# DDoS Detection in SDN using ML

## CSE 310 Group Project

Rediet Negash, Merry Mekonnen, Sudara Ranasinghe

# The problem

## SDN

**Software defined networking (SDN)** is an approach to using open protocols, such as **OpenFlow**, to apply globally aware software control at the edges of the network to access network switches and routers that typically would use closed and proprietary firmware.

## DDoS attack

A **distributed denial-of-service (DDoS)** attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

## DDoS attack on SDN

**SDN controller is highly vulnerable to DDoS attacks** due to its centralized nature. Thus, detection of the DDoS attacks in the controller at the earliest is an important research issue, but very few studies have been carried out in the context of SDN.

# Solution

Early detection of DDoS attacks on SDN using ML

The SDN controller can be injected with a trained ML model that will monitor network traffic and detect a DDoS attack at its early stages.

# Challenges deep-dive

## Early Detection of DDoS

**LSTM can be used to detect the attack.**

LSTM is used for time series analysis classification.

## Block DDoS attack

**POX controller blocks attacked switches/ports.**

An openflow control signal can be sent to the attacked switch to discard packets at the attacked ports.

## Enable normal traffic to continue

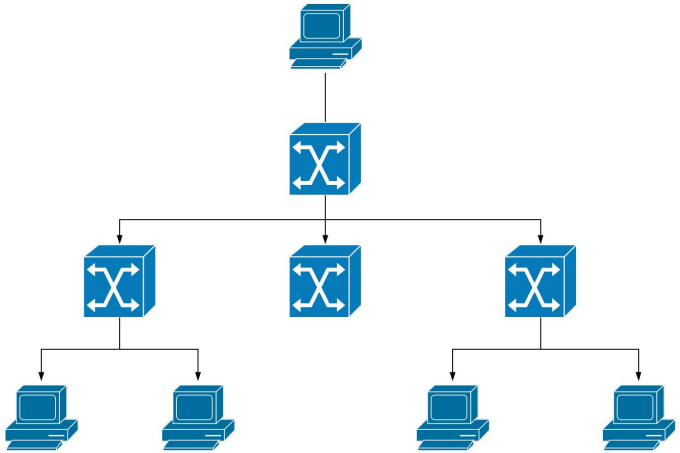
**POX controller will redirect normal traffic.**

The ML model in the controller will continue to monitor network traffic for DDoS attacks.

# Implementation

# Setup

- Github repository:
  - https://github.com/sudara999/SDN_DDos_Detection_ML
- Mininet setup with POX controller



# Project Breakdown

## 1. Packet Generation

- Module to generate normal traffic
  - Send packets from random source IPs to random destination IPs
- Module to launch a DDoS attack
  - Send many packets from random source IPs to a single destination IP in the network.
- Capture packets generated to train the ML model.

## 2. DDoS Detection

- LSTM model that trains on the generated dataset
- POX switch that loads the trained model and monitors the network traffic for DDoS attacks.

# >90%

Evaluation based on **accuracy** of ML algorithm

# Experiment

# Frameworks:

- Pox controller
- L3 learning switches
- Mininet
- Virtual machine as a platform
- Deep learning algorithms
  - => Keras (model)
  - => LSTM (RNN layer)

# Data Generation Process

Steps:

- Run the Pox controller:
  python pox.py forwarding.lstm_switch

- Run the mininet and build the topology:
  “mn  --switch ovsk --topo tree, depth=2, fanout = 8, --controller=remote, ip = “127.0.0.1”, port = 6633”

- Access individual nodes:
  “xterm  <h1 - h64>” - this will create a terminal for either one of the 64 nodes

- Create traffic:
  - Normal traffic
  - Attacks
    - UDP single attack
    - UDP multiple attack
    - UDP multiple fast attack

# Packet Capture

Different types of packets were captured and saved in a csv file

- Few cleaning processes were done to make sure the received data fits well in the training model
- After the data was sufficiently cleaned,  the data which is a collection of packets got reshaped into a 3-dimensional numpy Array: sequences, timesteps, features.

# Training

- Once the data was successfully reshaped, it got passed into a training model which has multiple layers ,optimizer, and other parameters.

- The trained data was saved and was loaded to make predictions on new packets.

# Prediction

- The loaded data had been split into a training data and a testing data with a ratio of 0.8:0.2 respectively.
- Testing data was able to be predicted using the trained model.
- The trained model successfully predicted the testing data with an accuracy of 93.25%.

# Links

Repo:

https://github.com/sudara999/UDP-Attack-Detection-in-SDN-using-ML

Demo:

https://youtu.be/J82LMIj5gRE