Internet Technology and Applications

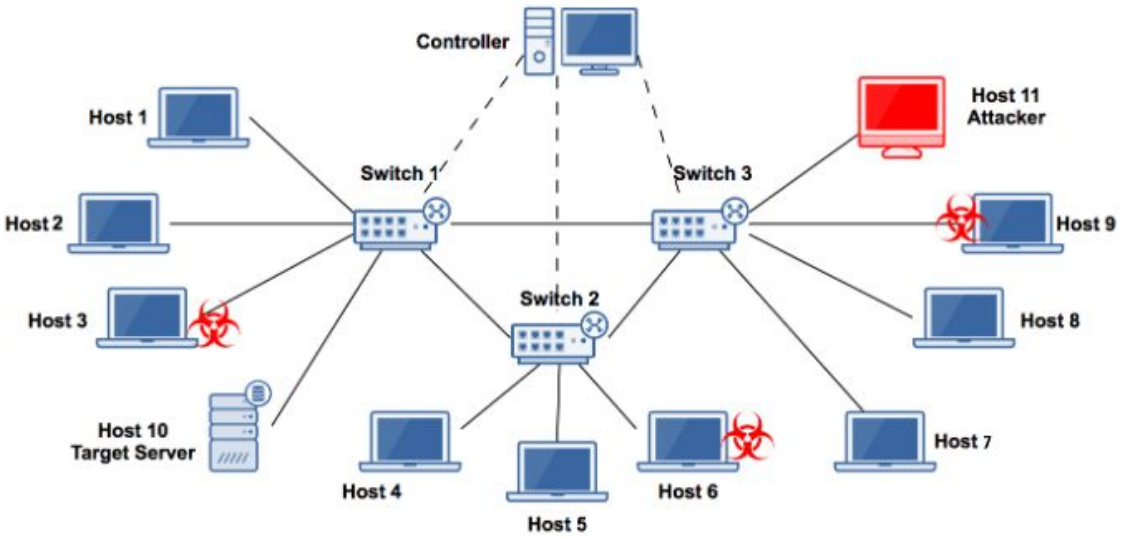
Analysis of DDoS attacks in SDN environments

Implementation phases

1. Setup of the test environment in mininet
2. Launch of DDoS attacks in the topology created
3. Detection of DDoS attacks using sample entropy and PCA
4. Comparison of the results of the above two schemes

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.

Flow Diagram