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

Achyuth Rao - 41056
Akib Shaikh - 41062
Arun Pottekat - 41054
Pranav Tale - 41070

Guide:- Prof. Mrs. Aparna Junnarkar

PES's Modern College Of Engineering

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.

Motivation

- The centralized controller is a potential single point of attack.
- The Southbound interface, OpenFlow is vulnerable to threats.
- DDoS attack renders an online service unavailable by overloading it.
- Thusly, there is a need to optimally detect DDoS in SDN.

Objective

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

Scope

- Set up of SDN environment.
- Entropy and SVM based DDoS detection method.
- OpenFlow Monitoring application using OpenDaylight API.

Literature Survey

Title	Author	Journal and Year	Description
DDoS Detection and Analysis in SDN-based Environment Using Support Vector Machine Classifier	Kokila RT, S. Thamarai Selvi, Kannan Govindarajan	IEEE 2014	This paper provides information about DDoS attack in SDN environment using Support Vector Machine to classify the attack.
An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking	Rui Wang, Zhiping Jia, Lei Ju	IEEE 2015	This paper provides information about DDoS attack in SDN environment using Entropy based mechanism to classify the attack.
Software-Defined Networking:The New Norm for Networks	Open Networking Foundation	ONF White Paper, 2012	Description about Software Defined Networks
Detection of DDoS Attacks using Enhanced Support Vector Machines with Real Time Generated Dataset	T.Subbulakshmi, Dr. S. Mercy Shalinie, D. AnandK, K.Kannatha	IEEE 2013	Provided information how to create and use datasets for SVM.
OpenFlow Switch Specification	Open Networking Foundation	Version 1.3.2 2013	Description about OpenFlow Protocol

Architecture Diagram

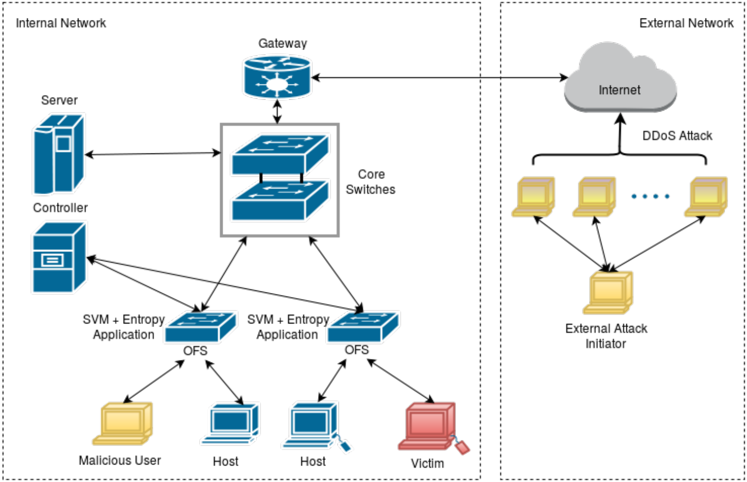

Figure: System Architecture

Mathematical Model

Algorithmic Strategies

Software Specifications

- Linux based Operating System.
- OpenDayLight Controller - 0.4.2 Berrylium SR2.
- Oracle VirtualBox.
- Mininet 2.2.1
- POX Controller.
- Tenzor Flow 1.4
- LibSVM.
- Python 2.7 or above.
- Nagios Core.
- ReactJS

Hardware Specifications

- Raspberry Pi Zero Controller.
- USB to LAN Connectors
- Ethernet Cables
- Zodiac FX OpenFlow Switch.

Dataset Specifications

- "DDoS attack 2007" dataset provided by the Center for Applied Internet Data Analysis(CAIDA).
- The 1998 DARPA's network traffic dataset provided by MIT Lincoln Lab.
- The 2000 DARPA intrusion detection scenario specific dataset provided by MIT Lincoln Lab which contains:

Table: 2000 DARPA Dataset details

Data Category	**No. of training instances**	**No. of test instances**
Break In	156	374
DDoS	963	1035
Installsw	318	204
IPSweep	101	684
Normal	2500	2501
Probe	54	94
Total	4092	4892

Results of Entropy Based Discretization

- Machine with Ubuntu 14.04, i5 CPU and 8G RAM.
- Mininet as a network simulator (Tree Topology, 800Mbps Link speed, 20 hosts).
- Open vSwitch.
- Floodlight controller.
- CAIDA's "DDoS Attack 2007" dataset.

Table: parameter values of the Traffic

S. No	**Average Traffic Rate(Mbps)**	**Attack Rate(pkts/s)**
Exp.1	50	50-200
Exp.2	100	300-500
Exp.3	500	1000-2000

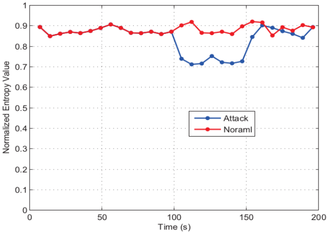

Figure: The normalized entropy value of IPdst Flow

Results of SVM based Method

- The normal traffic data is included from 1998 DARPA dataset.
- The attack traffic data is included from 2000 DARPA dataset.

Table: Accuracy with different parameters

Cost	Gamma	Classification Accuracy(%)	False Positive
10	0.1	94.23	0.011
10	0.01	95.11	0.008
10	0.001	93.86	0.013

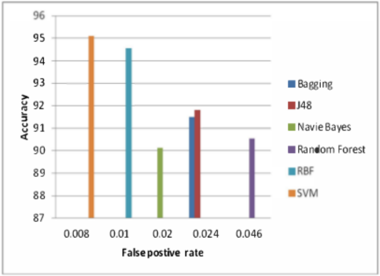

Figure: Camparison of classification methods

Conclusion

- Taking into consideration the advantages of SDN, security issues need to be resolved.
- This project will be a step towards enhancing the security in SDN which will soon replace the traditional networks.

References

- "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.
- "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.
- "Software-Defined Networking:The New Norm for Networks and Open Networking Foundation" - Open Networking Foundation - ONF White Paper April 13, 2012.
- T.Subbulakshmi , Dr. S. Mercy Shalinie, V.GanapathiSubramanian, K.BalaKrishnan, D. AnandK, K.Kannathal - IEEE-ICoAC 2011 - Department of CSE, TCE Madurai, India.
- "OpenFlow Switch Specification" - Open Networking Foundation - Version 1.3.2 2013.

Thank You. . .