KOHAT UNIVERSITY OF SCIENCE & TECHNOLOGY
3rd INTERNATIONAL CONFERENCE ON COMPUTATIONAL INTELLIGENT SYSTEMS 2024
KOHAT, PAKISTAN.
December, 2024

Push-ACK Flood DDoS Attack Detection in SDN Environment Using Deep Learning

M. Saibtain Raza, M. Nowsin Amin Sheikh and I-Shyan Hwang
Department of Computer Science and Engineering, Yuan Ze University

Presenter: Muhammad Saibtain Raza

Outline

- Overview
- Challenges
- Methodology
- Results
- Conclusion & Future work
- Q/A

Overview SDN and DDOS

- SDN creates a centralized brain for the network that can communicate and command the rest of the network
- A Distributed Denial of Service attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources

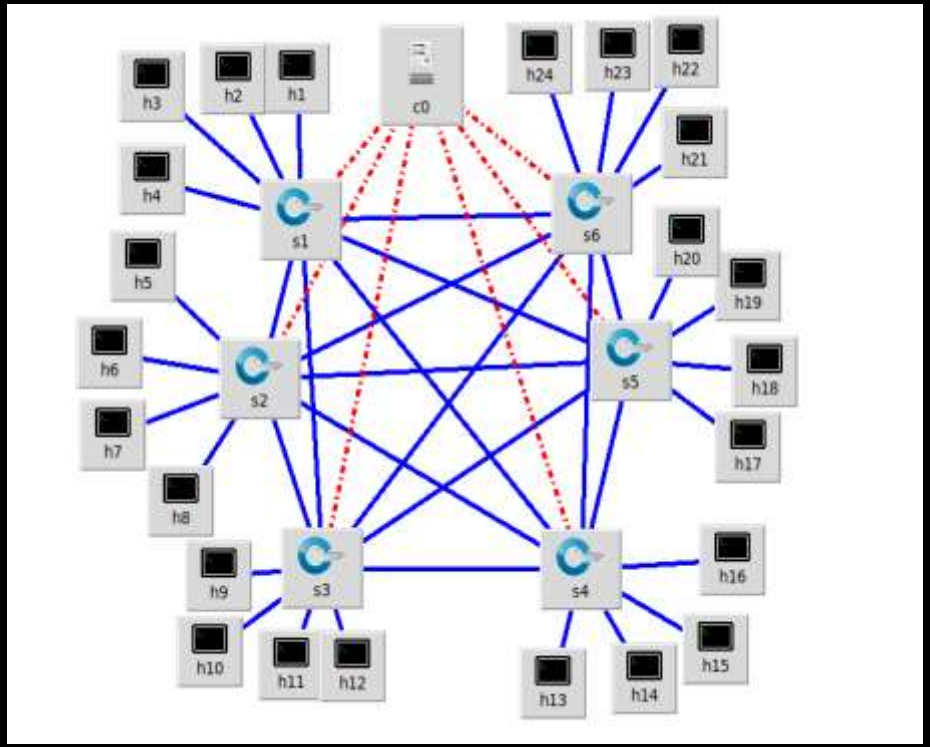
Software Defined Network

- Challenges in security
  - Fake Traffic flow
  - Forwarding Device Attack
  - Vulnerability of Communication Channel
  - Authenticity

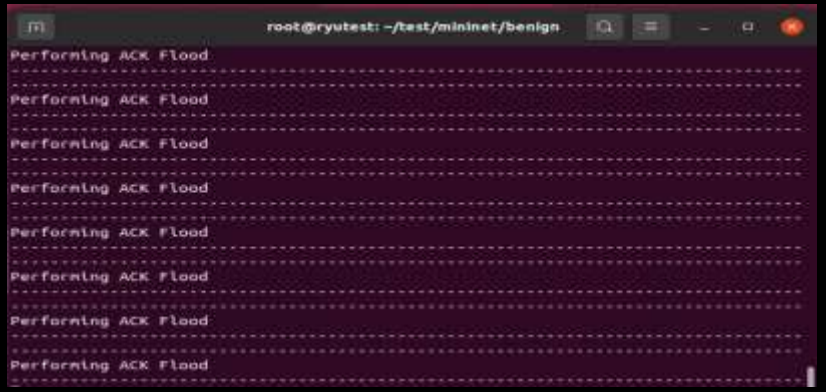
Our Methodology

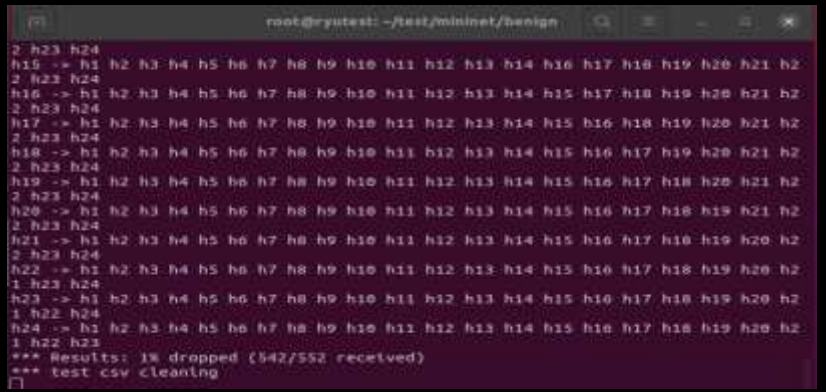
- Following major steps
  - Best features selected
  - Generate Mesh Topology
  - Mininet with RYU controller
  - Traffic collected (700k)
  - Preprocessing and model applying
  - Detected PUSH-ACK with high accuracy

Topology and Data collection



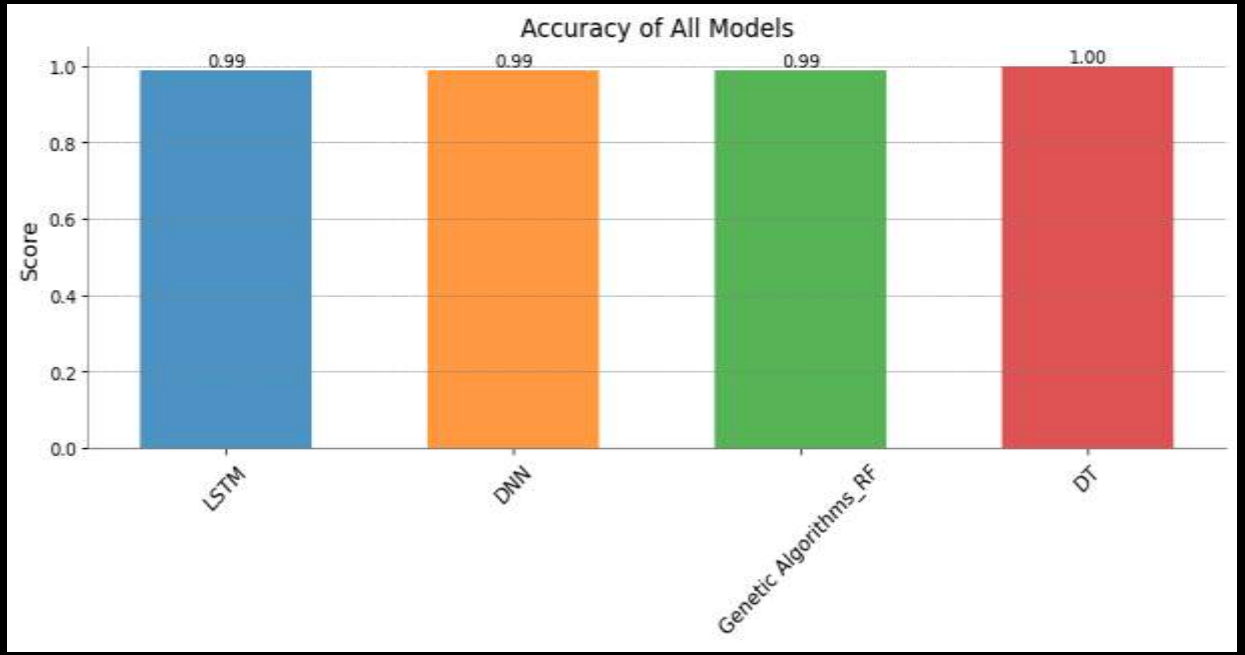
Mesh Topology





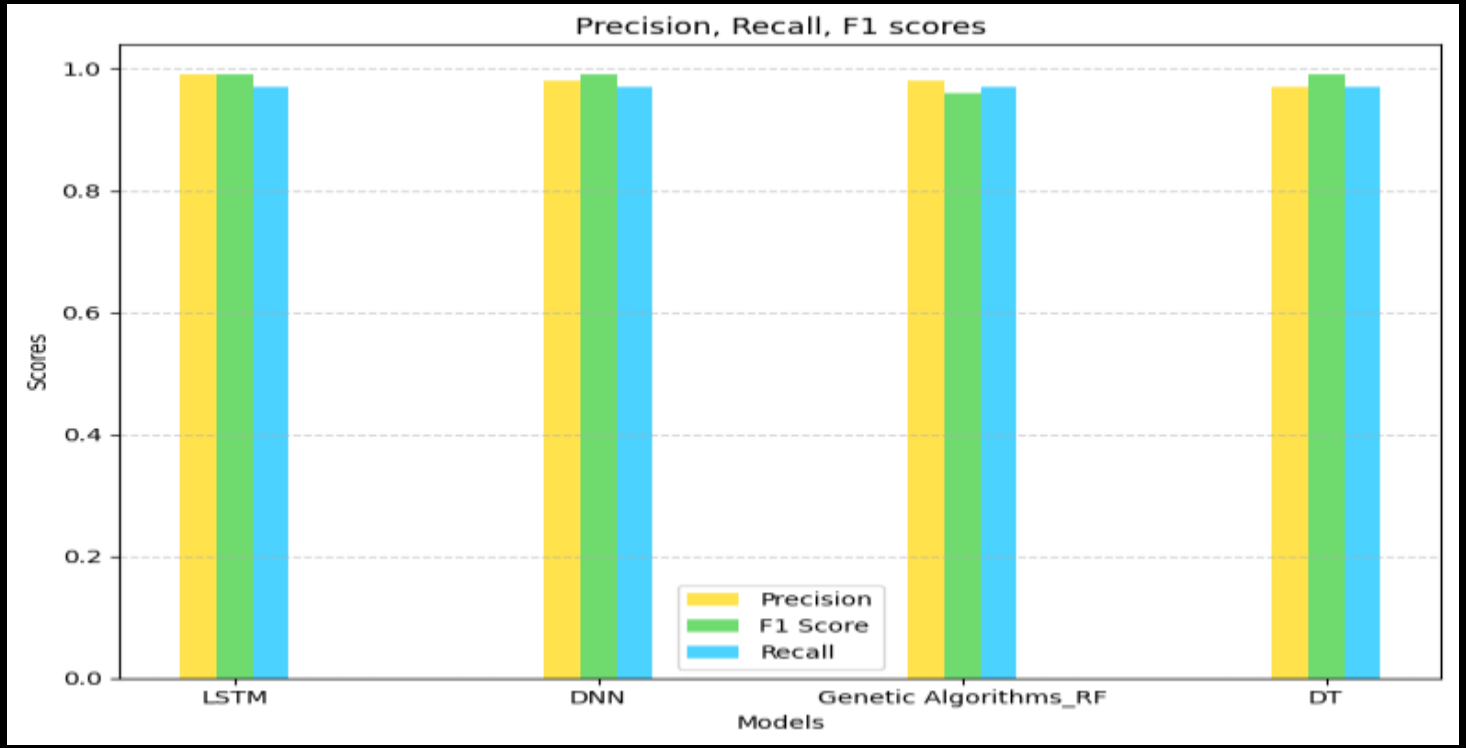
Results

- Applied Model
  - LSTM
  - DNN
  - Genetic_RF
  - Decision Tree



Accuracy

Performance Matrices



Scores

Best Features

Features	Description
Source port	Device identify
Timestamp	Network traffic tracking in real-time
Tp_dst	Determine which device is the connection's target.
Icmp_type	Improves Network Diagnostics with messages
Flow_duration_nsec	lifespan of a flow
Idle_timeout	Delete flow entries that are not referenced to aid in flow entry management.
Byte_count	The entire amount of data related to a flow.
Packet_count_per_second	Assist in monitoring the speed of packet transmission

Conclusions & Future Work

- We have found Push-ACK flood attacks can be easily detected by these four models
- Genetic algorithms can be useful for traffic data analysis
- How to mitigate DDOS attacks in SDN in real time?
- How to use fuzzy models in SDN to improve security

Thank You for Attention
Any Questions?