SDN Based DDOS Attack Detection System

Problem Statement: To provide a solution for the detection of DDoS attack in SDN environment using SVM and entropy based mechanism and monitoring OpenFlow statistics.

Aim: We propose a system that detects DDoS attacks (UDP,TCP,ICMP) by collecting network statistics from the forwarding elements and applying Machine Learning classification algorithms(SVM).

Objective--

- To apprehend different types of network attacks which can be launched on SDN.
- To compare different types ddos detection technique.
- To grasp an overview about the different network monitoring tools.

Methodology: SDN (Software Defined Network) has attracted great interests as a new paradigm in the network.And thus the security of SDN is important.

- **Our project focuses on two major methods for the detection of DDoS attack:**

  DDoS detection using Entropy.

  DDoS detection using SVM.

- **Entropy Based DDoS Detection:**
  -Using mininet emulator network topology is created which contains 9 switches and 64 hosts.
  -A window of 50 packets is collected,and the entropy is calculated from their destination IP address.
  -If entropy is less than the specified threshold then an attack is detected.
  -For multiple victim attacks detection we take Flow rate for the detection.
  -DDoS attack traffic and normal traffic is generated which is further used as a dataset to train our model.

- **DDoS Detection using SVM:**
  -This method is composed of two stages, the first one is the features extraction, and the second step is the classification.
  -The feature are extracted from all the training packets set and the entropy will be used to measure the distribution of each feature.
  -Then, the calculated feature entropy will be used in order to train nonlinear SVM.
  -For each new test packets, we extract features and calculate the entropy which will be given to the trained SVM model in order to decide if is normal or abnormal.
  -If the result is abnormal, it means that DDoS attack happens.

Platform/Technology used:

- **Hardware:** Ubuntu any version with 8 gb ram

- **Software:** Mininet simulator, Pox controller, Scapy and Hping3(Packet Generator), Wireshark(analyser)

Results:

- These attacks are detected using the above method and results are further compared with each method.
- The port or switch with respect to attack is further blocked as a preventive measure.

S. No.	Attack	Detection Method
1	UDP Flood	Flow rate of packets
2	ICMP	Bandwidth Overload(Traceroute)
3	TCP-SYN	Monitoring TCP states

Impression of Project on Environment

- SDN is regarded as the novel networking architecture for detecting a DDoS attack.
- Helps to reduce the security issues that rises due to the intruders.
- The detection accuracy rate of the methods used is high and the false alarm rate is low.
- Reduce human intervention for the solving security issues.