Distributed Denial of Service Attack Detection Using SDN

Group Members:

1. Bimal Bhattarai

2. Ranjeet Singh

3. Samin Yasar

4. Himangshu Das

Project Plan:

The topology we are planning to use is a tree topology with n switches. We will create our topology using Mininet. We will POX as the SDN controller to connect with the network created using Mininet. Scapy will be used to created network packets. We will carry out demonstration and simulations of the SDN network topology for the analysis of performance and workings of each components created. Our goal in this project is to acquire knowledge related to SDN. Learn about the SDN attacks performed at different layer of the SDN, which are the application layer, the control layer and the infrastructure layer. We have chosen to create a simulation environment, which detects the DDOS attacks. As this is a recent technology, being employed in our infrastructure the vulnerabilities related to it is vast and needs to be addressed. As we know what a DDoS attack does is exhaust the bandwidth on the network i.e. sending enormous amount of traffic to device greater than its buffer. If this happens, there is congestion of traffic within the network and packets are dropped in the network. Because of this, we do not get the desired service. We will typically limit the quantity of packets that is being sent to the controller. We will also simulate the DDos attack in the network topology created by Mininet, Scapy to create network packets and POX to run controller. The main theme behind our detection is Entropy, which means the measure of disorder in a system. Although there is an accepted range of entropy, but when being under DDoS attack there will be a sudden variation in the Entropy value.