Analysis of DDoS attack on SDN environments

January 10, 2017

Team

Aswath P P - 15CO112
Mohammed 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.

Goals

1. **Analysing the behaviour of traditional DDoS attacks on SDN environments.**
2. **Analysing the effect of new type DDoS attack on SDN environments by Principal Component Analysis.**
3. **Analysing the network by means of sample entropy and Principal Component Analysis.**

Specifications

Tools : mininet , ns3 (not sure whether it supports SDN functionalities), Virtual Labs like Orbit Lab etc.

Milestones

1. Understanding the paper

   First phase is to understand the concept behind SDN, Principal Component Analysis, normal and new type of DDoS attacks in SDN environment.

2. Analysing Principal Component Analysis on traditional and SDN networks

   We follow the method proposed in “Mining Anomalies Using Traffic Feature Distributions”, by A. Lakhina, M. Crovella, and C. Diot to analyse this phase.

3. Analysing the effect of New Type DDoS Attack in SDN

   We will follow the original paper where the author suggests to analyse the traffic.