Department of Information Technology

V R Siddhartha Engineering College

Preventing Network Attacks: An Integrated Approach using Support Vector Machine (SVM) and Software Defined Networking (SDN)

Network Security, Cyber Security
and Information Security

B.Tech in Information Technology

Mini Project Review Presentation

Presented by

Mr. Dinakar Laxmi Viswanath (208W1A1201)

Mr. Sotsava Skandhaa (208W1A1202)

Under the guidance of

S. Kranthi , Assistant professor

AGENDA

- Introduction
- Problem Statement
- Objectives of the Project
- Literature Review and Summary
- Dataset and Requirements
- Architecture diagram
- Description of Base Paper

INTRODUCTION

The field of network security is a critical aspect of modern computing systems, with software-defined networking (SDN) offering new opportunities for effective security. The objective of this project is to explore the potential of deep learning algorithms for intrusion detection in SDN environments. The project involves selecting a DDOS attack network security dataset from Kaggle and using deep learning techniques to train a model that can detect and classify different types of attacks. The trained model will be integrated with a software-defined network (SDN) environment, which will use controllers to block the detected attack. This project aims to demonstrate the feasibility and effectiveness of deep learning for intrusion detection in SDN and contribute to the advancement of network security research.

PROBLEM DEFINITION

The increasing number of cyber-attacks on networks has become a major concern for organizations and individuals. Traditional security solutions, such as firewalls and intrusion detection systems, are becoming less effective in defending against these attacks. This project aims to address this problem by using a deep learning model-based solution for detecting and preventing DDOS network attacks in a software-defined networking (SDN) environment. The solution uses a trained linear Support Vector Machine (SVM) algorithm model to control the behavior of one or more SDN controllers to prevent attacks.

OBJECTIVES

- To develop an efficient machine learning model that can classify the given network traffic dataset to various attacks with maximum accuracy.

- Using SDN controllers to stop traffic from a host based on its Mac address.

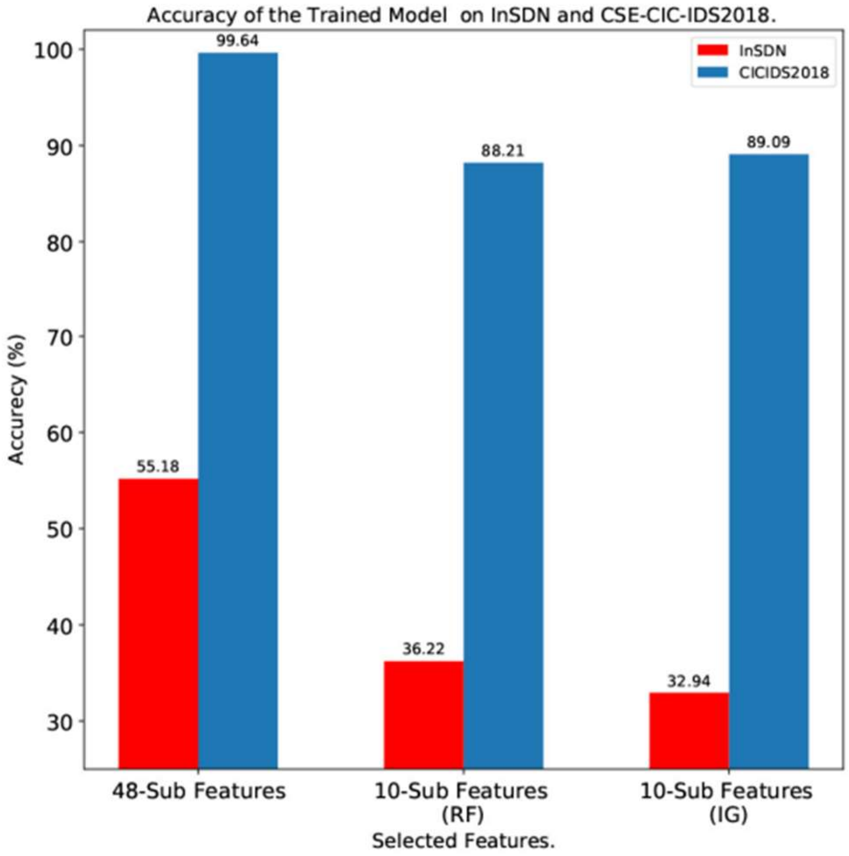
LITERATURE SURVEY

Title of the Project	Authors	Methodology	Source	Summary
A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs	Mahmoud Said El Sayed Nhien-An Le-Khac , Marianne A. Azer and Anca D. Jurcut (2020)	LSTM-Autoencoder	IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING	Our approach provides a high detection rate and presents a more efficient better time to build the model. We further tested the trained model on the performance of the SDN controllers to evaluate how the used dataset can impact on the performance of the SDN controller. The results showed that the proposed approach does not deteriorate the network performance
Deep Neural Networks for Intrusion Detection in Software-Defined Networking	Wang et al. (2019)	Random Forests	IEEE (Institute of Electrical and Electronics Engineers)	The authors evaluate the performance of their proposed solution using both simulated and real-world network security datasets and show that deep neural networks can significantly improve the accuracy of intrusion detection in SDN

Title of the Project	Authors	Methodology	Source	Summary
End-to-end intrusion detection in software-defined networks using deep reinforcement learning	Qin et al. (2019)	A K-mean clustering and random forest based multilevel model .	IEEE (Transactions on Network and Service Management)	The proposed solution can effectively detect various types of network attacks in real-time and provide a flexible and scalable solution for SDN security.
Anomaly-based Intrusion Detection in Software-Defined Networks: A Deep Learning Approach	Zhang et al. (2019)	Naïve Bayes classifier	IEEE Access	The proposed method uses an autoencoder to learn the normal behavior of the network and identify anomalies, which are then classified as either benign or malicious using a deep neural network.
Distributed abnormal behavior detection approach	Naila Marir HuiqiaWa Guangshe Bingyang	DBN and SVM	IEEE, 2018	DBN is used to extract SVM ensemble characteristics and to anticipate the voting process.

REVIEW PAPER : Mahmoud Said El Sayed Nhien-An Le-Khac , Marianne A. Azer and Anca D. Jurcut. "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs." In 2022 IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

SUMMARY :



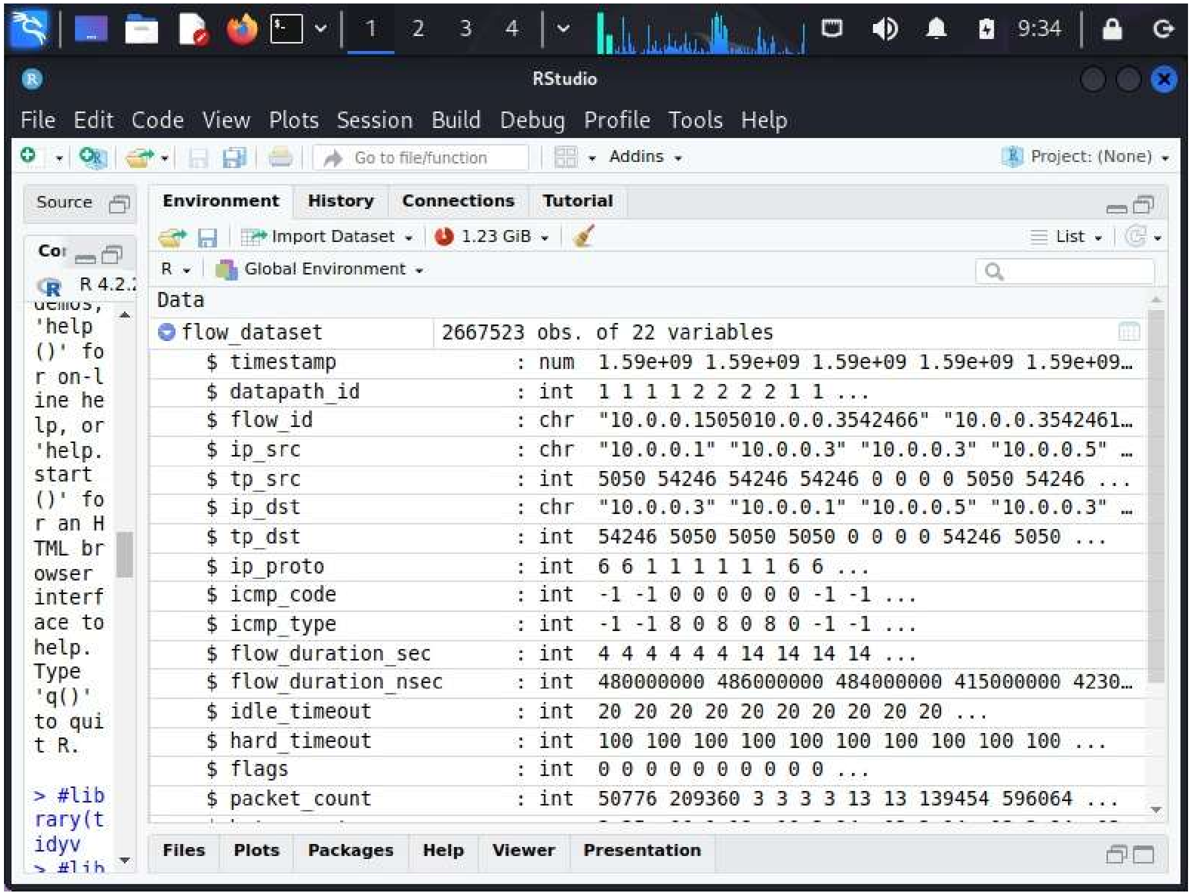
REVIEW PAPER : Mahmoud Said El Sayed Nhien-An Le-Khac , Marianne A. Azer and Anca D. Jurcut. "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs." In 2022 IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

SUMMARY :

The aim of this work is to reduce the redundant or irrelevant features without any significant impact on the classification accuracy. We have selected 10 features out of available 48 features using two common feature selection methods IG and RF. The approach provides a high detection rate and presents a more efficient better time to build the model. We further tested the trained model on the performance of **More Than One SDN controller** to evaluate how the used dataset can impact on the performance of the SDN controller. The results showed that the proposed approach does not deteriorate the network performance.

DATASET DESCRIPTION

- We have a huge amount of data entries (2667523 Observations)
- This is a snapshot of the sample data with column names.


1
2
3
4
9:34
RStudio
File Edit Code View Plots Session Build Debug Profile Tools Help
Go to file/function
Addins
Project: (None)
Source
Environment History Connections Tutorial
Import Dataset
1.23 GiB
List
R
Global Environment
Files Plots Packages Help Viewer Presentation

```
Co
R 4.2.
demos,
'help
()' fo
r on-l
ine he
lp, or
'help.
start
()' fo
r an H
TML br
owser
interf
ace to
help.
Type
'q()'
to qui
t R.

> #lib
rary(t
idyv
> #lib
```

```
Data
flow_dataset          2667523 obs. of 22 variables
    $ timestamp          : num  1.59e+09 1.59e+09 1.59e+09 1.59e+09 1.59e+09…
    $ datapath_id        : int  1 1 1 1 2 2 2 2 1 1 ...
    $ flow_id            : chr  "10.0.0.1505010.0.0.3542466" "10.0.0.3542461…
    $ ip_src             : chr  "10.0.0.1" "10.0.0.3" "10.0.0.3" "10.0.0.5" …
    $ tp_src             : int  5050 54246 54246 54246 0 0 0 0 5050 54246 ...
    $ ip_dst             : chr  "10.0.0.3" "10.0.0.1" "10.0.0.5" "10.0.0.3" …
    $ tp_dst             : int  54246 5050 5050 5050 0 0 0 0 54246 5050 ...
    $ ip_proto           : int  6 6 1 1 1 1 1 1 6 6 ...
    $ icmp_code          : int  -1 -1 0 0 0 0 0 0 -1 -1 ...
    $ icmp_type          : int  -1 -1 8 0 8 0 8 0 -1 -1 ...
    $ flow_duration_sec  : int  4 4 4 4 4 4 14 14 14 14 ...
    $ flow_duration_nsec : int  480000000 486000000 484000000 415000000 4230…
    $ idle_timeout       : int  20 20 20 20 20 20 20 20 20 20 ...
    $ hard_timeout       : int  100 100 100 100 100 100 100 100 100 100 ...
    $ flags              : int  0 0 0 0 0 0 0 0 0 0 ...
    $ packet_count       : int  50776 209360 3 3 3 3 13 13 139454 596064 ...
```

REQUIREMENTS

User Interface:

- This system's user interface is the Linux os, which is a user-friendly interface.

Hardware Interfaces:

- Oracle Virtual Machine, Kali Linux, and Kaggle

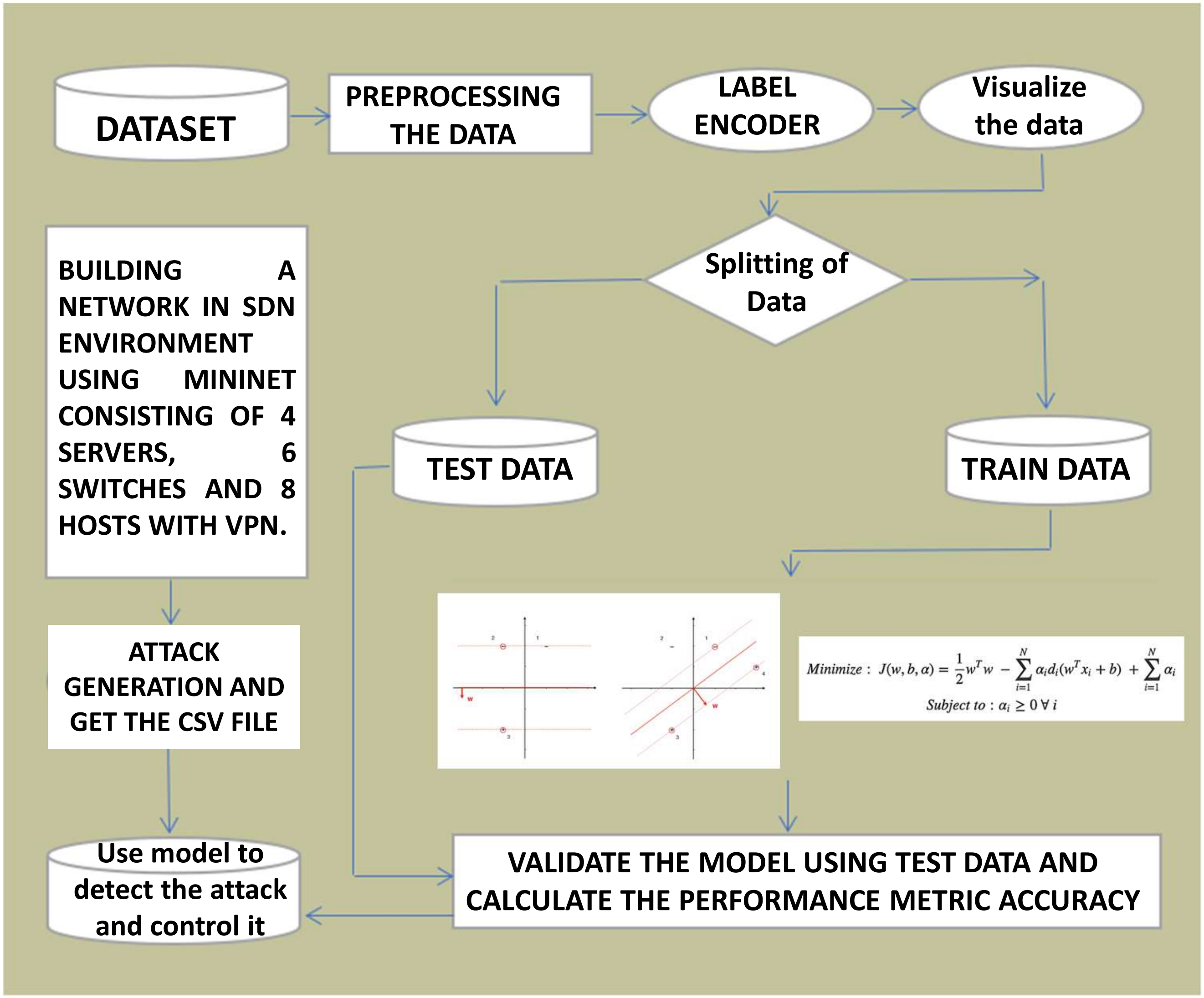
Software Interfaces:

- Required modules (tidyverse, e1071, caret, graphics, ggplot2, class, KNN, SVM)

Hardware Requirements:

1. Processor – Pentium-IV
2. RAM – 4GB (Minimum)
3. HDD/SSD – 256GB (Minimum)

Architecture Diagram



DATASET

PREPROCESSING THE DATA

LABEL ENCODER

Visualize the data

Splitting of Data

TEST DATA

TRAIN DATA

$$\textit{Minimize} : \; J(w,b,\alpha) = \frac{1}{2}w^T w - \sum_{i=1}^{N} \alpha_i d_i (w^T x_i + b) + \sum_{i=1}^{N} \alpha_i$$

$$\textit{Subject to} : \alpha_i \geq 0 \; \forall \, i$$

VALIDATE THE MODEL USING TEST DATA AND CALCULATE THE PERFORMANCE METRIC ACCURACY

BUILDING A NETWORK IN SDN ENVIRONMENT USING MININET CONSISTING OF 4 SERVERS, 6 SWITCHES AND 8 HOSTS WITH VPN.

ATTACK GENERATION AND GET THE CSV FILE

Use model to detect the attack and control it

DESCRIPTION OF BASE PAPER

[1]. Mahmoud Said El Sayed Nhien-An Le-Khac , Marianne A. Azer and Anca D. Jurcut. "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs." In 2022 IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

In this paper, the goal is to find the most important features that can help detect DDoS attacks in SDN networks more accurately. Two methods, Information Gain (IG) and Random Forest (RF), are used to do this. By selecting the most relevant features, the system can better spot abnormal activities and reduce false alarms.

Additionally, a technique using Deep Learning (DL) is suggested to deal with DDoS attacks in SDNs. This technique, based on Long Short Term Memory (LSTM) and Autoencoder, helps recognize these attacks. The researchers tested everything on three different datasets: InSDN, CICIDS2017, and CICIDS2018. They also checked how this DL method affects the network's performance and found that it identifies DDoS attacks well without slowing down the network significantly.