Kammavari Sangham (R) - 1952
K.S.INSTITUTE OF TECHNOLOGY
(Affiliated to VTU, Belgaum. Approved by AICTE, New Delhi)
No.14, Raghuvanahalli, Kanakapura Main Road, Bengaluru - 560109
Phone : 080-28435722 / 24, Fax : 080-28435723, Email : principal.ksit@gmail.com, Website : www.ksit.ac.in

Detection of DDoS attack using Machine Learning Algorithms in SDN Environment

BATCH-05

Guided By:

Mrs. Sougandhika Narayan

Assistant Professor

Dept of CSE, KSIT

Presented by:

Dakaraju Viswateja	1KS16CS018
Keerthi M	1KS16CS032
Kiran Kumar M	1KS16CS034
Manipi Manoj	1KS16CS039

Contents

Abstract

- Computer intrusion and attack detection has always been a significant issue in networked environment. In most cases, there are two levels in which an intrusion may take place, namely the system level and the network level.
- This project discusses an algorithms to protect from a specific kind of network-level attack called Distributed Denial of Service attack.

Introduction

- A distributed denial of service (DDoS) attack is when a hacker uses a botnet to send your web server an overwhelming number of HTTP requests in a very short period of time.
- DDoS attacks are the most common attacks in these technical era. So, that most of the important websites which are useful for finishing some of our daily tasks are DDoS attacked which is leading to unavailability of the web resources.
- By using wireshark a network monitor these bots are detected with the help of Machine Learning techniques which in turn prevents the attack of DDoS.

Literature Survey

- A Saboor et al[3] proposed the detection of DDoS attack based on correlation algorithm and IAFV algorithm. They used different time series with sliding windows for improving the detection rate.
- Saurav Nanda et al. [5] used Bayesian Network and achieved an accuracy of 91.68 % which indicates that out of 278,598 attacks, their model was able to accurately predict 254,834 attacks.
- Gisung Kim, et.al[6] proposed a hybrid learning model to detect the DDoS attack and to protect the Open Flow switches. They found that their model work well for unknown attacks also.

Literature Survey

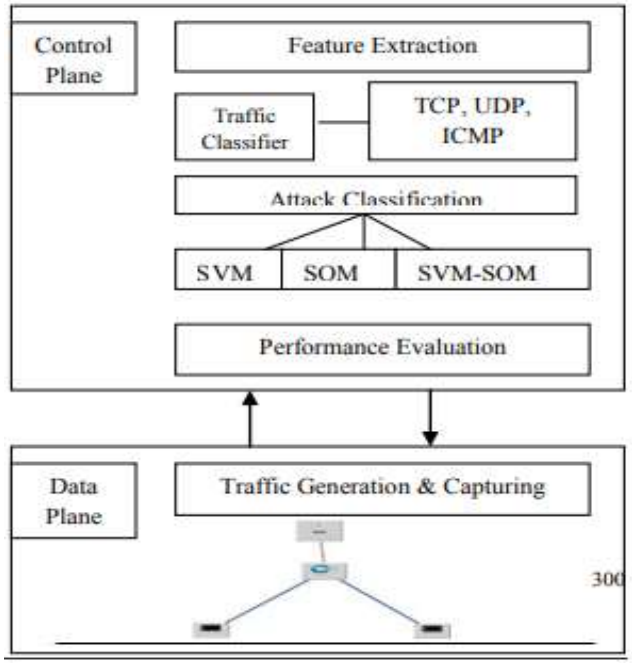
- Ahmad Y. Javaid et al. [7] used deep learning methods to detect the DDoS attack in SDN environment. They had collected the traffic from home wireless network (HWN) scenario. And they got 96.65% accuracy.
- Lohit Barki et al.[8] have used different machine learning techniques such as Naive Bayes, K-nearest neighbor, K-Means, K-medoids to detect the DDoS attack. They found that Naïve Bayes model work well compared to other considered algorithms with highest accuracy.
- The researchers have designed the system to detect DDoS attacks based on a decision-tree technique, and they traced back to the approximate locations of the attacker with a traffic flow pattern-matching technique .

Problem Identification

- The main aim of DDoS attacks is to prevent the legitimate user to access the service for a long time.In this attack, attacker tries to compromise the multiple numbers of hosts to send a huge amount of traffic intentionally towards a legitimate user. This leads to unavailability of service for large amount of time.
- Two Algorithms are used to detect the DDoS attack one is SVM (Support vector Machine) another is SOM (Self Organized Map).Since SVM is a supervised machine learning model, it should be trained with labelled data only.
- In case of SOM, it is an unsupervised machine learning model, as they apply competitive learning as opposed to error-correction learning and in the sense that they use a neighborhood function to preserve the topological properties of the input space..
- In order to handle this DDoS attack, we have proposed a combination of two machine learning based model with Support Vector Machine (SVM) and Self Organized Map(SOM).

Methodology

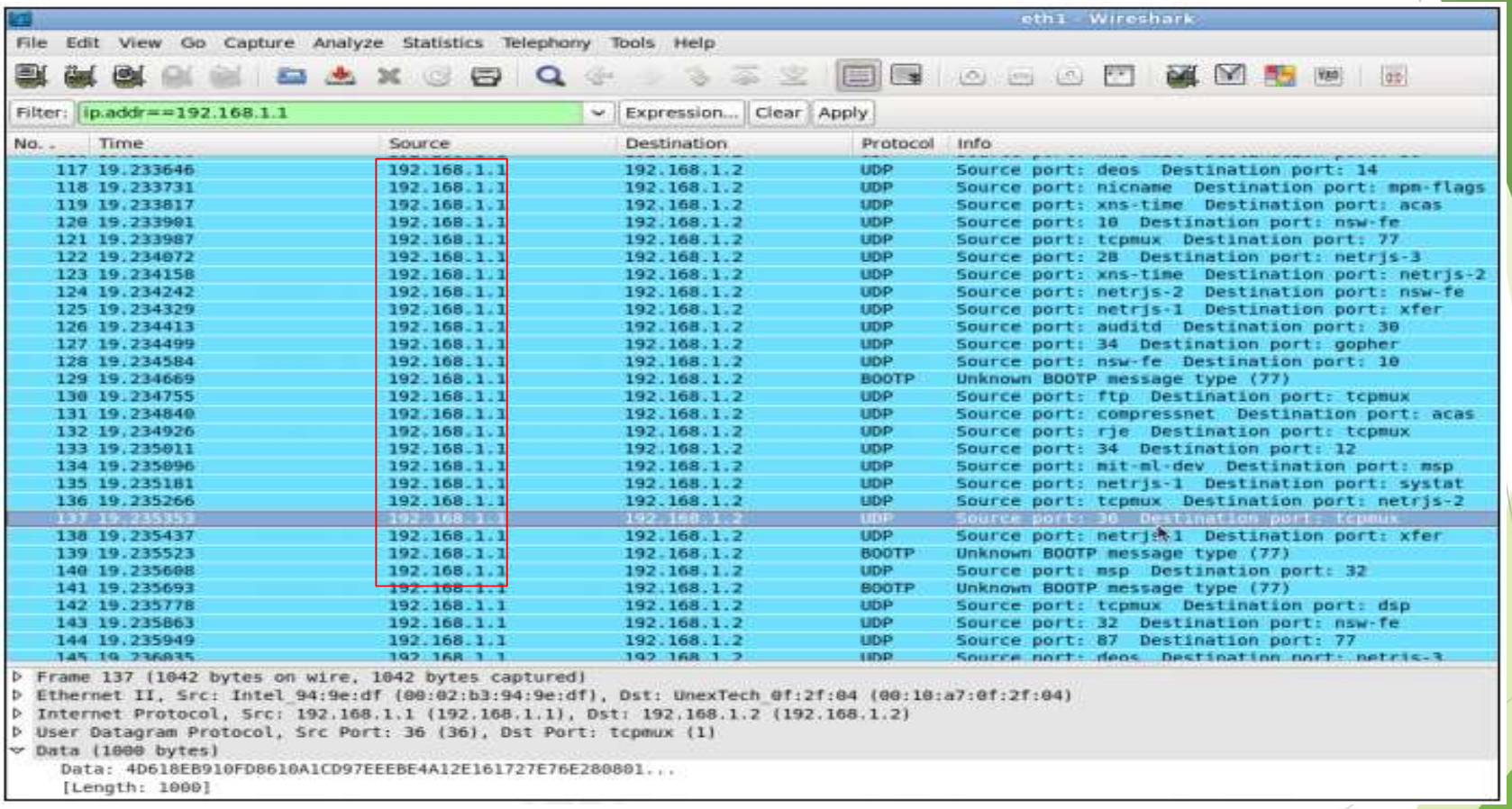
- Below Figure shows the architecture of our proposed method.



wireshark

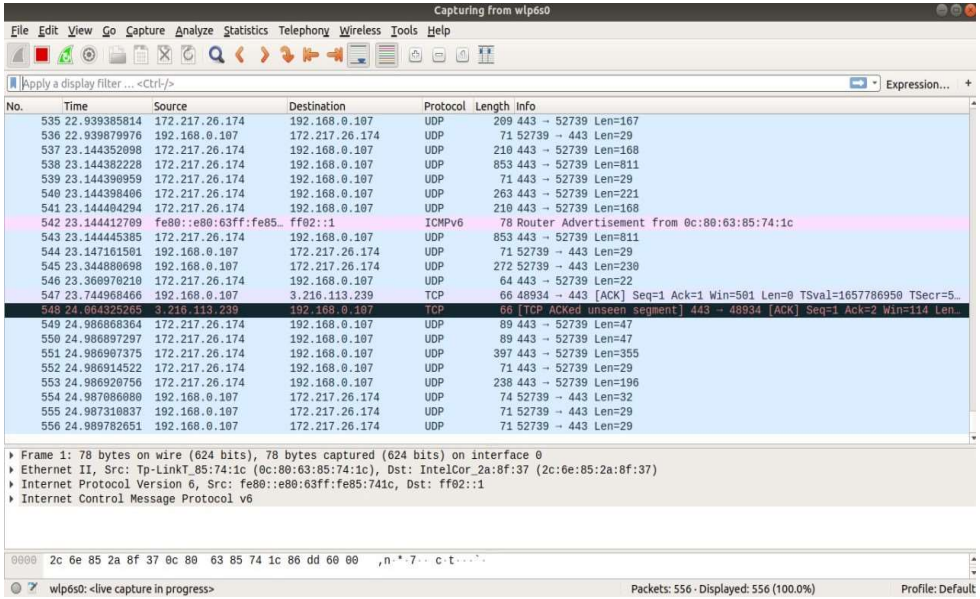
Topology

Methodology

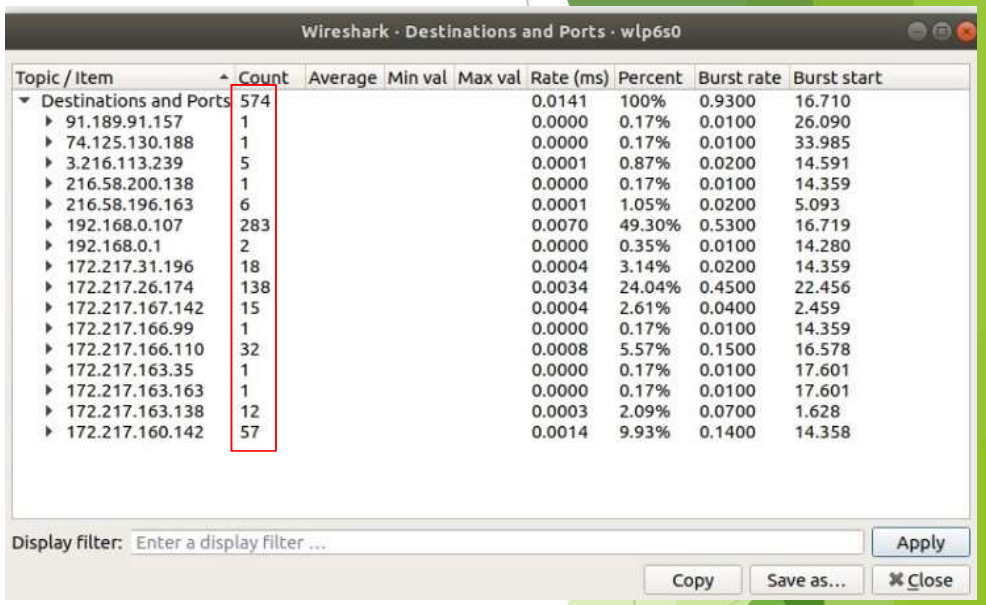


Flooding a Particular Network

Methodology



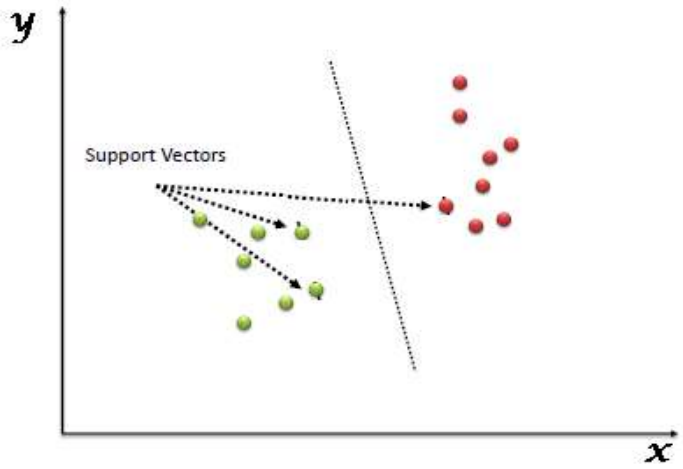
Monitoring particular network using Wireshark



Analyzing the network and generation of DataSet

Methodology

- "Support Vector Machine" (SVM) is a supervised machine learning which can be used for both classification or regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well (look at the below snapshot).



SVM Algorithm Classification

Project Goal

- The main goal of our project is to build a model which must be able to detect a DDoS attack.

Contribution to Society

- Prevention against DDoS attacks is the most desirable defence technique to fight against the DDoS attacks. DDoS put an immense threat to the resources of the victim as well as to the network bandwidth and Infratructure.
- Therefore, if an attack has been already launched and become successful, it may cause significant compromise to the Victim's system.
- Thus, protection against DDoS attacks is more effective against DDoS attack traffic as well as manages large attack load before it may cause the attack to be successful. This ensures normal operation of the victim.

References:

- https://github.com/jivoi/awesome-ml-for-cybersecurity
- https://www.analyticsvidhya.com/blog/2017/09/understaing-support-vector-machine-example-code/
- https://helpdeskgeek.com/how-to/how-to-identify-a-ddos-attack-on-your-server-stop-it/
- https://www.svm-tutorial.com/2017/02/svms-overview-support-vector-machines/