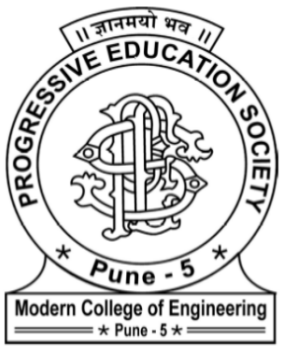
Detection of DDoS in SDN environment using SVM and Entropy based discretization.

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

Guide:- Prof. Mrs. Aparna Junnarkar



PES's Modern College Of Engineering

Contents

Introduction

- SDN separates intelligence from the hardware.
- SDN controller acts as network Operating System.
- This networking paradigm faces some issues.
- DDoS attack makes the network resources unavailable.

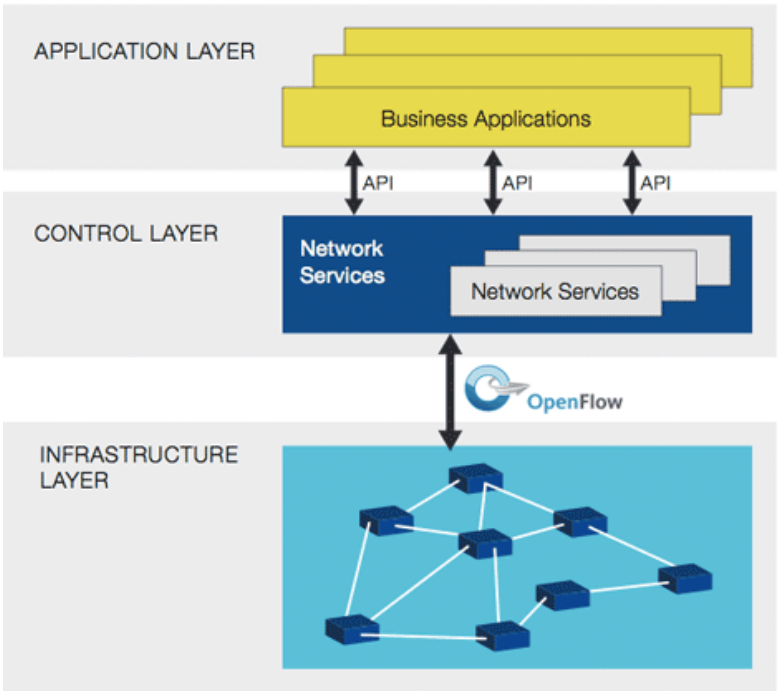


Figure 1: SDN Architecture

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

- Number of cyber attacks is increasing day by day.
- Reluctance to adopt SDN due to lack of security solutions.
- A single DDoS attack can cost an enterprise over $1.6 million.
- SDN market is expected to grow to $56 Billion by 2022.
- Automation of attack detection is required.
- Integration of Machine Learning and Data Mining with SDN.

Objective

- To apprehend different types of network attacks which can be launched on SDN.
- To compare different types of DDoS detection techniques.
- To propose the best effective method for a specific environment.
- 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

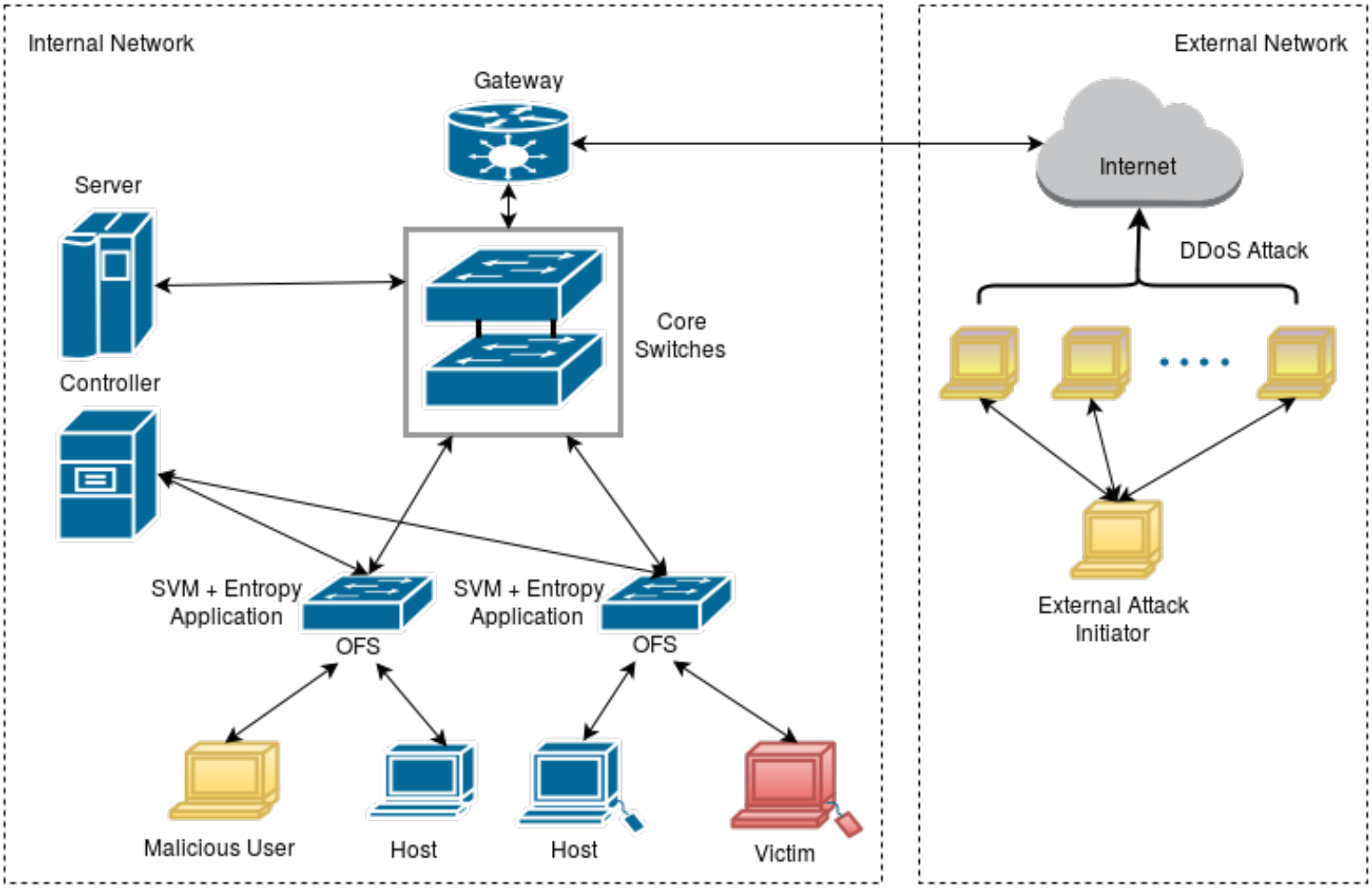


Figure 2: System Architecture

UML Diagrams

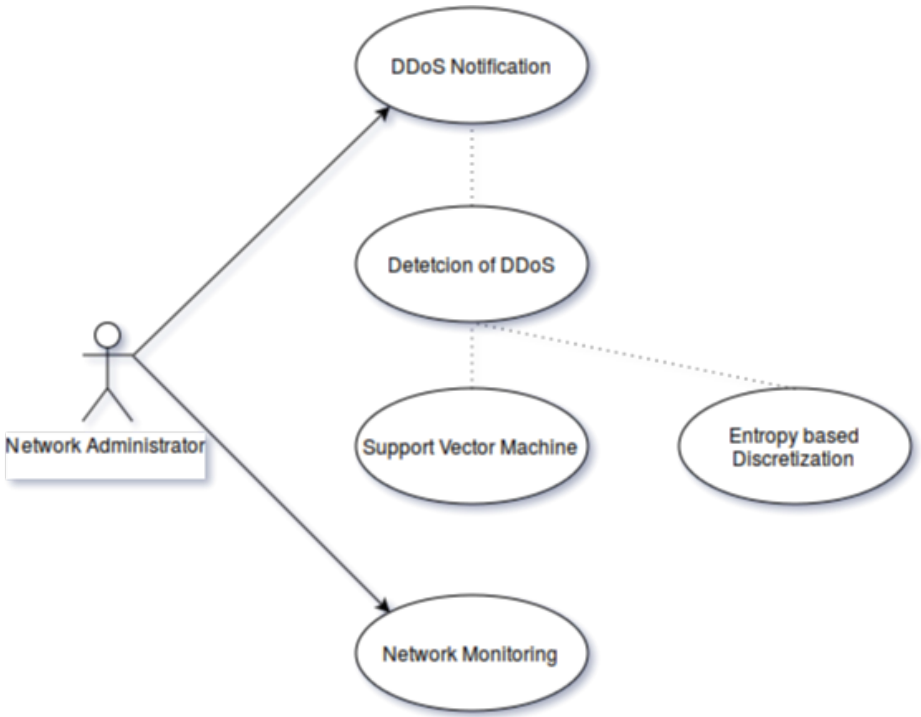


Figure 3: Use Case Diagram

UML Diagrams

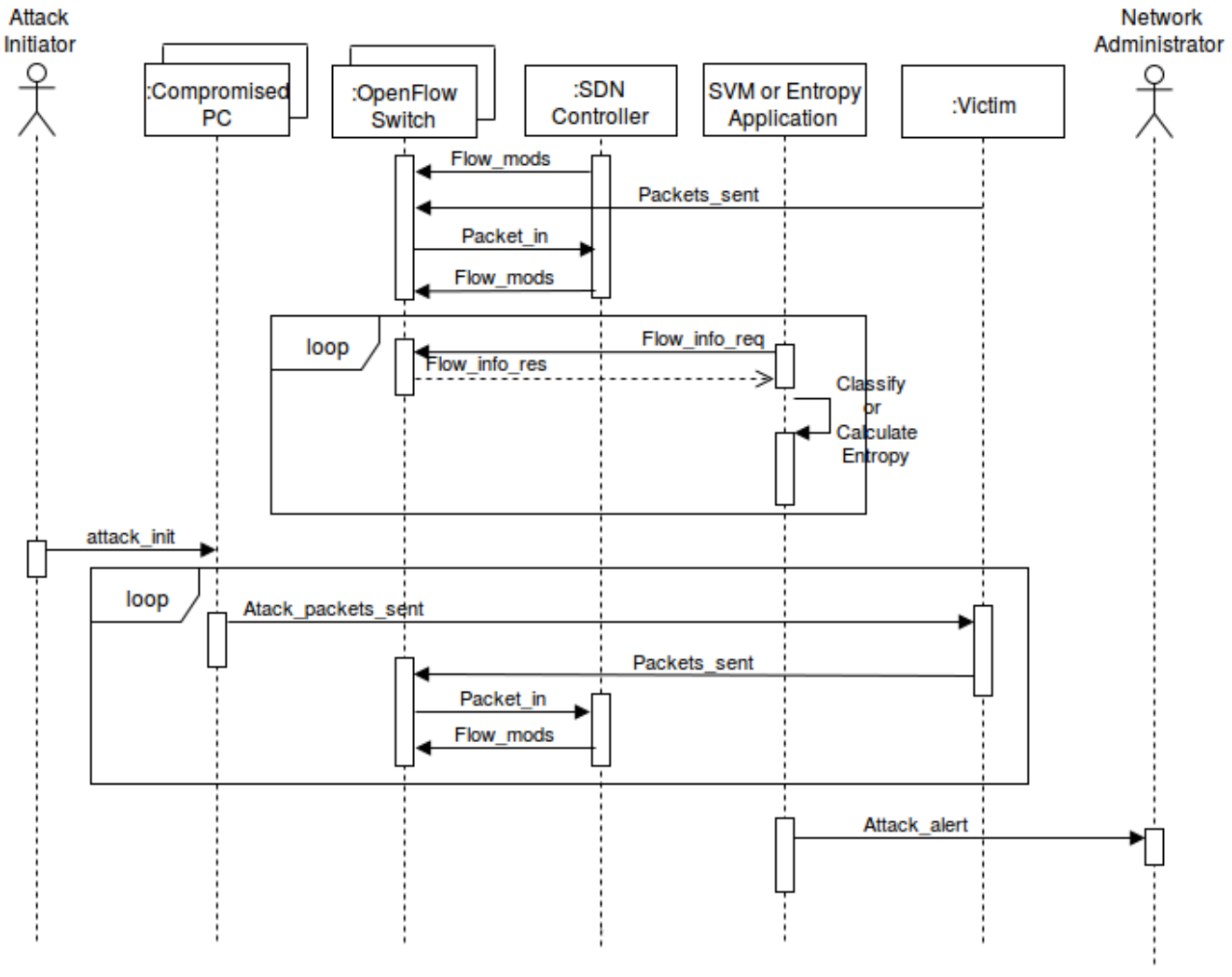


Figure 4: Sequence Diagram

Mathematical Model

$S = \{\{I\}, \{P\}, \{O\}\}$

$I = \{N\}$
where,
$N = \{$ Network Statistics $\}$,
$F = \{F_i \mid F_i \in T, \forall i \ F_i =$ Individual entry $\}$,
$T = \{$ Flow Table $\}$,
$F \subseteq N$

$P = \{P_{EBD}, P_{SVM}\}$

$O = \{O_{EBD} \cup O_{SVM}\}$

Mathematical Model

P_{EBD} (I_{EBD}, O_{EBD})
{

- $I_{EBD} = \{U_i \mid U_i = (\text{ Src. Addr., Dest. Addr., Port no., Count}),\ U_i \subset F_i\}$
- $P_i = \frac{C_i}{N}$
- $\varepsilon = \sum_{i=0}^{n} -P_i log P_i$
- $(\lambda < \varepsilon) \rightarrow (\beta = 0)$
  $(\lambda > \varepsilon) \rightarrow (\beta = 1)$
- $O_{EBD} = \{\beta \mid \beta \in (0, 1)\}$

}

P_{SVM} (I_{SVM}, O_{SVM})
{

- $I_{SVM} = \{V_i \mid V_i = (\text{ Src. Addr., Dest. Addr., Port no., Time, Prot., Count})\}$
- $RBF = e^{-\gamma(|x_1 - x_2|)+c}$
- $y = \overline{\omega} * x + b$
- $(y \leq -1) \rightarrow (\alpha = 1)$
  $(y \geq 1) \rightarrow (\alpha = 0)$
- $O_{SVM} = \{\alpha \mid \alpha \in (0, 1)\}$

}

Algorithmic Strategies

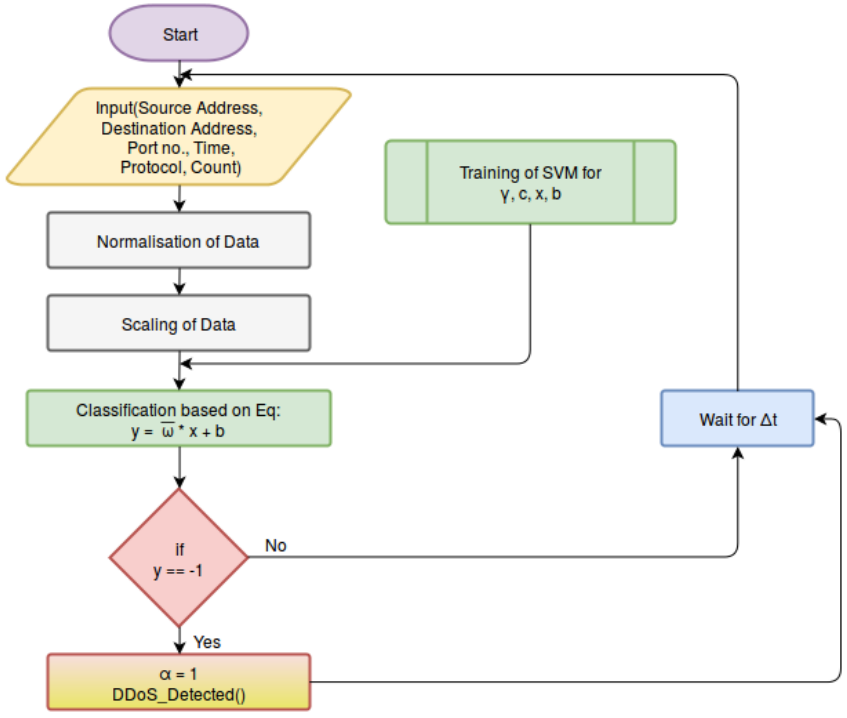


Figure 5: Flowchart: Support Vector Machine Algorithm

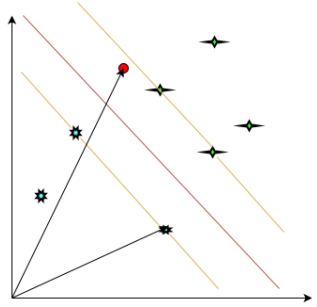


Figure 6: Support Vector Machine Graph

Algorithmic Strategies

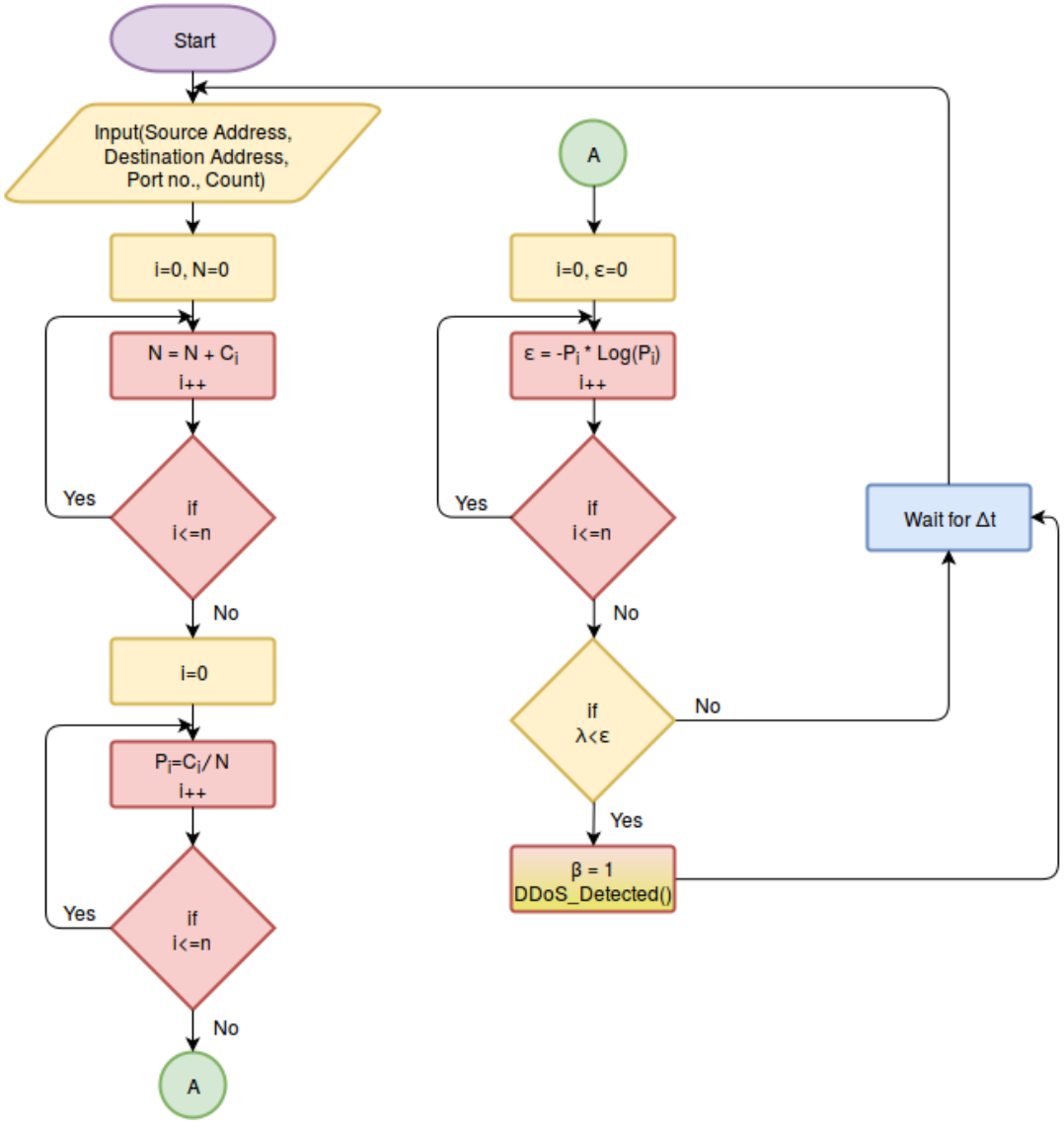


Figure 7: Flowchart: Entropy Based Discretization Mechanism

Software Specifications

- Linux based Operating System.
- OpenDayLight Controller - 0.4.2 Berrylium SR2.
- Open vSwitch (OVS).
- PicOS / OpenSwitch.
- Oracle VirtualBox.
- Mininet 2.2.1.
- POX Controller.
- LibSVM.
- Python 2.7 or above.
- Nagios Core.
- NodeJS + AngularJS (JavaScript Framework).

Hardware Specifications

- Any Enterprise/ Data Center/ Campus Network Topology with 100/1000 Mbps.
- Manageable switches that support OpenFlow Protocol / Whitebox Switches.
  - HPE Altoline 6900 48G ONIE AC Switch.
  - Pica8 P-3297 48 X 1Gbe.
  - HP 2920 Switch Series.
- Server Running the Controller
  - Dell PowerEdge R720

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:

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

Table 1: 2000 DARPA Dataset details

Test Cases

Id	Description	Scenario	Expected Output
1	Time span between attack detection and alert generation	Attack has occured	Instantaneous alert generation
2	Normal Network Traffic, Log file not altered and attack is not detected	SDN functioning in normal mode	Alert not generated

Scenario: Attack Traffic

Id	Description	Input	Expected Output
1	Simple DoS attack	Large no. of same type of packets	Attack detected
2	UDP flood attack	Large no. of UDP packets	Attack detected
3	Varying DDoS attack bandwidth	Large no. of packets	DDoS attack should be detected only when bandwidth exceeds normal threshold traffic.

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.

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

Table 2: parameter values of the Traffic

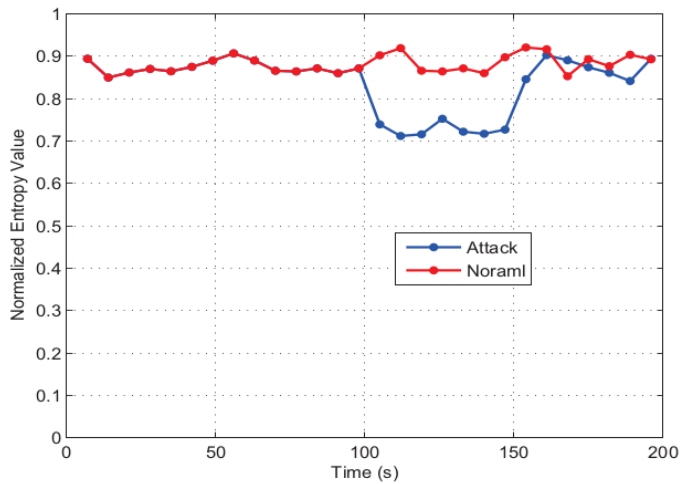


Figure 8: The normalized entropy value of IPdst Flow

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.

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

Table 3: Accuracy with different parameters

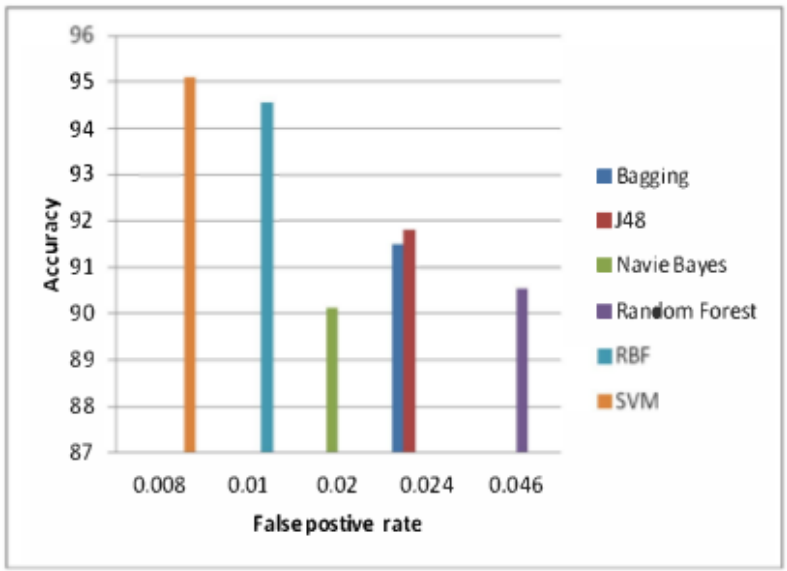


Figure 9: Camparison of classification methods

Conclusion

- Proposing a solution for DDoS detection in SDN environment and also comparing the effectiveness of both methods (SVM and Entropy based Discretization) in a specific environment which would be a step towards solving the security issues and accelerating the adoption of SDN.

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. . .