DDOS ATTACK DETECTION AND MITIGATION USING STATISTICAL AND MACHINE LEARNING METHODS IN SDN

NAME:- VISHAL KUMAR SINGH

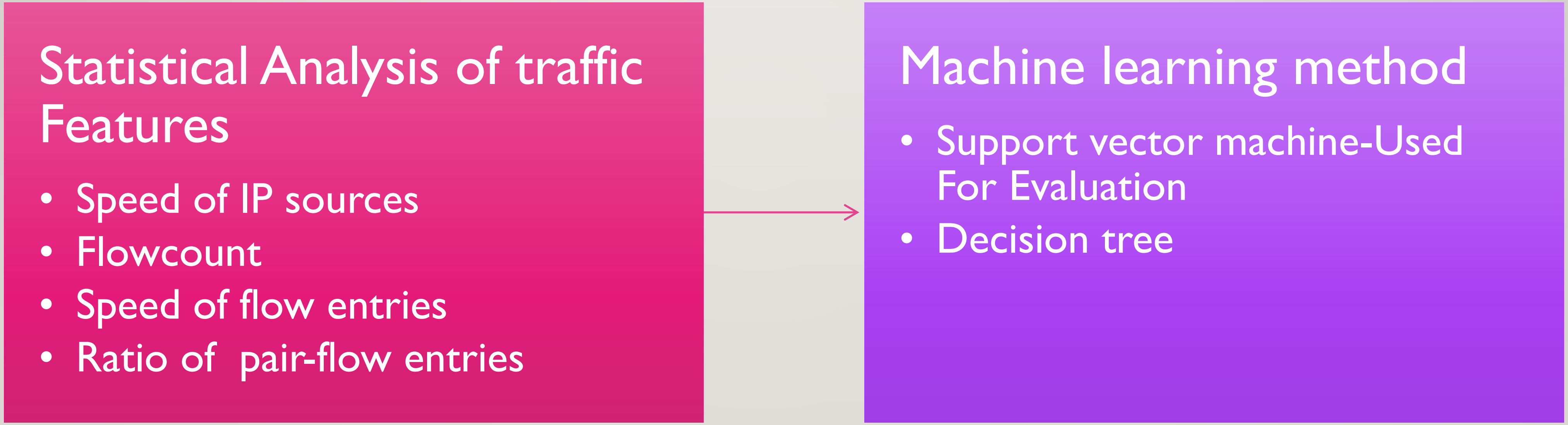
X18201687

CLICK HERE TO OPEN THE ONEDRIVE PROJECT VIDEO

RESEARCH QUESTION

- *“Can Software defined networking improve the detection and mitigation of DDOS attacks in a cloud environment”*

METHODOLOGY



Statistical Analysis of traffic Features

- Speed of IP sources
- Flowcount
- Speed of flow entries
- Ratio of pair-flow entries

Machine learning method

- Support vector machine-Used For Evaluation
- Decision tree

METHODOLOGY

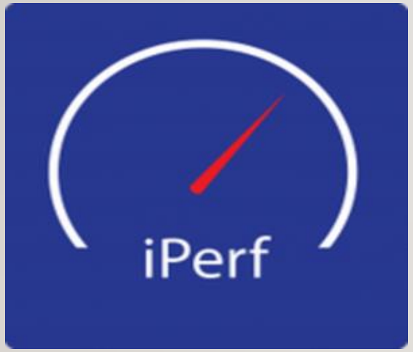
- Data Collection of the statistical features.
- Normal traffic
- Attack traffic

- SVM will be using this dataset to train itself and to predict the traffic as normal or DDOS attack traffic.

DEVELOPMENT TOOLS

- Platform setup on virtual machine with Ubuntu 20.04 OS
- OpenFlow Protocol for SDN
- Ryu controller – Python Based

SIMULATION TOOLS

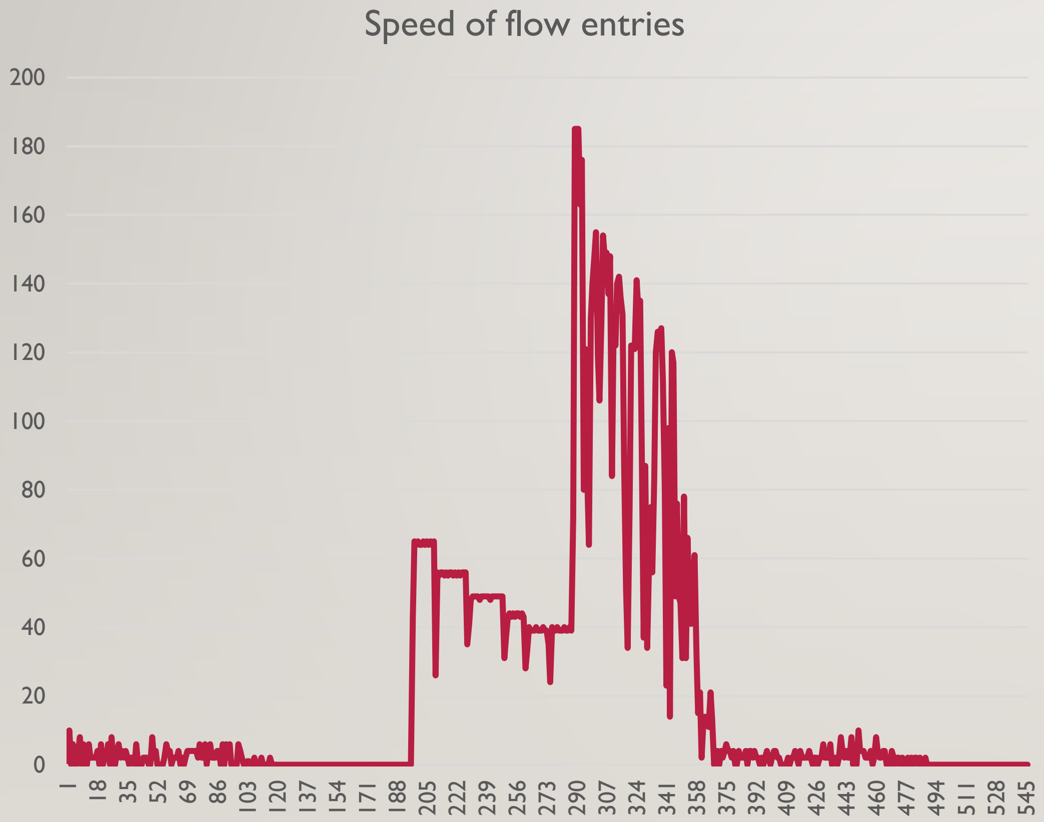


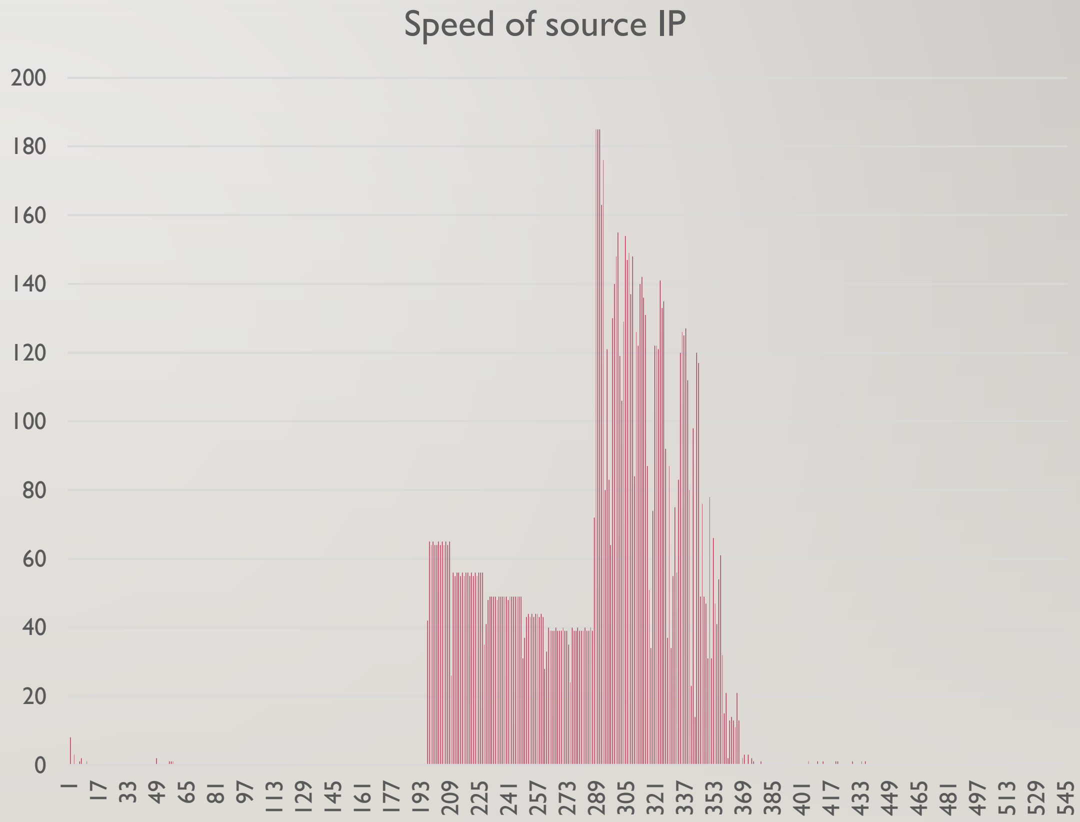
- Mininet
- Hping3
- Iperf

DEMONSTRATION OF THE PROJECT

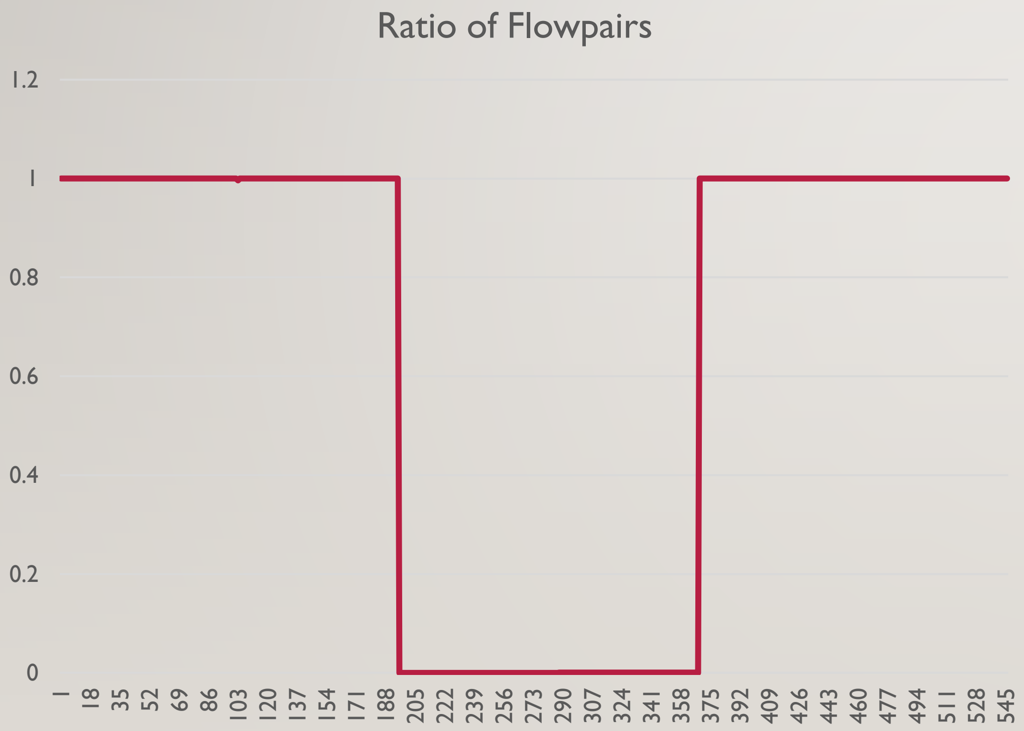
- OneDrive Video Link-
- https://studentncirl-my.sharepoint.com/:v:/g/personal/x18201687_student_ncirl_ie/EXOe698taxNFIZIjcpfPaEEBI8jAlhyWpxEQGeMP9_VmnQ?e=qd1ujN

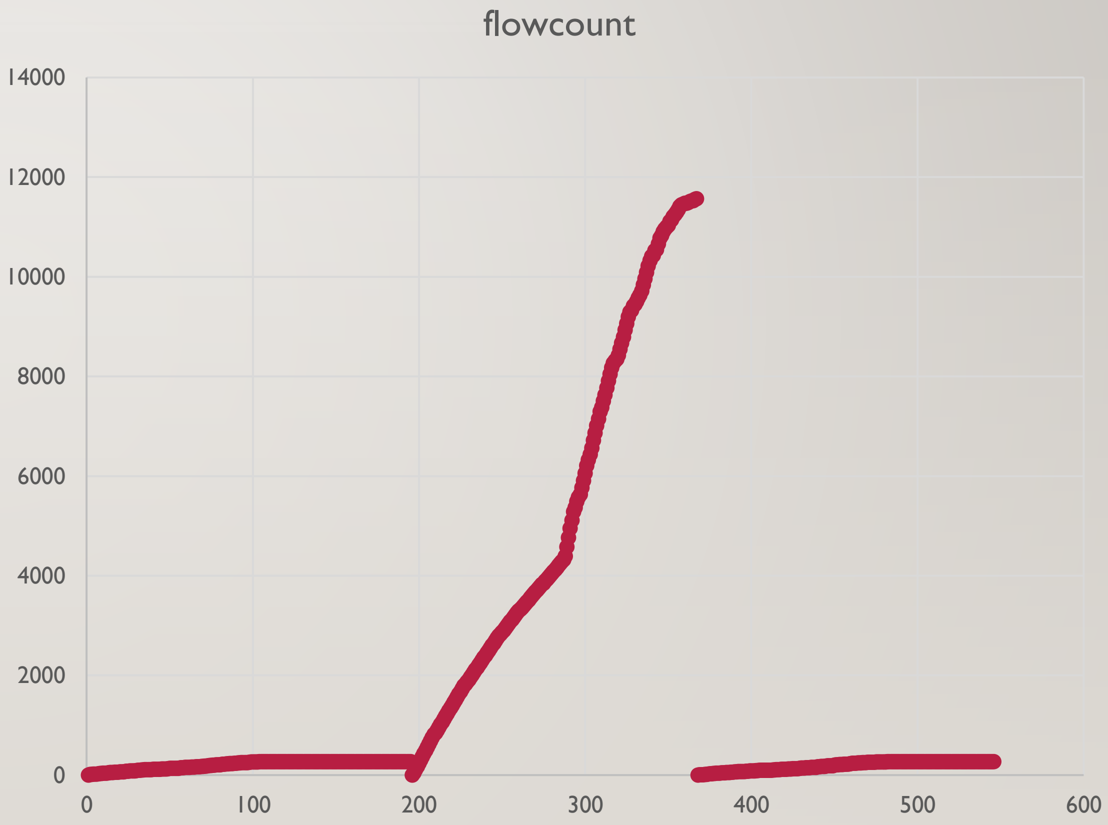
EVALUATED RESULTS

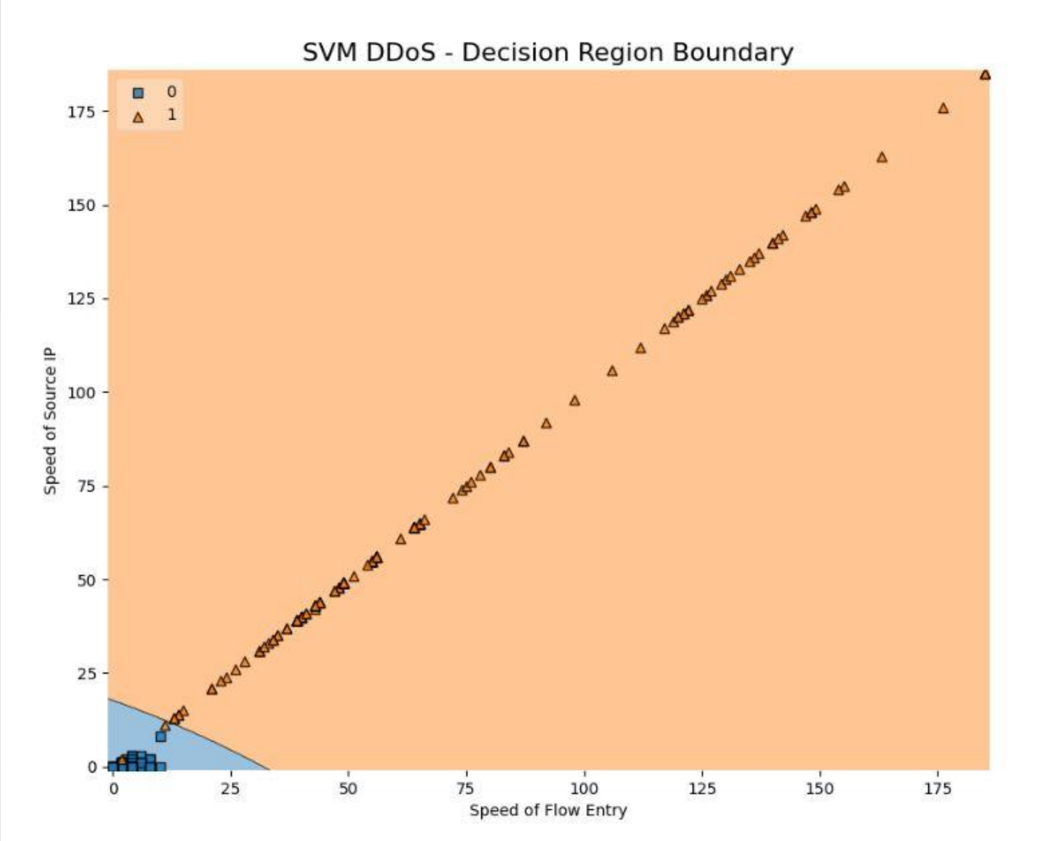

Speed of flow entries


Speed of source IP

EVALUATED RESULTS


Ratio of Flowpairs


flowcount



SVM PREDICTION GRAPH

LIMITATION OF THIS METHOD

- Faulty dataset trained to the SVM
- Trusted IP can be used to attack the network which the SVM would not detect.

FUTURE WORK

- Multiple controller and switches network topology
- More parameters defined and features extracted from the network
- Deployment in real time network traffic.

- Thank You