



KOHAT UNIVERSITY OF SCIENCE & TECHNOLOGY INTERNATIONAL CONFERENCE 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



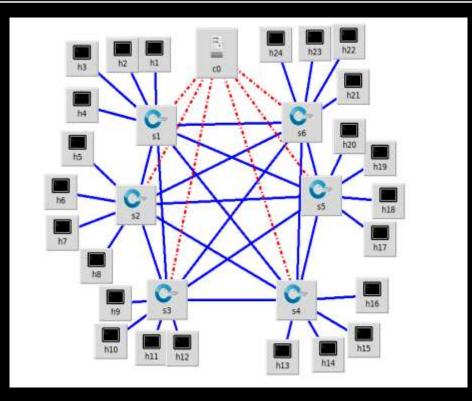
Our Methodology

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

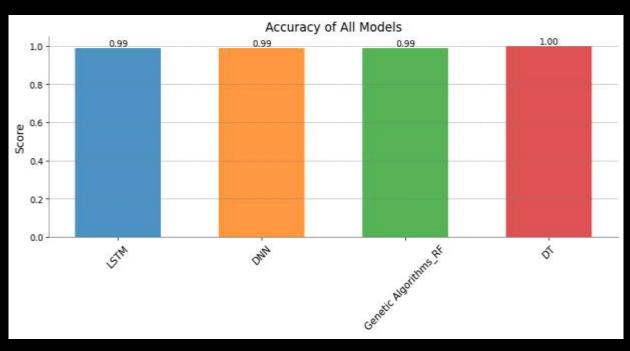


	root@ryutest	t: -/test/mininet	/benign	Q =		e. 🐵
Performing ACK Flood						
Performing ACK Flood						
Performing ACK Flood						
Performing ACK Flood						
Performing ACK Flood						
Performing ACK Flood						
Performing ACK Flood						
Performing ACK Flood						marile 1
			- CATAT			
	root@ryutest	:-/test/mininet	/benign			
2 h23 h24	CONTRACTOR OF STREET	CANADA NASARANA	NATE OF STREET	energy and	THE RESERVE	Marine Marine
his hi h2 h3 h4 h5 h6 2 h22 h24						
his -> hi h2 h3 h4 h5 h6 2 h23 h24	h7 h8 h9 h10	hii hiz hii	h14 h15 h	117 h10	h19 h26	h21 h2
hi7 hi hz ha ha h5 h6	h7 h8 h9 h10	hii hiz hi3	h14 h15 b	16 h18	h19 h28	h21 h2
2 h23 h24 h18 -> h1 h2 h3 h4 h5 h6	hr he he had	h11 h12 h13	h14 h15 h	16 517	h39 h20	h21 h2
2 h23 h24						
h19 -> h1 h2 h3 h4 h5 h0 2 h23 h24	h2 hm h9 h10	hii hi2 hi3	h14 h15	116 h17	h18 h28	h21 h2
h20 -> h1 h2 h3 h4 h5 h6	h7 h8 h9 h10	h11 h12 h13	h14 h15 t	116 h17	h18 h19	h21 h2
2 h23 h24 h21 -> h1 h2 h3 h4 h5 h6	h7 h8 h9 h14	h11 h12 h14	h14 h15 1	110 017	h10 h19	h20 h2
2 h23 h24						
h22 h1 h2 h3 h4 h5 h6 1 h23 h24	hy ha ha his	hii hi2 hi3	h14 h15 l	110 117	h18 h19	hze hz
h23 -> h1 h2 h3 h4 h5 h6	h7 h8 h9 h10	h11 h12 h13	h14 h15 h	110 h17	h18 h19	h20 h2
1 h22 h24 h24 h1 h2 h3 h4 h5 bb	he he he had	har has has	h14 h15 t	110 017	han han	h20 h2
1 h22 h23			enter have	need the second	Market Has	MICENTER
*** Results: 1% dropped (*** test csv cleaning	542/552 reci	etved)				



Results

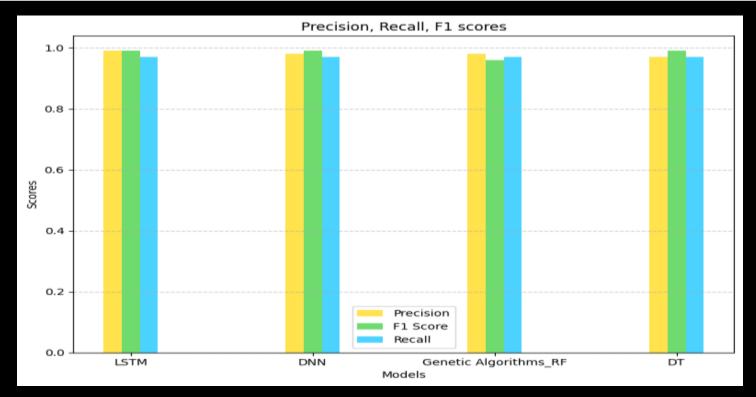
- Applied Model
 - LSTM
 - DNN
 - Genetic_RF
 - Decision Tree



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_sec	Assist in monitoring the speed of packet					
ond	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?