Detection of DDoS in OpenSDN environment using SVM and Entropy based mechanism.

PROJECT SYNOPSIS

BACHELOR OF ENGINEERING
Computer Engineering

SUBMITTED BY

Achyuth Rao
Akib Shaikh
Arun Pottekat
Pranav Tale

July 2016

P. E. S. MODERN COLLEGE OF ENGINEERING, PUNE

Contents

List of Figures

List of Tables

1 Title

Detection of DDoS in OpenSDN environment using SVM and Entropy based mechanism.

2 Domain

Networking, Machine Learning and Physics

3 Keywords

SDN, SVM, Entropy, DDoS

4 Team

Group Id: 2

Team Members:

1. Achyuth Rao - 41056
2. Akib Shaikh - 41062
3. Arun Pottekat - 41054
4. Pranav Tale - 41070

5 Objective

1. To apprehend the different type of network attacks which can be launched on SDN.
2. To compare different types of DDoS detection mechanisms.
3. To grasp an overview about the different network monitoring tools.

6 Scope

1. To setup Software Defined Network environment and network monitoring tool to analyse the environment.
2. To understand the working of Support Vector Machine classifier and Entropy based mechanism in a Software Defined Network environment to detect DDoS attacks.
3. To analyse the OpenFlow statistics and develop an application to confirm the alert generated.

7 Feasibility Study

1. One can setup SDN environment virtually which is meant for research and testing needs.
2. Entire project will be based on Open Source technologies and thus numerous resources and documentation is easily available
3. For training of the SVM many datasets are available, for our project we will be using the dataset provided by DARPA.
   DARPA 2000 Scenario Specific dataset.

8 Technical Details

Platform

1. Software Defined Network
2. Linux Operating System
3. OpenFlow Switches

Software Specification

1. OpenDayLight Controller - 0.4.2 Berrylium SR2
2. Oracle VirtualBox
3. Mininet 2.2.1
4. POX Controller
5. Tenzor Flow - 1.4
6. libsvm
7. Python 2.7+, 3.0+
8. Nagios 4
9. GruntJS
10. Text Editor

Hardware Specification

1. Raspberry Pi Zero
2. USB to LAN Connectors
3. Ethernet Cables
4. System Configuration :-
   (a) Processor : i3 5th generation Machines
   (b) RAM : 4GB

Dataset

1. DARPA 2000 Scenario Specific dataset

9 Innovativeness and Usefulness

1. Entropy and SVM based applications are light weight and can be run on network devices without clogging it.
2. Our solution can be deployed in the enterprise networks for enhancing security.
3. Integrating Machine Learning and Artificial Intelligence with the new norms of networking i.e. SDN.
4. Run-time alert about DDoS attacks using Nagios.

10 Market Potential and Competitive Advantage

1. Since 2013 there have been many SDN deployements in production as it enables centralized network management.
2. SDN is estimated to reach approximately $35 billion by 2018 - Market Landscape Report.
3. A single DDoS attack can cost a company more than 4 lakh dollars and hence it becomes a necessity to detect such attacks quickly and efficiently.
4. Integrating applications like SVM and Entropy help to improve the security features of SDN.

11 Brief Description

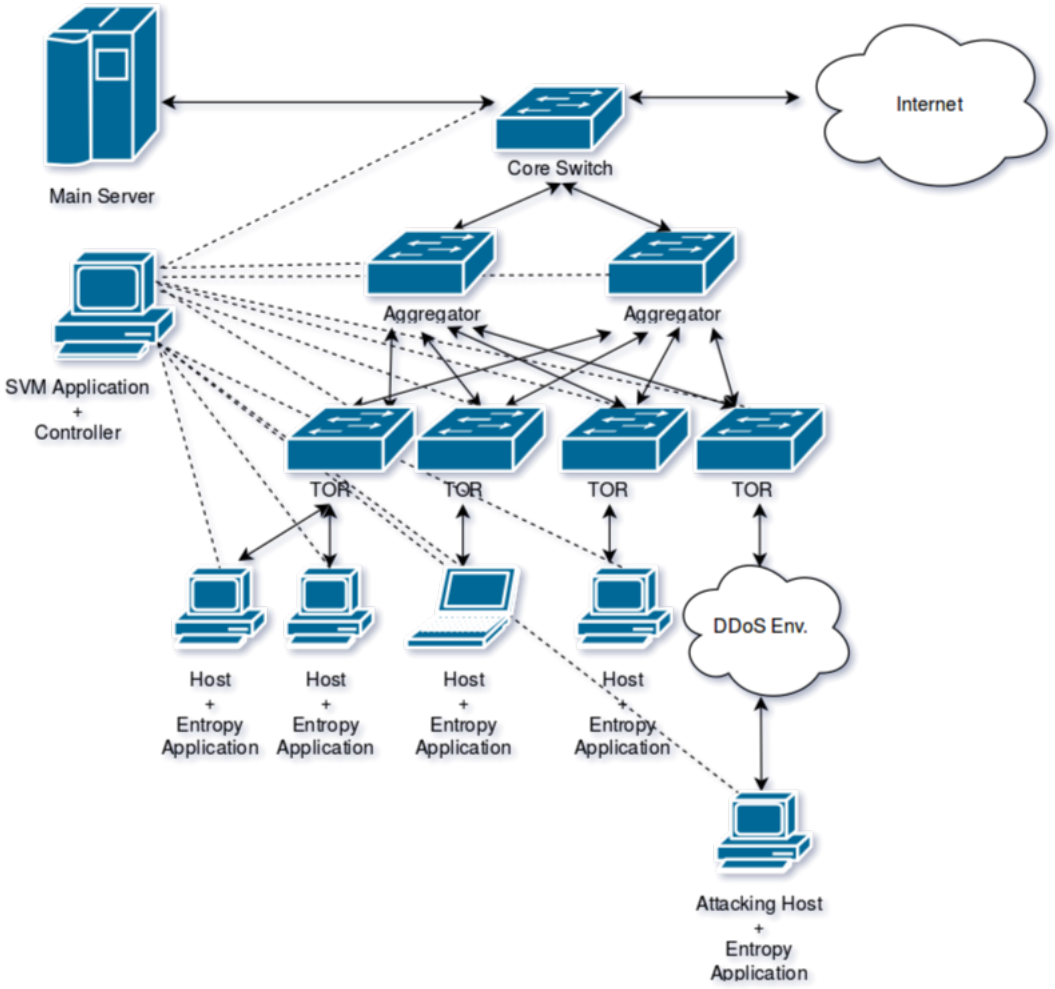

Figure 1: System Architecture Diagram

sdn-architecture.png

Figure 2: SDN Architecture Diagram

1. Software Defined Networks involves seperation of the control plane and data plane.
2. Forwarding of packets is done in the data plane and intelligence of the entire network resides in the control plane, making it vulnerable to network attacks.
3. DDoS attacks which cause heavy utilization of bandwidth must be detected dynamically with high rate of accuracy.
4. Thus, we compare two solutions for fast and effective detection :-
   (a) Entropy based Discretization :- Entropy is a measure of the probability of an event happening with reference to the total number of events occurring.

(b) Support Vector Machine Classififer :- is an accurate classifier capable of decision making from uncertain information.

5. As soon as the attack is detected a ticket will be raised to the network team by a network monitoring tool like Nagios

6. It is necessary to verify the alert by viewing the statistics of OpenFlow switches which will be provided as an application running on top of the controller for the network administrator.

12 Major Milestones and Dates

Sr. No	Module	End Date
1.	Setup of SDN Environment.	August 2016
2.	Monitoring SDN traffic using network monitoring tool to generate ticket in case of detection of DDoS attack.	March 2017
3.	Implementation of Support Vector Machine to detect DDoS attack.	December 2016
4.	Implementation of OpenFlow statistics monitoring application.	January 2017
5.	Implementation of Entropy based discretization to detect DDoS attack.	March 2017

Table 1: Major Milestones and Dates

13 References

[1] ”DDoS Detection and Analysis in SDN-based Environment Using Support Vector Machine Classifier” -Kokila RT, S. Thamarai Selvi, Kannan Govindarajan - 2014 Sixth International Conference on Advanced Computing(ICoAC) - Department of Computer Technology, Anna University (MIT Campus), Chennai

[2] ”An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking” - Rui Wang, Zhiping Jia, Lei Ju - 2015 IEEE Trustcom/BigDataSE/ISPA - School of Computer Science and Technology Shandong University Jinan, China

[3] ”Software-Defined Networking:The New Norm for Networks and Open Networking Foundation” - Open Networking Foundation - ONF White Paper April 13, 2012

[4] ”Detection of DDoS Attacks using Enhanced Support Vector Machines with Real Time Generated Dataset” - T.Subbulakshmi , Dr. S. Mercy Shalinie, V.GanapathiSubramanian, K.BalaKrishnan, D. AnandK, K.Kannathal - IEEE-ICoAC 2011 - Department of CSE, TCE Madurai, India.

[5] ”OpenFlow Switch Specification” - Open Networking Foundation - Version 1.3.2 2013