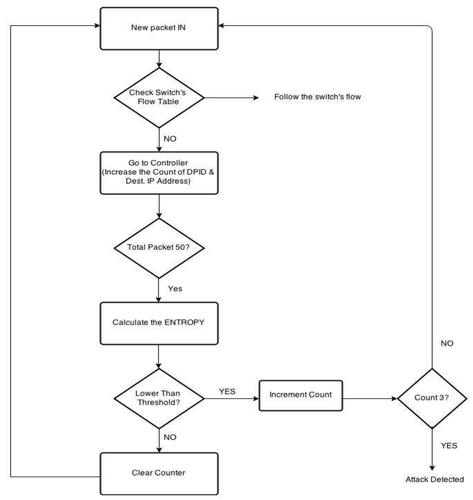


Figure 5: Controller maintaining table for DPID and Dest. IP Addresses

Flow Chart:



Results

Custom Topologies: Maximum Throughput: Performance parameters, ping time, bandwidth etc. are calculated using controller on various complex networks and in different nodes. Hub mode provides maximum throughput and better performance when compared to learning switch mode.

DDoS Detection: When randomness is high then entropy would be maximum and when randomness is less in that case entropy would be lower. On the basis of entropy, a threshold can be set and if the value of entropy goes lower than threshold, attack can be considered.

Summary

Controller is the important component in the SDN networks and making it robust is the most challenging thing. DDoS is a big threat for any traditional or SDN network but in SDN it plays a more crucial role as controller is the backbone of the whole SDN network and it aims to down the controller. By using the entropy method the DDoS attacks can be detected as early as possible and controller can perform better as well as the overall system performance would be better.

Key References

[1] Chandan Pal, Veena S, Ram P. Rustagi and K.N.B.Murthy, "Implementation of Simplified Custom Topology Framework in Mininet", APCASE. (2014). Retrieved February 2015, from http://ieeexplore.ieee.org.libaccess.sjlibrary.org/stamp/stmp.jsp?tp=&arnumber=6924470&tag=1

[2] "Software Defined Networks", White paper, ONF (2012, April, 13). Retrieved December , 2014, from https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

[3] A research paper on Early Detection of DDoS Attacks in Software-Defined Networking by Seyed Mohammad Mousavi.

[4] A blog on "DDoS Attacks" by Imperva. https://www.incapsula.com/ddos/ddos-attacks/

Acknowledgements

We would thank our family and friends who were a constant support during our project period. We would like to thank our project advisor Prof. Chao-Li Tarng for his guidance and support. Thanks to Prof. Nader Mir, Prof. Thuy Le for guiding in every step towards completion of our master's project and entire Electrical Engineering Department.