

CO-368 Internet technology and Application

Analysis of DDoS Attacks in SDN Environments

Team

Aswanth P P 15CO112

Md. Ameen 15CO131

Joe Antony 15CO220

Overview

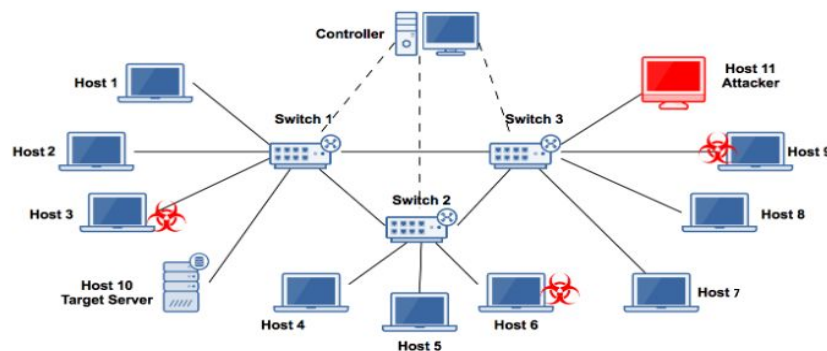
In this project we are trying to analyse the DDoS attack on SDN environment based on the journal “**A Novel DDoS Attacks Detection Scheme for SDN Environments**” by Di Wu (Department of Computer Science University of Tsukuba, Japan) , Jie Li (Department of Computer Science University of Tsukuba, Japan) , Sajal K. Das (Department of Computer Science Missouri University of Science and Technology, USA) , Jinsong Wu (Department of Electrical Engineering University of Chile, Santiago, Chile) , and Yusheng Ji §(Information Systems Architecture Research Division National Institute of Informatics, Japan).


A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. We are trying to analyse this effect on SDN environments.

Design

1. Setup test environment

We set up a test environment by using mininet, creating a small scale network of ring topology consisting of three switches and 11 nodes (which could be a terminal or another network) directly connected to switch.





There are 11 hosts in this network, so that there could be 11 origin nodes, and 11 destination nodes, although the origin node cannot be the same as the destination node. We choose such kind of network because it is one of the most popular topologies, and switches could connect with each other directly.

2. Launch DDoS attack

We will be generating dummy traffic, simulate normal traffic since time 0 and launch a DDoS attack at 180,second, and collect all data in 200 seconds (DDoS attack last for 20 seconds). Since these are 11 nodes, the OD flows number is 121 maximum, to get enough number of time interval,the time interval is set to “1 second”, so that the number of time interval will be 200.

3. Detect DDoS attack

We demonstrate two methods to detect DDoS attacks in the network: Sample entropy and Principal Component Analysis (PCA).

Sample entropy, a general way for DDoS detection in SDN is conducted by collecting the flow statistics or traffic features from the switches, and calculating the entropy measure randomness in the packets that are coming to a network. The higher the randomness, the higher is the entropy and vice versa. By setting a threshold, if the entropy passes it or below it, depending on the scheme, an attack is detected.

Principal Component Analysis (PCA) is a coordinate transformation method that maps the measured data onto a new set of axes. These axes are called the principal axes or components, where each principal component has the property that it points in the direction of maximum variation or energy remaining in the data, given the energy already accounted for, in the preceding components.

4. Compare the two schemes

Finally, we compare the results obtained from the detection of DDoS attacks using sample entropy and PCA.

Literature Survey

We explored a variety of references to implement the detection of DDoS attacks via Sample Entropy and Principal Component Analysis. The following are some of the papers we referred, to understand the concept of Sample Entropy and PCA:

1. [DDoS Attack Detection Algorithm Based on IP Entropy Model](#) (Wang xintong , Liu guqing , Yang jungang , Ran jinshi)
2. [Mining Anomalies Using Traffic Feature Distributions](#)(Anukool Lakhina, Mark Crovella, Christophe Diot)
3. [Diagnosing Network-Wide Traffic Anomalies](#)(Anukool Lakhina, Mark Crovella, Christophe Diot)
4. [Structural Analysis of Network Traffic Flows](#)(Anukool Lakhina, Konstantina Papagiannaki, Mark Crovella, Christophe Diot, Eric D. Kolaczyk, and Nina Taft)

Implementation

At this stage, we have created a custom topology in which used for analysing the traffic and attack in mininet . Also capable to generate normal traffic among the nodes in created topology.We are using pox controller to control the flow among the nodes also created [detection.py](#) in pox controller to measure the entropy of flow in each node.We created [traffic.py](#) to generate normal traffic also pox controller will measure the entropy of this flow in each node using [detection.py](#) .Here are the steps to reproduce our results till now.

Steps To Reproduce the Result

Prerequisites

1. Install Python
 2. Install mininet along with pox controller
- I. mininet installation : <http://mininet.org/download/>
- II. pox controller :
- Clone the repository : <http://github.com/noxrepo/pox>

Creating Test Environment

1. Clone the repo :

<https://github.com/aswanthpp/Analysis-of-DDoS-Attacks-in-SDN-Environments>

2. Copy contents from cloned repository to mininet custom folder

[src/traffic.py](#) to [mininet/custom/traffic.py](#)

3. Enter the following command to run the pox controller:

```
$ cd pox
```

```
$ python ./pox.py forwarding.I3_editing
```

4. Now create a mininet topology by entering the following command in

another terminal:

```
$ sudo mn --switch ovsk --topo tree,depth=2,fanout=8 --controller=remote,ip=127.0.0.1,port=6633
```

5. Now open xterm for an host by typing the following command

```
mininet>xterm h1
```

6. In the xterm window of h1, run the following commands to launch the traffic:

```
$ cd mininet/custom
```

```
$ python traffic.py -s 2 -e 7
```


7. Now the pox controller generates a list of values for entropy.

The least value obtained is the threshold entropy for normal traffic. To avoid false positives and negatives due to loss of a switch we choose an entropy value as 1.00 instead of 1.14. This implies 10% fault tolerance.

Future Works

Currently we are capable to create normal traffic among nodes and capable to measure the entropy of each flow. Next steps

1. Find a mechanism to measure the randomness of each flow in each node using PCA
2. Launch DDoS attack and try to capture it with both the methods

- 
3. Trying to come up with a new mechanism other than PCA and sample entropy measuring to detect DDoS attack in SDN environments effectively
 4. Compare the results of all three methods