ARMY INSTITUTE OF TECHNOLOGY PUNE
DEPARTMENT OF INFORMATION TECHNOLOGY

BE Project Phase I Review-I

SDN Based DDOS attack detection System

Ankita Kumari(4409)
Prachi Dwivedi(4437)

Gayatri Basera(4223)
Varsha Kanwar(4456)

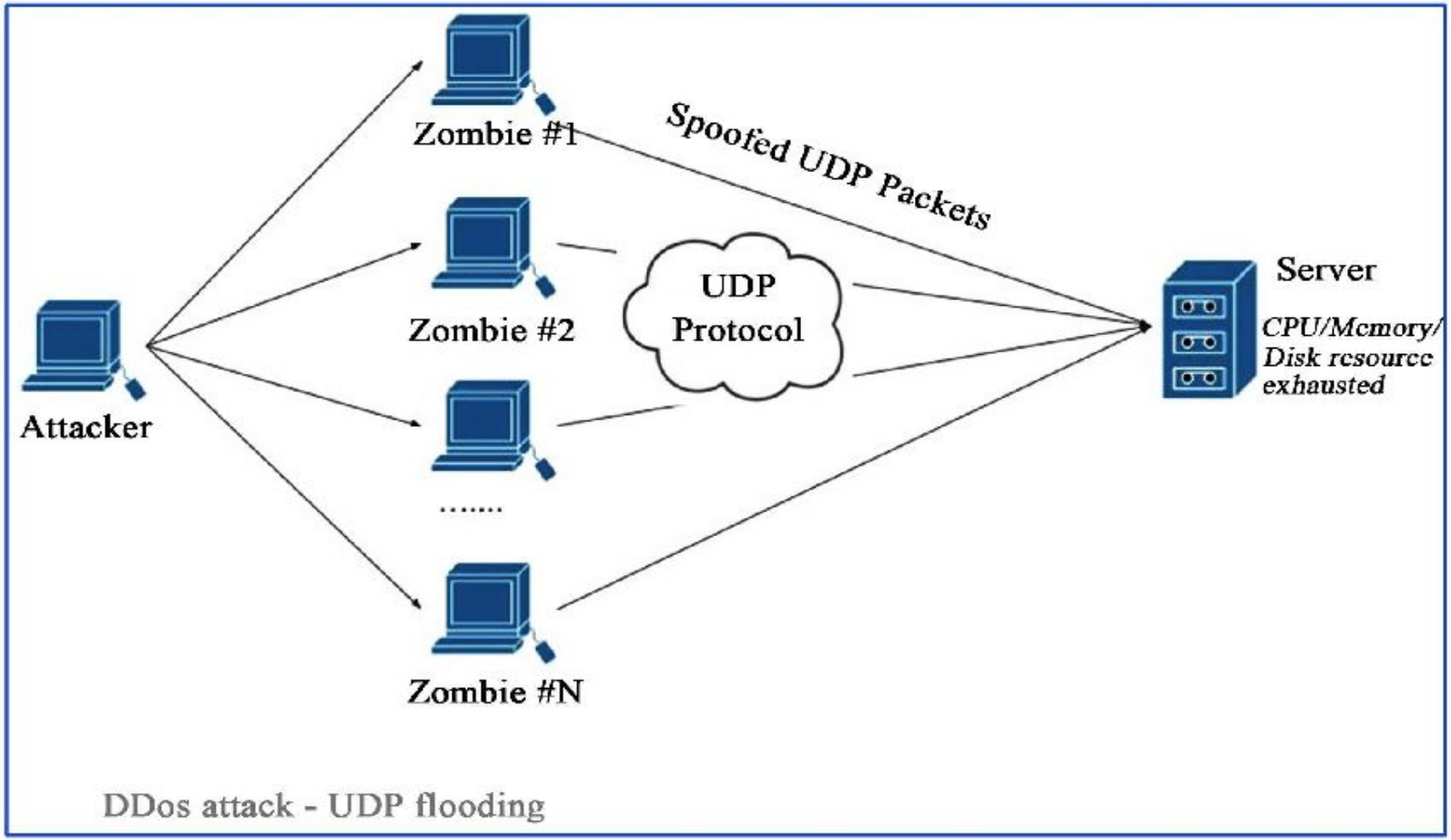
Prof. Geeta Patil

Project Guide

December 14, 2019

1. Introduction

- A high quality network security system can reduce the risk of attack and improve user experience.
- Software Defined Networking (SDN) is a promising paradigm that allows the programming of the logic behind the network's operation with some abstraction level from the underlying networking devices.
- Cyber-attacks, especially those based on DDoS, are more and more prevalent, and their impact is greater than ever on the network infrastructure, online services, and digital information assets.
- This includes an IDS that automatically detects several DDoS attacks, and then as an attack is detected, it notifies a Software Defined Networking (SDN) controller.


Zombie #1
Spoofed UDP Packets
Zombie #2
UDP
Protocol
Server
CPU/Memory/
Disk resource
exhausted
Attacker
.....
Zombie #N
DDos attack - UDP flooding

2. Objective & Scope

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

Scope - To detect known and unknown DDoS attacks in real time environments using a emulator(Mininet),packet generation tools(scapy).

-Solves the problem of network administrator in managing multiple networks at the same time.

In the last five years, the size of DDoS attacks has been increasing exponentially, as shown in Figure.

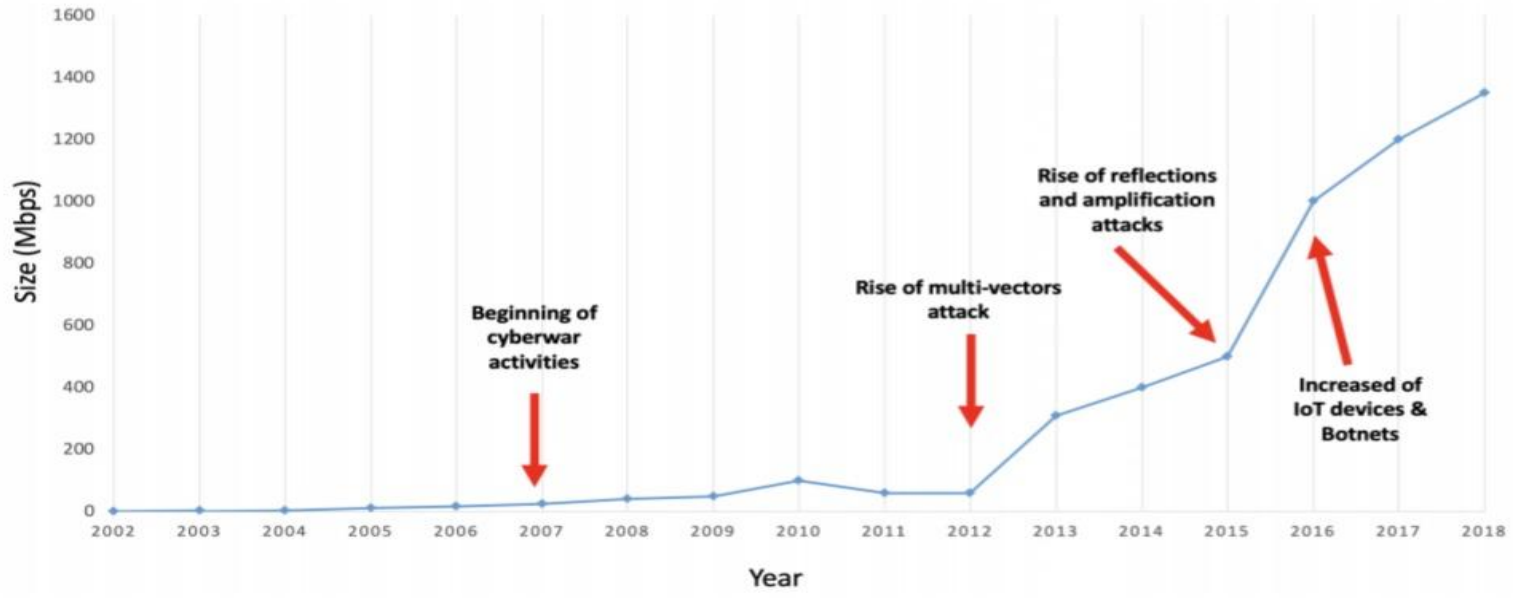


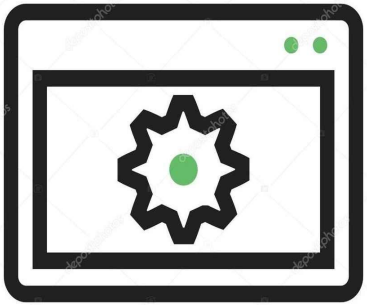
Figure 1.1: DDoS Attack Growth in Terms of Size (Mbps) from 2002-2018 [8, 9, 10]

3. Literature Review

S.no	AUTHOR NAME	TITLE	FINDINGS	PUBLISHER
1.	Irfan Sofi , Amit Mahajan , Vibhakar Mansotra	DDoS attack detection and mitigation using SDN: Methods, Practices, Solutions	In this the work is carried out on the new dataset which contains the modern type of DDoS attacks such as (HTTP flood, SIDDoS). This work incorporates various machine learning techniques for classification: Naïve Bayes, MLP, SVM, Decision trees	Springer, Computer Engineering and Computer Science, 2017
2.	Keisuke Kato, Vitaly Klyuev	Detection of known and unknown DDoS attacks using Artificial Neural Networks	In this , we analyzed large numbers of network packets provided by the Center for Applied Internet Data Analysis and implemented the detection system using a support vector machine with the radial basis function (Gaussian) kernel. The detection system is accurate in detecting DDoS attack.	Elsevier, 2016
3.	Marwane Zekri, Said El Kafhali, Noureddine Aboutabit and Youssef Saadi	Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques	Designed a DDoS detection system based on the C.4.5 algorithm to mitigate the DDoS threat. This algorithm, coupled with signature detection techniques, generates a decision tree to perform automatic, effective detection of signatures attacks for DDoS flooding attacks.	International Conference on Smart Systems and Inventive Technology (ICSSIT 2018) IEEE

Sn.	AUTHOR NAME	TITLE	FINDINGS	PUBLISHER
4.	Mouhammd Alkasassbeh,Ahmad B.A Hassanat, Ghazi Al-Naymat	Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN)	In this a new dataset is collected because there were no common data sets that contain modern DDoS attacks in different network layers, such as (SIDDoS, HTTP Flood). This work incorporates three well-known classification techniques: Multilayer Perceptron (MLP), Naïve Bayes and Random Forest.	Hindawi Journal of Computer Networks and Communications Volume 2019
5.	Jin Ye,Xiangyang Cheng ,Jian Zhu, Luting Feng, Ling Song	A DDoS Attack Detection Method Based on SVM in Software Defined Network	Here, the SDN environment by mininet and floodlight (Ning et al., 2014) simulation platform is constructed, 6-tuple characteristic values of the switch flow table is extracted, and then DDoS attack model is built by combining the SVM classification algorithms.	Hindawi Security and Communication Networks Volume 2018
6.	Adel Alshamrani, Ankur Chowdhary, Sandeep Pisharody, Duo Lu Dijiang, Huang	A Defense System for Defeating DDoS Attacks in SDN based Networks	Current SDN-based attack detection mechanisms have some limitations. Here they investigate two of those limitations: Misbehavior Attack and New flow Attack. We propose a secure system that periodically collects network statistics from the forwarding elements and apply ML classification algorithms.	MobiWac'17, November 21–25, 2017, Miami, FL, USA 2017 Association for Computing Machinery. ACM

4. Platform/Technology Used

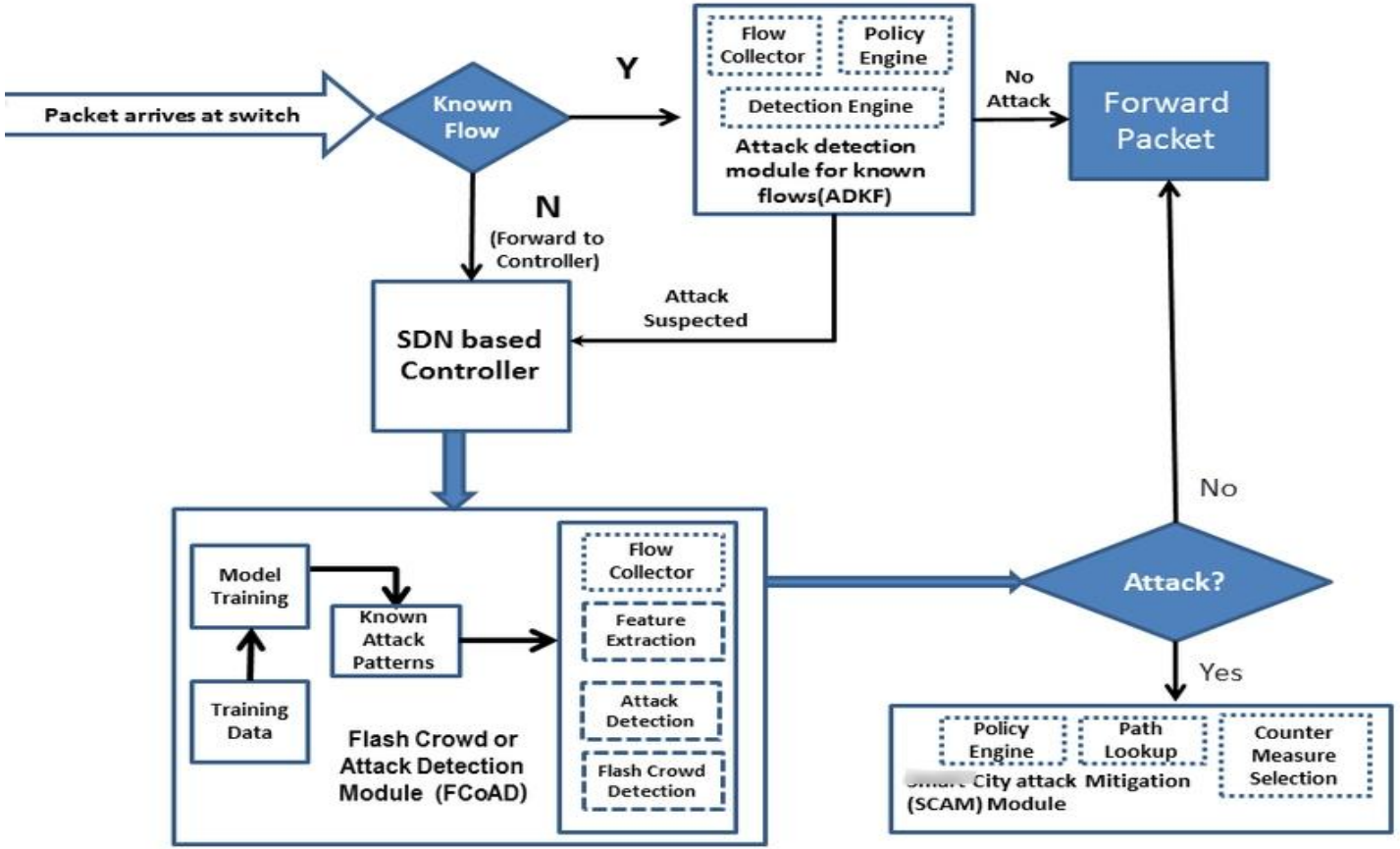


- **Hardware**
  - OS - ubuntu Version 16.04 and 8 GB ram
- **Software**
  - Simulator-Mininet
  - Controller- Pox(python based sdn controller)
  - Scapy
  - Wireshark

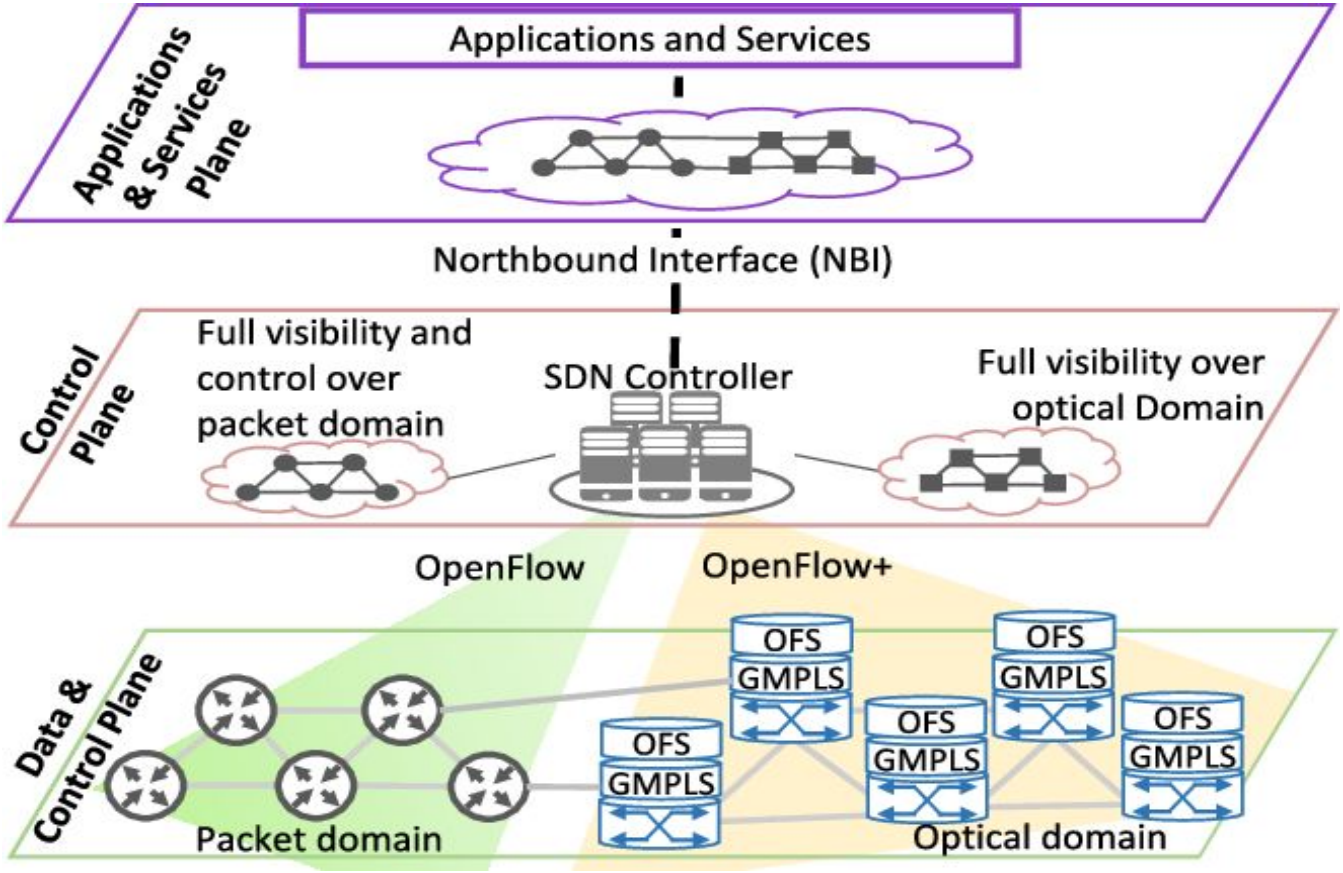
Types Of DDoS Attack and Detection Method

S.No	Attack	Detection Method
1	UDP	Flow rate of packets
2	Ping of Death	Size of packet
3	ICMP	Bandwidth Overload(Traceroot)
4	TCP	Monitoring TCP states

5. Project Architecture



- **SDN Architecture**



6. Algorithms

6a. Entropy based detection

- Sample Entropy is a method used to detect DDoS attacks in SDN. There are two essential components to DDoS detection using entropy: window size and a threshold.

- Window size is either based on a time period or number of packets. Entropy is calculated within this window to measure uncertainty in the coming packets. To detect an attack, a threshold is needed. If the calculated entropy passes a threshold or is below it, depending on the scheme, an attack is detected.

- The main reason for choosing entropy is its ability to measure randomness in a network. The higher the randomness, the higher is the entropy and vice versa.

DDos Detection Using Entropy

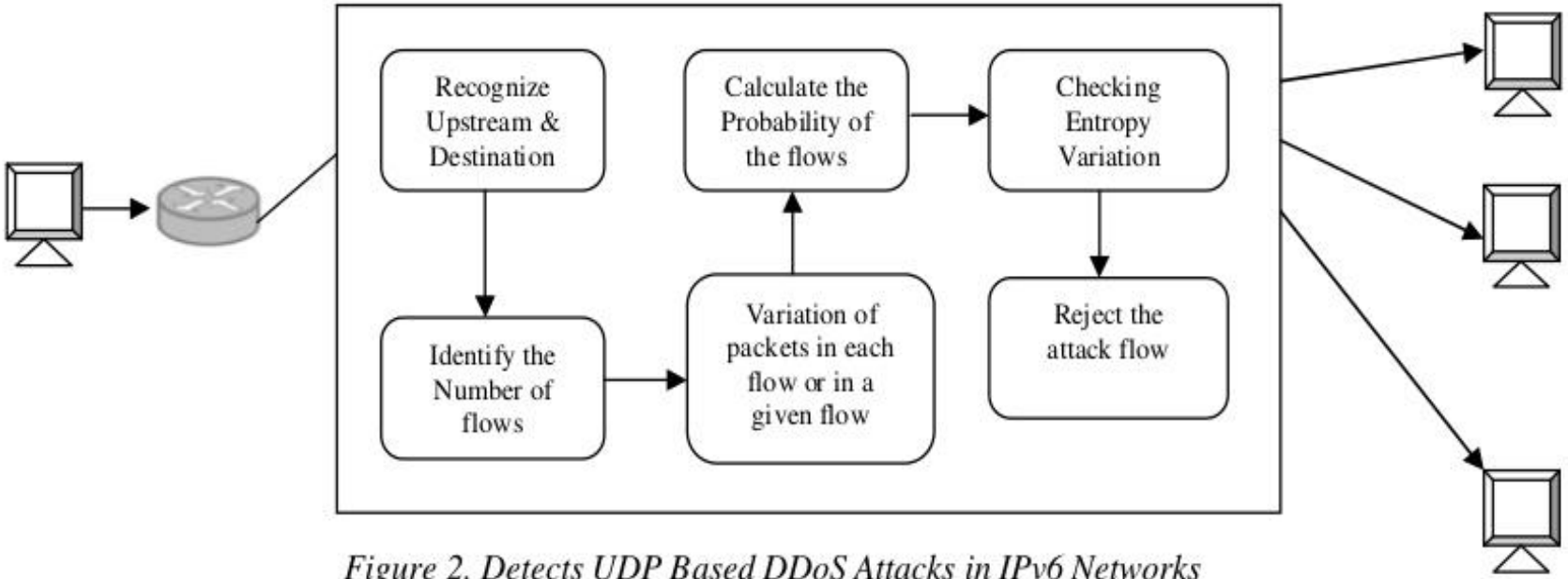
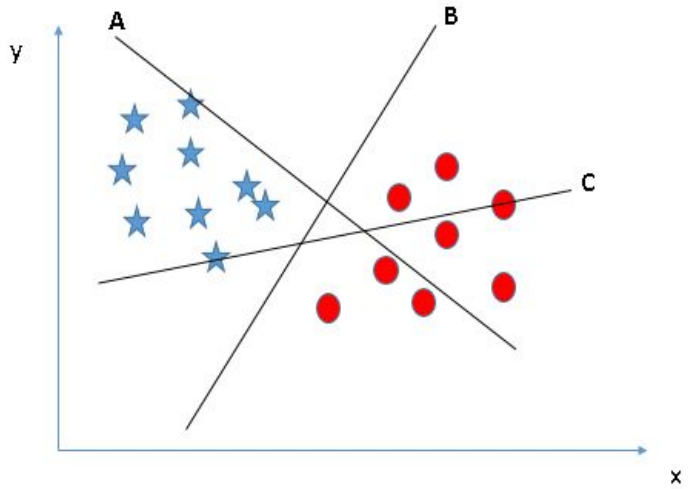


Figure 2. Detects UDP Based DDoS Attacks in IPv6 Networks

6b.SVM

- Identify the right hyper-plane (Scenario-1):



- Identify the right hyper-plane (Scenario-2):

Fig .a.

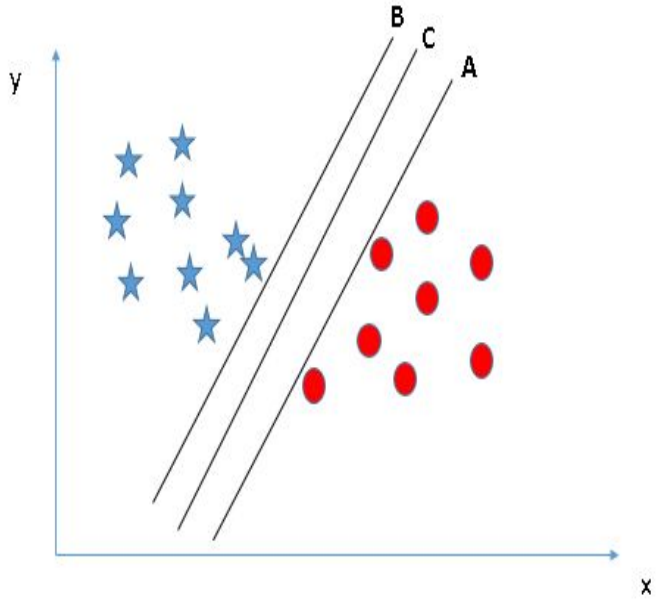
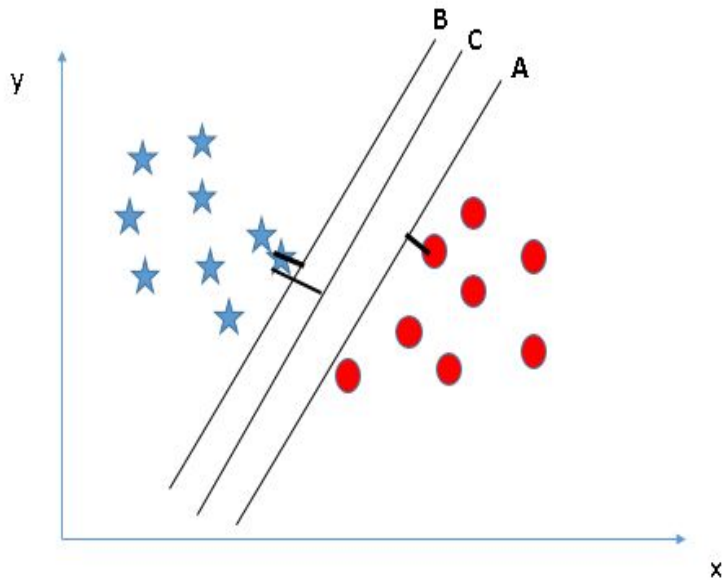
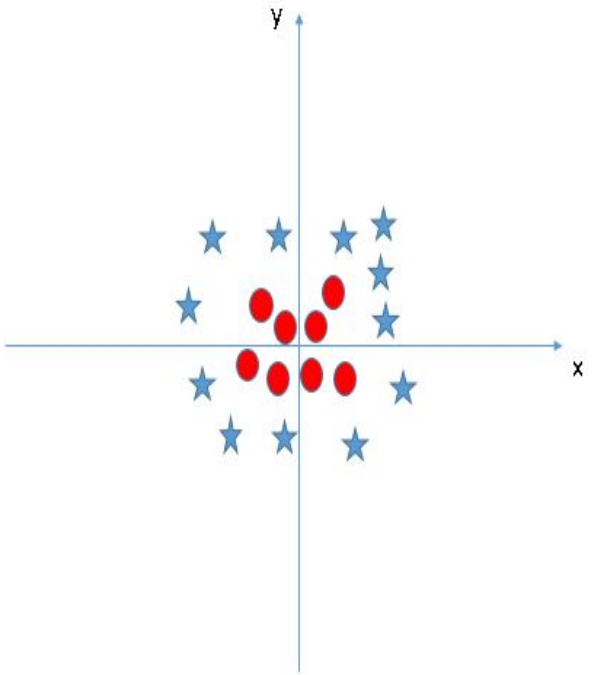
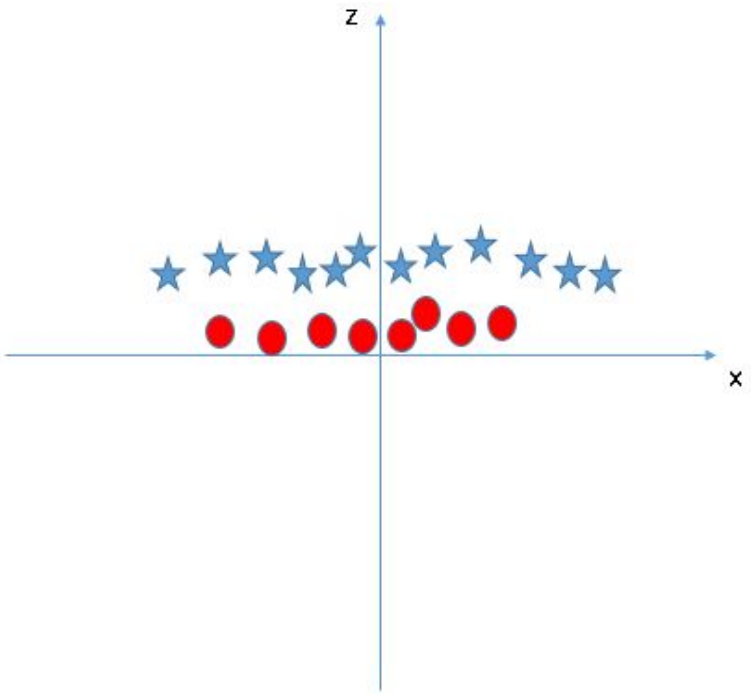


Fig.b.

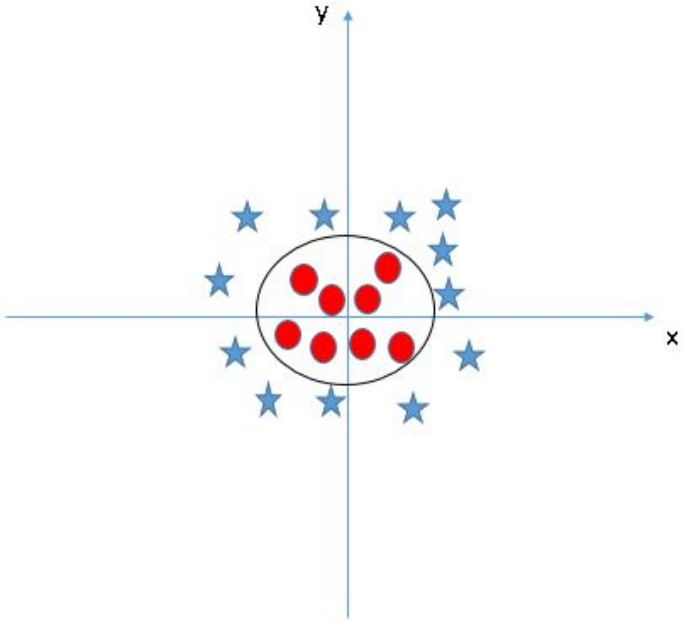


- **Find the hyper-plane to segregate to classes (Scenario-3):**
  - Fig.a. Fig.b.



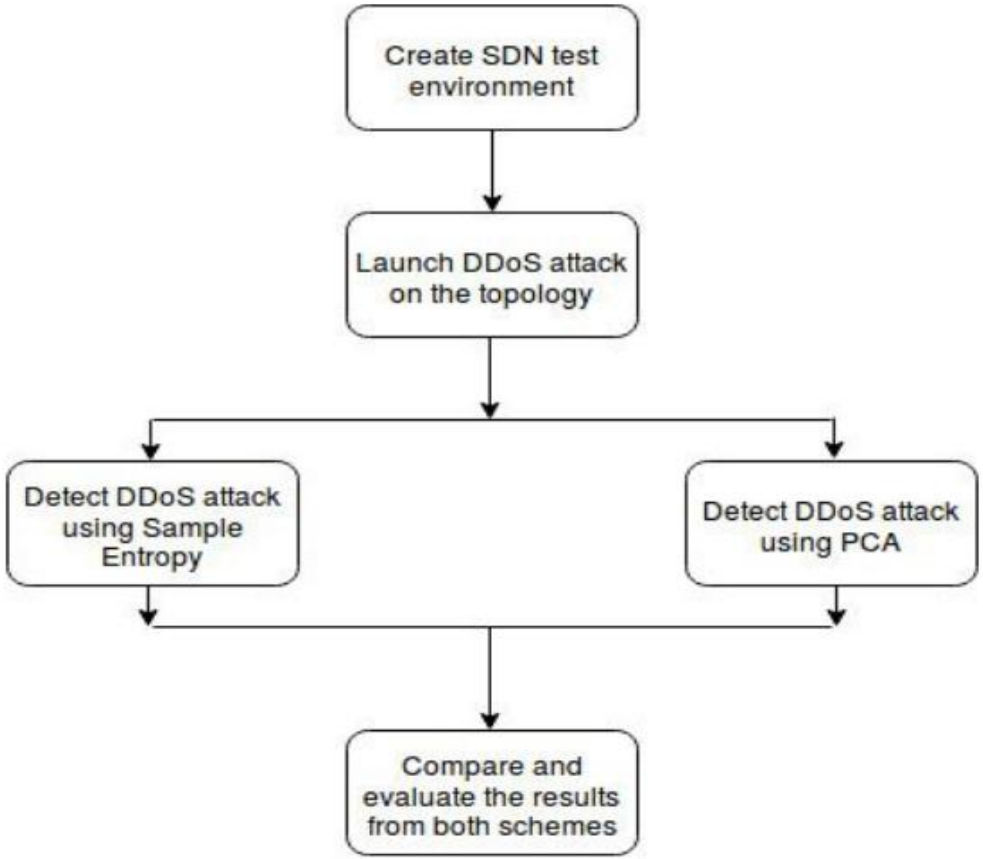


❑ Kernel trick

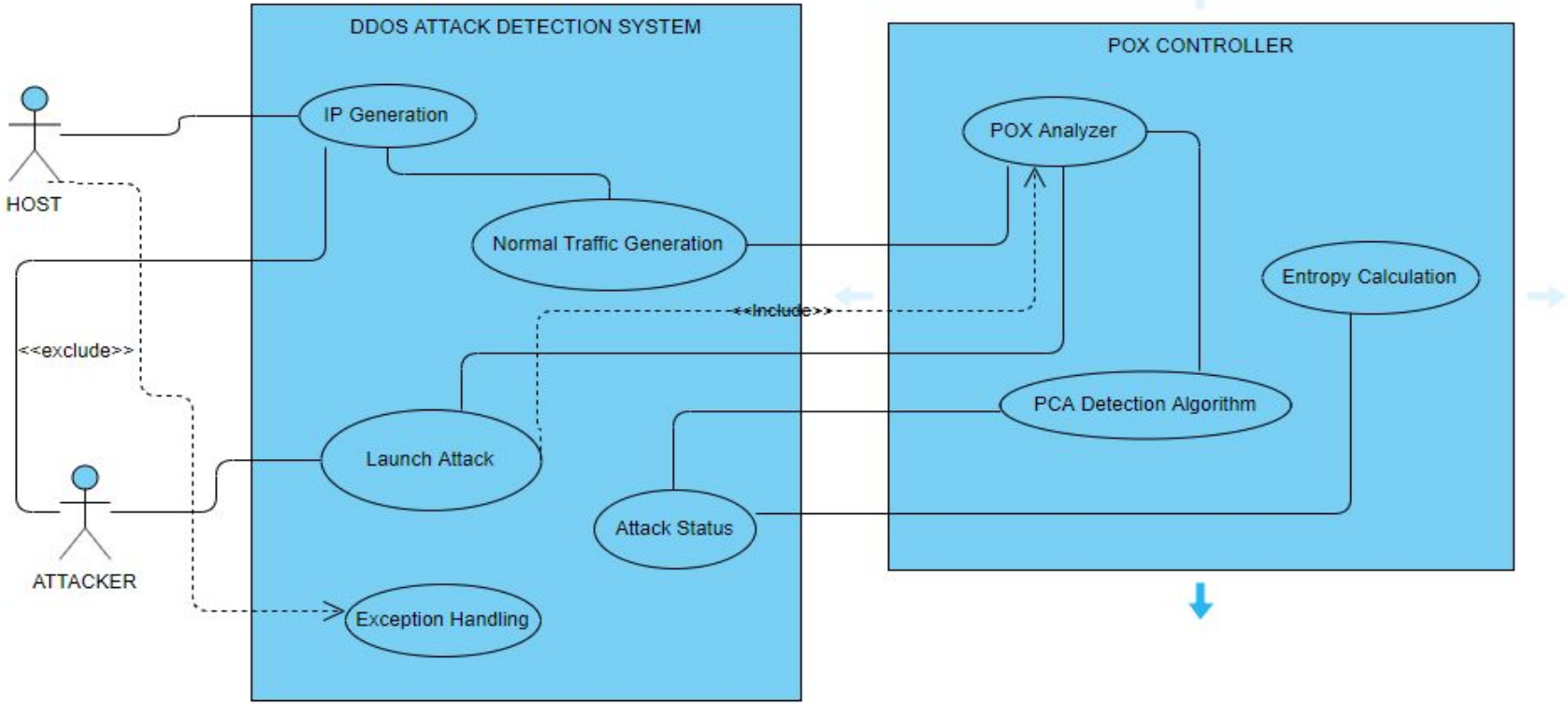


7. UML DIAGRAMS

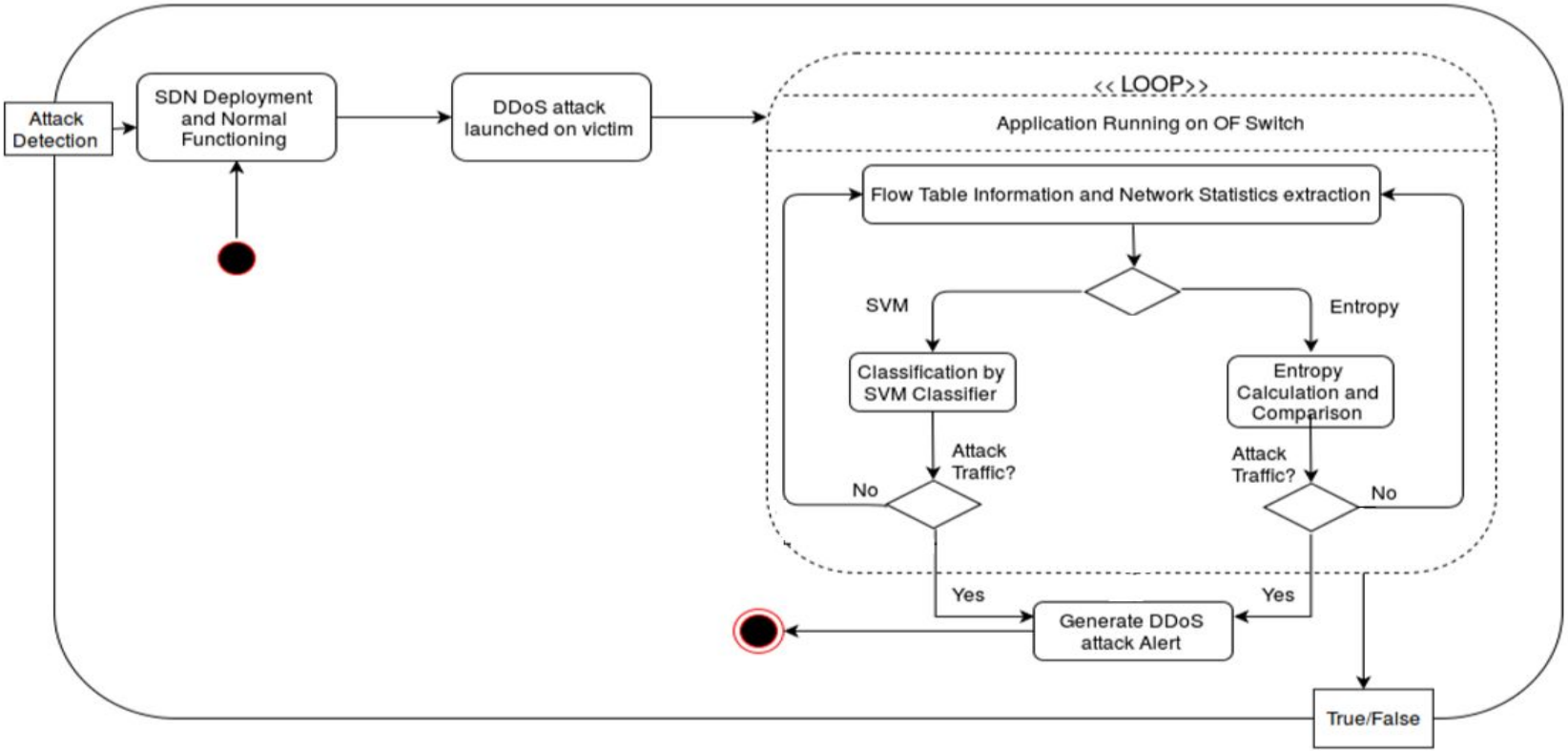
7a. Flow Diagram



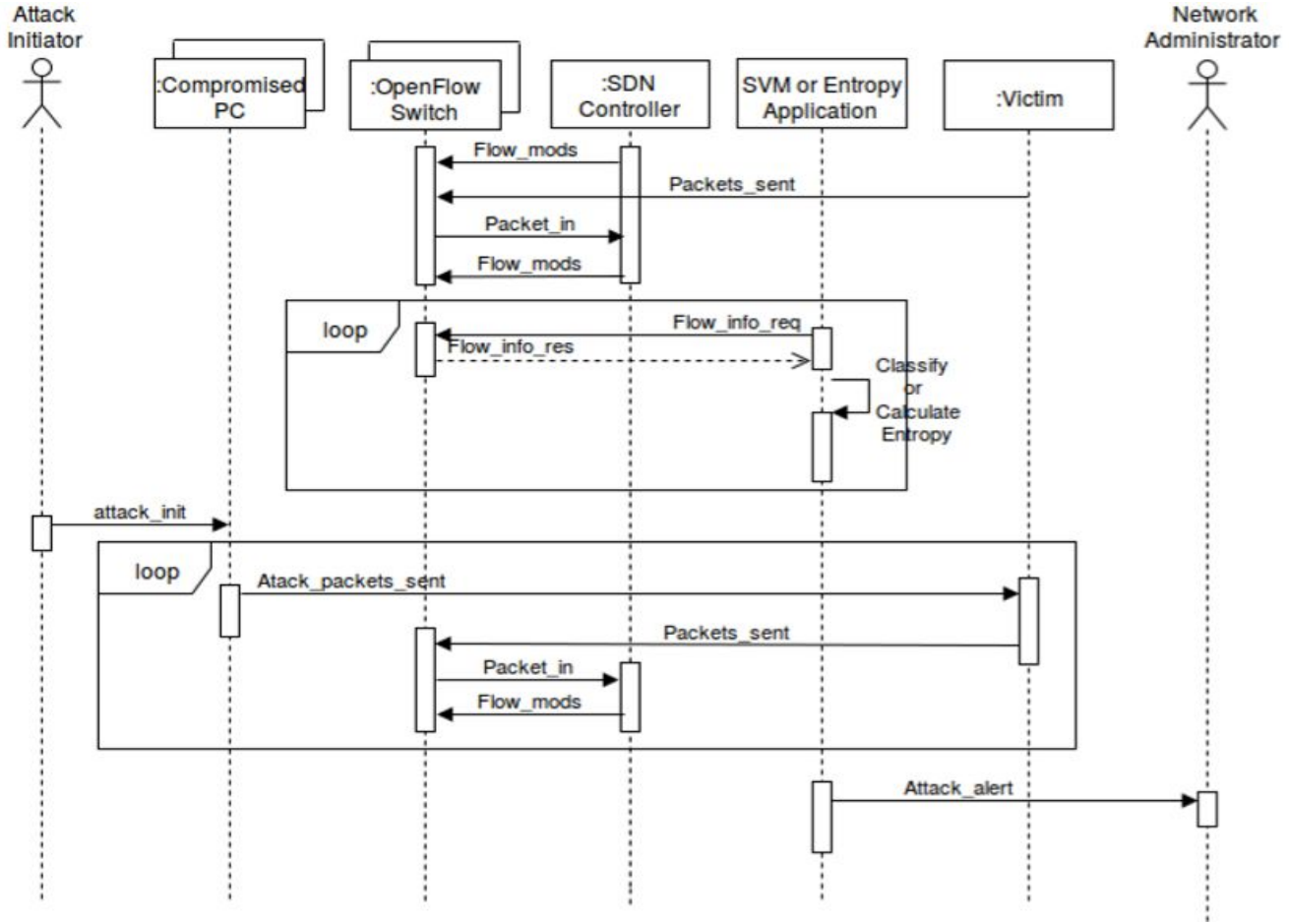
7b. Use Case Diagram



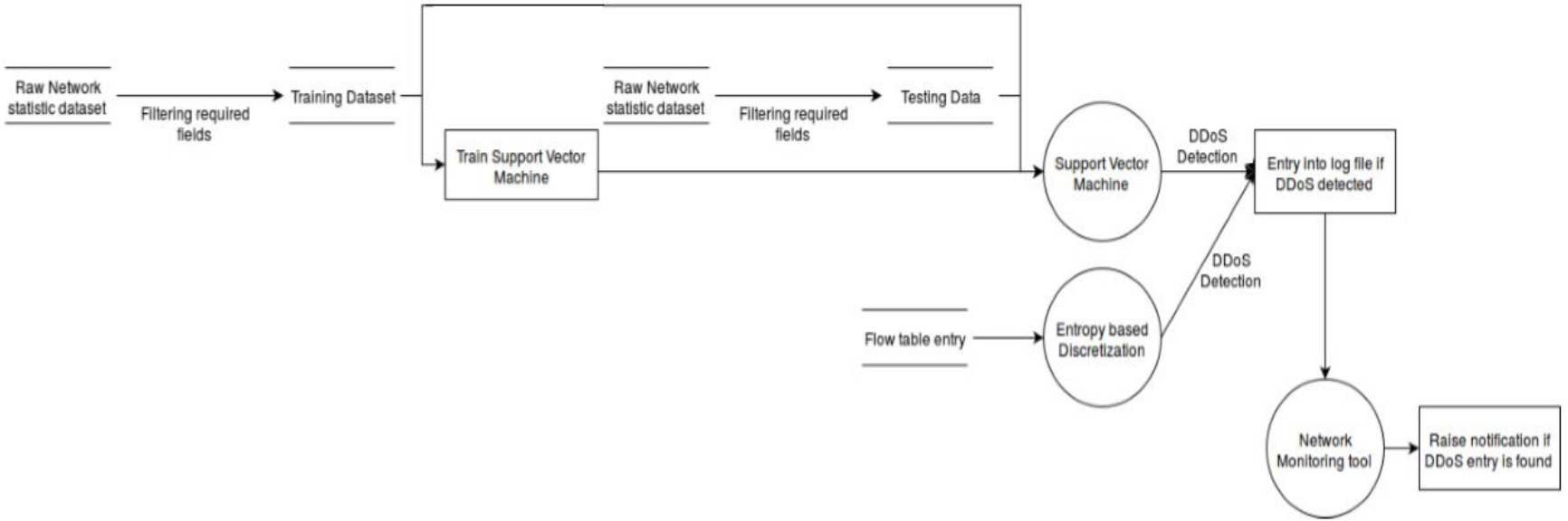
7c. Activity Diagram



7d. Sequence Diagram



7e. Data Flow Diagram



8. Implementation and Results

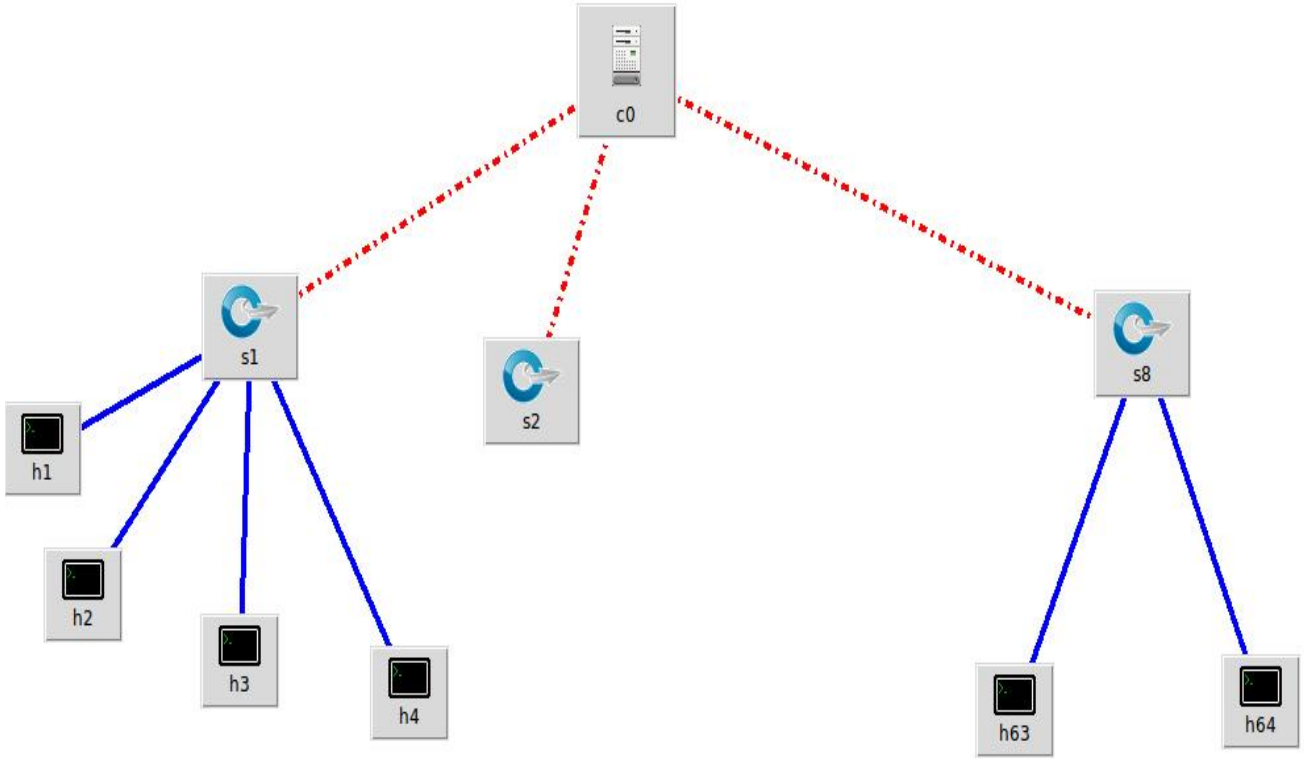
Implementation-

- **Dataset -** DDos attack traffic and normal traffic is generated which is further used as a dataset to train our model.
- Now the project is divided into 2 parts **---1 packet generation & analysis, ---2 attack and detection.**
- ***1-Packet generation*** *:*
- ***2- Attack detection :***

  3- After that for every 5 sets of process i.e. 250 packets entropy is below the threshold value then DDos is detected and those ip are blocked.

Results-

- The machine learning algorithm is applied on collected data to classify DDOS attacks ,that increases the efficiency .
- Using entropy based method,where DDos UDP attack is detected.


c0
s1
s2
s8
h1
h2
h3
h4
h63
h64

9.1 Work Done till date

- DDos UDP attack is detected using entropy based method where packets are generated using Scapy and analysed by the Poc Controller.

9.2 Work Planned

- Different types of attacks will be detected like ICMP, TCP, SYN flooding attacks, Smurf attack.
- SVM algorithm will be used for ddos attack detection and then accuracy and other metrics are calculated and compared with other algorithm.
- Result is evaluated by measuring a false alarm rate, detection rate and accuracy.

10.Paper Prepared

11.Conclusion

- SDN based Topology created.
- Packet generation using Scapy and analysis using POX controller.
- DDoS detected using Entropy based mechanism.

Bibliography

[1] SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks,Pedro Manso, Jose Moura, and Carlos Serrao,January 2019.

[2] A DDoS Attack Detection Method Based on SVM in Software Defined Network, Jin Ye, Xiangyang Cheng , Jian Zhu, Luting Feng, and Ling Song, April 2018.

[3] A Defense System for Defeating DDoS Attacks in SDN based Networks, Adel Alshamrani, Ankur Chowdhary, Sandeep Pisharody, Duo Lu ,Dijiang Huang, Acm 2017.