Vulnerability Assessment of Ad Hoc Networks under Different Simulation Scenarios

ENSC 833: NETWORK PROTOCOLS AND PERFORMANCE

Professor Dr. Ljiljana Trajkovic

TEAM # 02

Spring 2022

Project Webpage: https://malhotrarohil2.wixsite.com/ensc833team02

Name	SFU ID	SFU Email Address
Hossain Mahbub	301465556	hmm7@sfu.ca
Rohil Malhotra	301472836	rma118@sfu.ca
MD Nawshaad Khan	301448823	nawshaad_khan@sfu.ca

April 11, 2022

Outline

- Motivation & Goal
- Introduction
- Mobile Ad Hoc Network (MANET)
- Routing Algorithms
- Classification of Major Attacks
- Related Works
- Simulation Scenarios & Results
- Conclusion
- Future Work
- Reference List

Motivation and Goals

- In this modern time, all the devices are connected to the internet and now that these devices have gone wireless, they can establish connection to almost any other wireless device.

- Ad Hoc Networks are more vulnerable to security attacks than wired networks. So, security is one of the most essential requirements in ad hoc networks.

- By the end of this project, it is our goal to understand how the attack works and the damages it cause.

Introduction

- Ad Hoc networks are a collection of mobile nodes with links that are made or broken in an arbitrary way.
- Each node acts as a host and router to assist in transmitting data to other nodes in range.
- There are many types of Ad Hoc Networks depending on the nature of their application like:
  - Mobile Ad Hoc Network (MANET)
  - Vehicular Ad Hoc Networks (VANETs)
  - Wireless Mesh Networks
  - Smart Phone Ad Hoc Networks (SPANs)

❑ To maintain a reliable and secure network, the main security goals are:

- Confidentiality, Dynamic Topology, Authentication, Integrity, Availability

❑ **According to Cloudflare, in Q4 of 2021** [7]:

- Ransom DDoS attacks increased by 29% year-on-year and 175% quarter-on-quarter.
- The manufacturing industry received the most application-layer DDoS attacks, recording a 641% increase quarter-on-quarter in the number of attacks.
- In December 2021 alone, there were more network-layer DDoS attacks than all the attacks seen in Q1 and Q2 of 2021 separately.

Mobile Ad Hoc Network (MANET)

- A Mobile Ad Hoc Network (MANET) is a type of decentralized network.
- Data is flowed using the participating nodes in the network i.e., each node is used to forward data to the next node using routing algorithms.
- Dynamic topology
- Fast and quick implementation and hop-by-hop communications
- No single point of failure
- Limited Bandwidth due to :
  - High Bit Error Rate
  - High Packet Collision
  - High End to End Delay

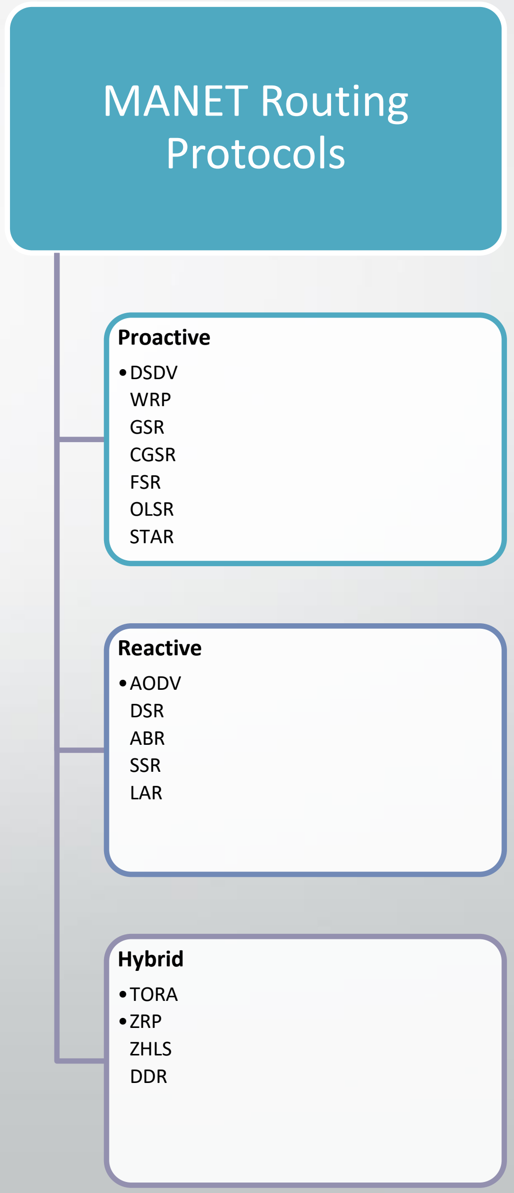
Routing Algorithms

Proactive Routing Protocols [2]:

- Routers in the network exchange information periodically to update their own routing table.
- Feasible for smaller networks comprising about 50 nodes hence it has reduced scalability.

Reactive Routing Protocols [2]:

- Routes are explored, and routing information is updated depending on necessity.
- The process is initiated when there is a change in the topology.
- Lesser traffic is generated in comparison to proactive routing protocol.



MANET Routing Protocols

Proactive

- DSDV
  WRP
  GSR
  CGSR
  FSR
  OLSR
  STAR

Reactive

- AODV
  DSR
  ABR
  SSR
  LAR

Hybrid

- TORA
- ZRP
  ZHLS
  DDR

DSDV: Destination-Sequenced Distance-Vector Routing
ZRP: Zone Routing Protocol

Routing Algorithms (Contd.)

- **Ad hoc On-Demand Distance Vector (AODV) [1][8]:**
  - 3 types of messages: Route request (RREQs), Route reply (RREPs) and Route errors (RRERs)
  - Routes: constructed based on demand, exploration based on query and reply
  - Any node disconnected: error message raised; other nodes notified
  - Nodes: No necessity to maintain total network information

- **Temporally Ordered Routing Algorithm (TORA) [2][8]:**
  - Three functions: creation, maintenance, and erasure of nodes
  - Source initiated, loop free, multipath routing protocol
  - Link Reversal: localize and distribute control messages based on topology
  - Node coordination to prevent count to infinity problem

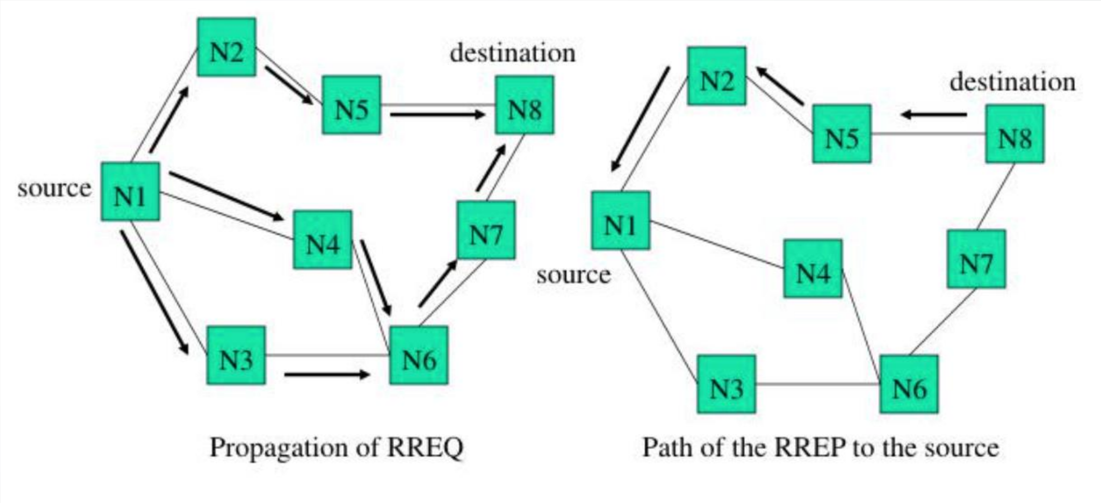


Figure 1: AODV Routing Protocol

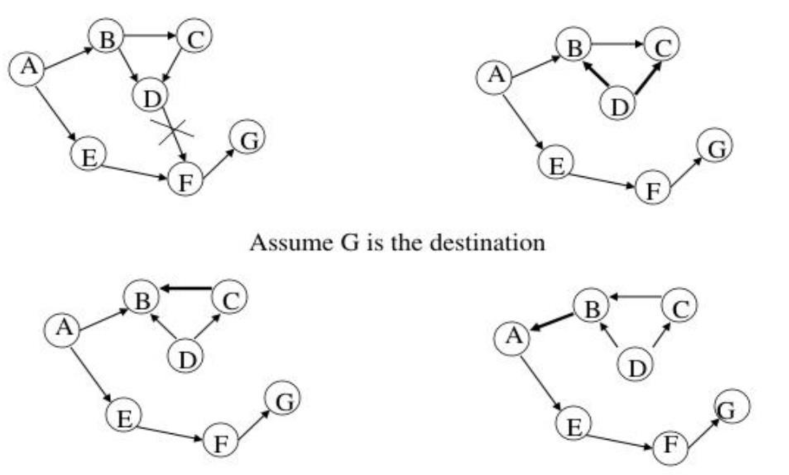
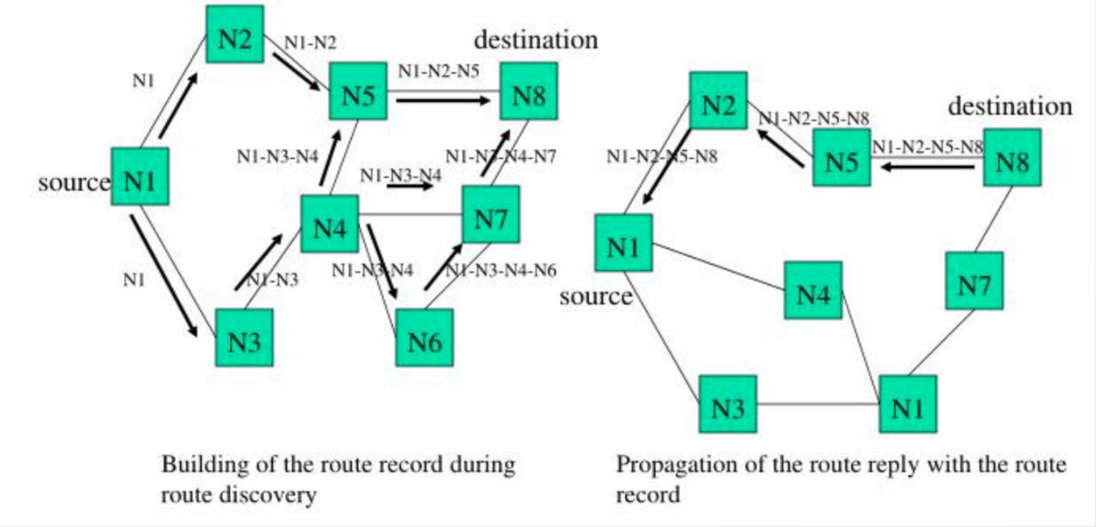


Figure 2: TORA Routing Protocol

Routing Algorithms (Contd.)

- **Dynamic Source Routing (DSR) [1][8]:**
  - Two mechanisms: Route Discovery and Route Maintenance
  - Multiple routes allowed, efficient route discovery and maintenance
  - No periodic message, reduced bandwidth and battery usage
  - Designed for multi-hop wireless ad hoc networks consisting mobile nodes
  - Each packet contains complete source to destination routing information
  - Less possibility of count to infinity problem



Building of the route record during route discovery

Propagation of the route reply with the route record

Figure 3: DSR Routing Protocol

Classification of Major Attacks

DDoS Attack [5]:

- It is a Distributed Denial-of-Service Attack.
- The attacker first compromises many hosts and then uses these hosts to launch the attack by exhausting the target network.
- The main intention of a DDoS attack is to make the end user unable to use the resources.

Sybil Attack [4]:

- The attacker can gain influence on the network by forging multiple false identities of trusted node and gain influence in the network.
- Due to an absence of authority in the network the sybil nodes can generate a chain of trust with the malicious nodes therefore compromising all identities in the network.

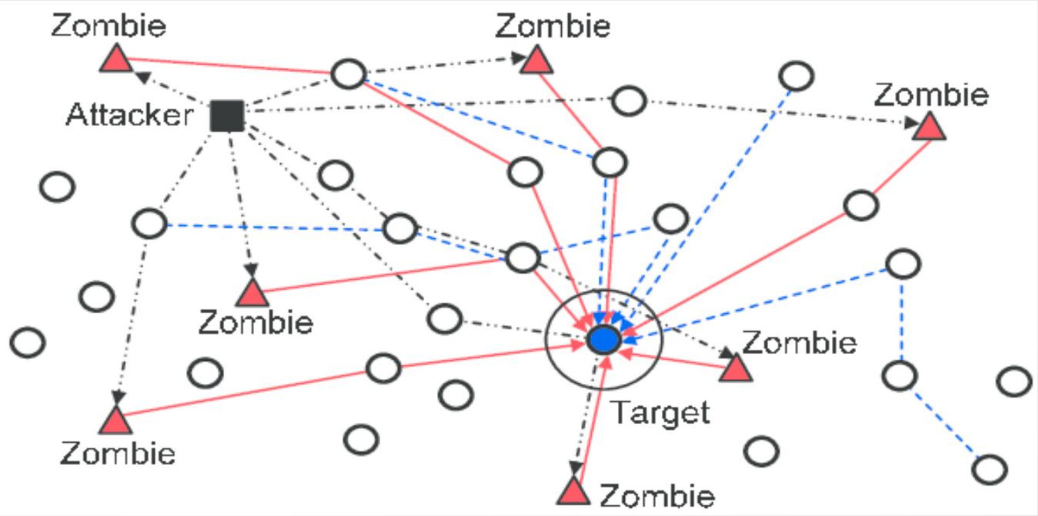


Figure 4: DDoS Attack

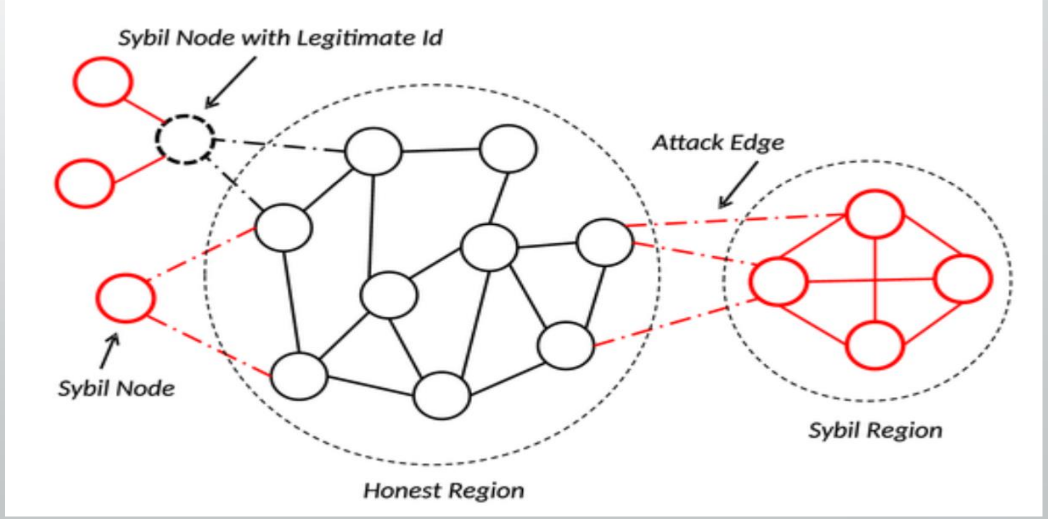


Figure 5: Sybil Attack

Classification of Major Attacks (Contd.)

Wormhole Attack [4]:

- A malicious node records packets at one location of the network and then tunnels them to another location.
- Due to the fault routing information the malicious node can then disrupt routes in network.

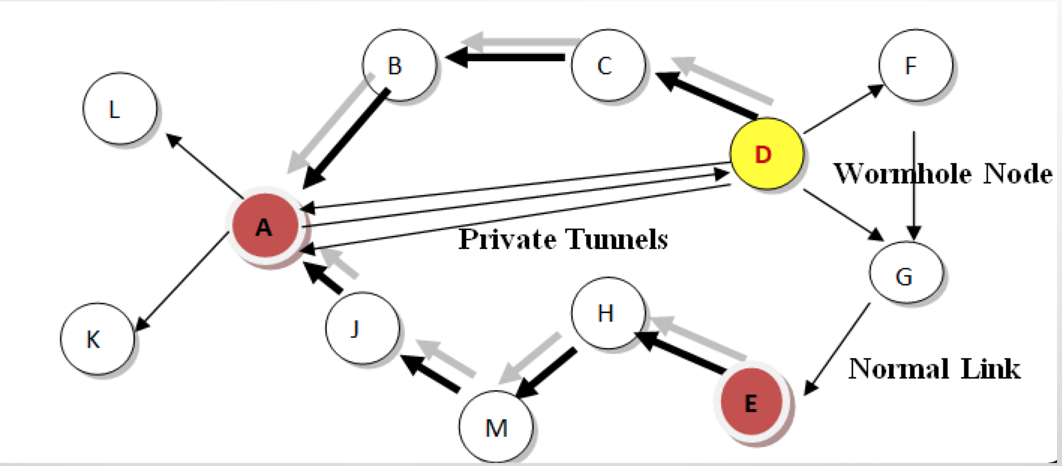


Figure 6: Wormhole Attack

Related Works

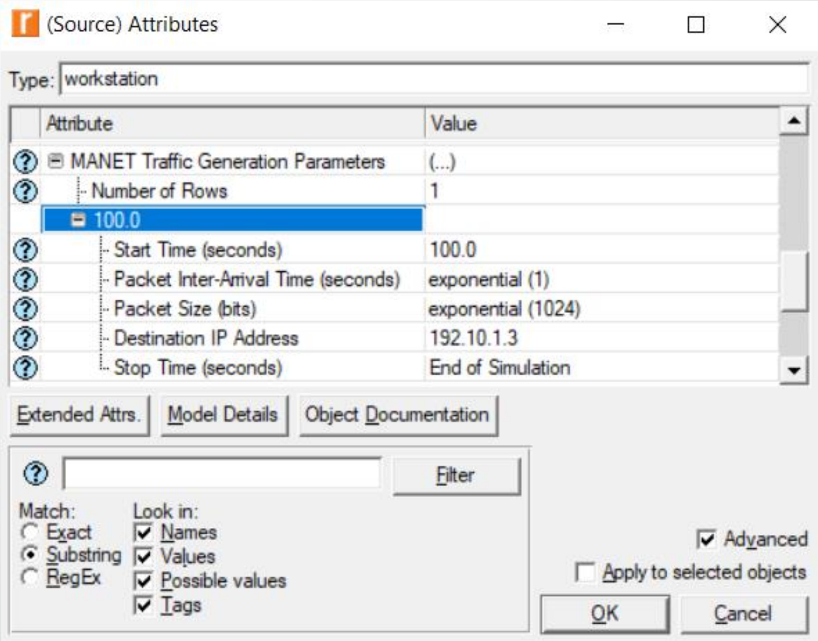
Related Works	Key Findings
S. Sinha et. al. (2013), “The sybil attack in Mobile Adhoc Network: Analysis and detection” [3]	• Discussed different types of security attacks in MANET with emphasis particularly on the Sybil attack. • Proposed a new approach to detect Sybil attack based on clustering and resource testing.
R. Das et al. (2016), “Performance analysis of various attacks under AODV in WSN & MANET using OPNET 14.5” [4]	• Introduced an algorithm to design a Mobile Ad-hoc network (MANET) or Wireless Sensor Network (WSN) and compares the effect of different network and physical layer attacks. • Simulate various attacks using the network simulator OPNET 14.5, and then analyze them in the basis of some quality-of-service parameters under AODV routing protocol.
Waleed Iftikhar et. al. (2020), “The Impact Of DDOS And Ping Of Death On Network Performance” [5]	• Several scenarios were discussed and demonstrated about DOS and DDoS attacks on Riverbed Modeler.
M. Chhabra et. al. (2013), “A Novel Solution to Handle DDOS Attack in MANET” [6]	• A novel solution is recommended to handle DDoS attacks in mobile ad hoc networks (MANETs).

Simulation Criteria and Parameters-I

<u>Scenario-01:</u>

- Implemented **AODV** routing protocol for a 20-node wireless **MANET** network.
- Implemented simulation for Ideal and Sybil Attack scenarios.
- Nodes are arranged in random order and no specific topology is used.
- Demonstrated this simulation scenario by using Riverbed Modeler 17.5 academic edition.
- Configured Traffic Generation Parameters at MANET Source node for generating traffic.
- **Packets sent and received are traced in this scenario.**
- Important Network Parameters for this scenario are:

Simulation Time	30 Minutes
Routing Algorithm	AODV
Number of Nodes	20
Source Data Rate	24 Mbps
Transmission Power	0.005 W
Packet Size	1024 bits
Traffic Type	MANET
Physical Characteristics	802.11g (Extended Rate PHY)



(Source) Attributes

Type: workstation

Attribute	Value
⊟ MANET Traffic Generation Parameters	(...)
Number of Rows	1
⊟ 100.0	
Start Time (seconds)	100.0
Packet Inter-Arrival Time (seconds)	exponential (1)
Packet Size (bits)	exponential (1024)
Destination IP Address	192.10.1.3
Stop Time (seconds)	End of Simulation

Match: ○ Exact ● Substring ○ RegEx

Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

☑ Advanced

□ Apply to selected objects

Figure 7: MANET Traffic Generation Parameters at Source

Scenario-1 (MANET-Ideal Case)

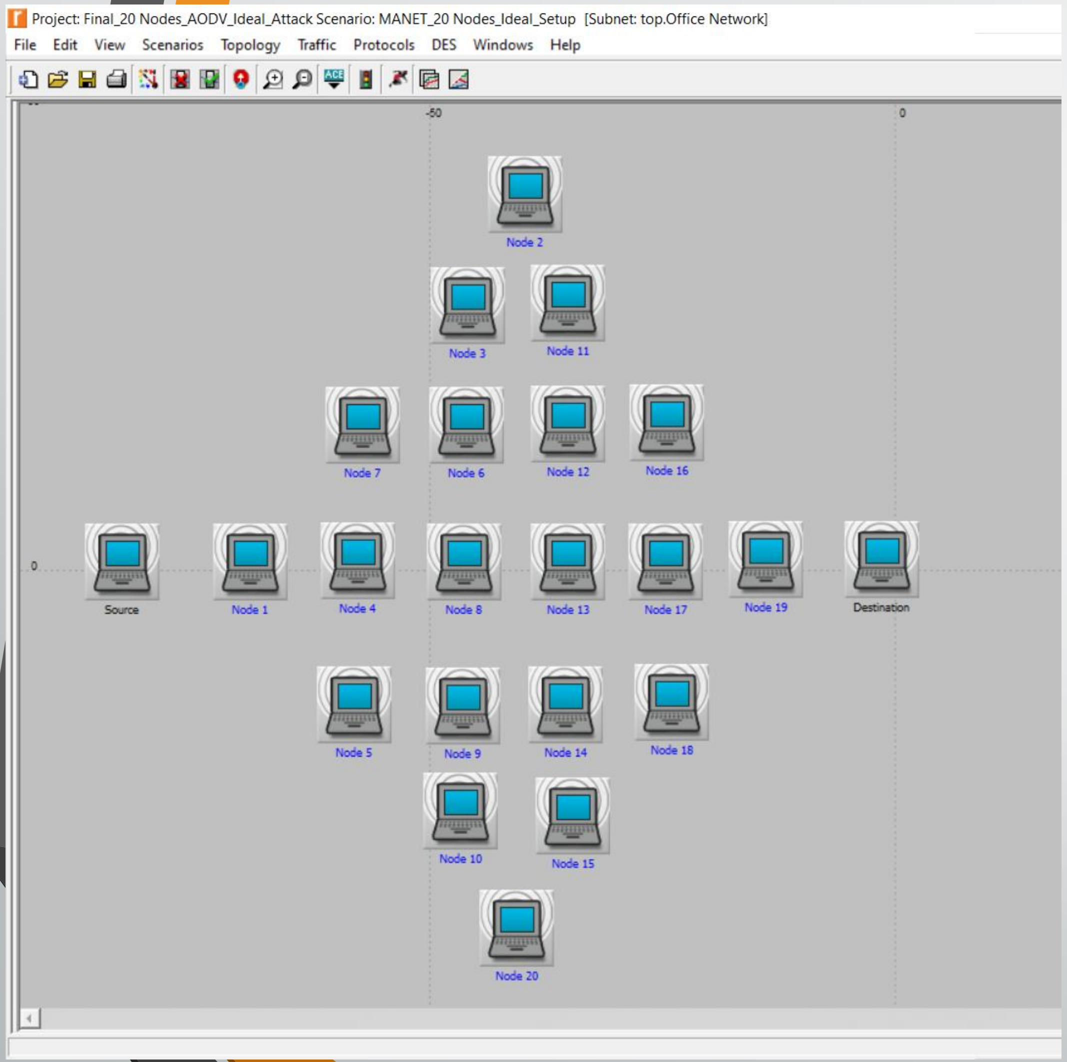
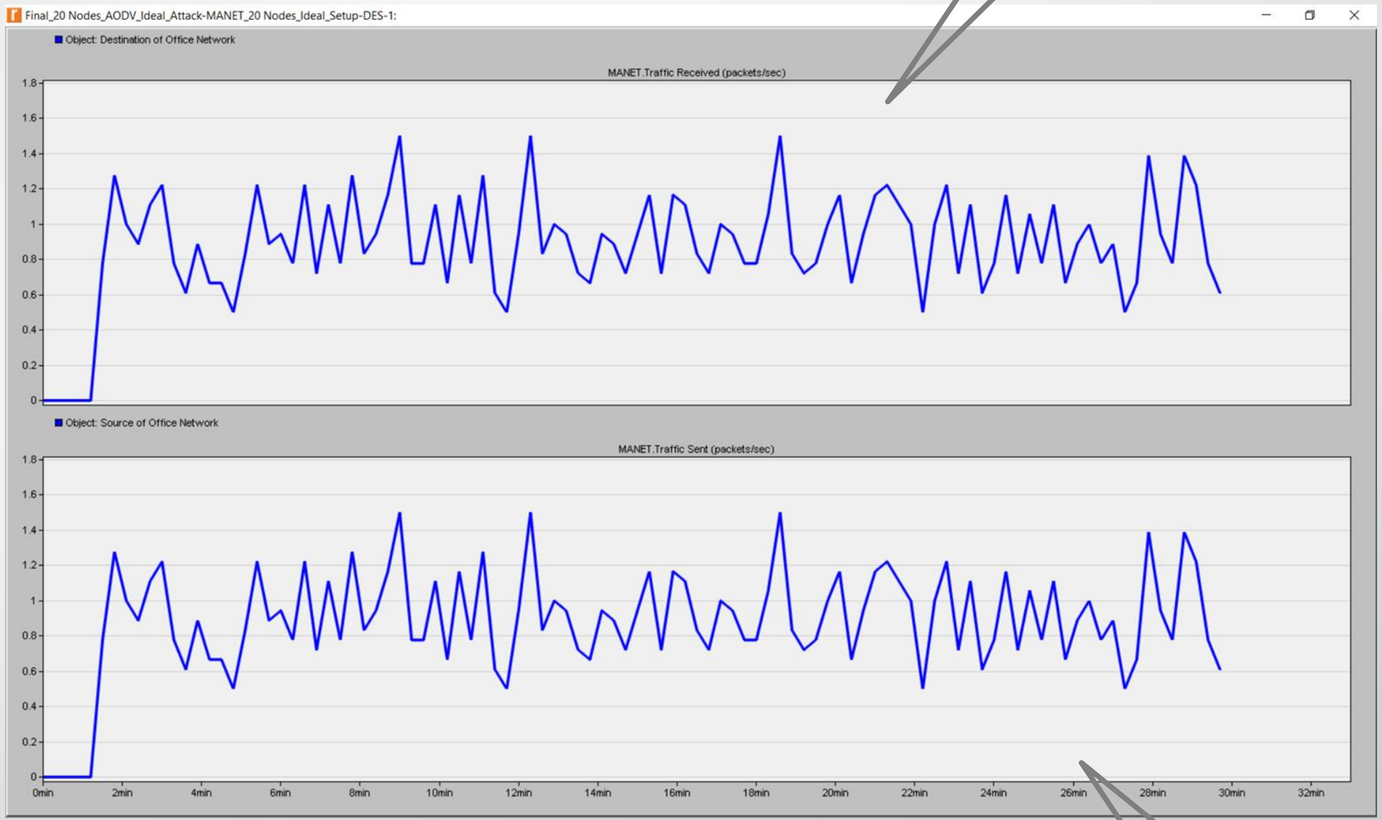


Figure 8: MANET Network with AODV Routing Protocol



Traffic Received at Destination

Traffic Sent from Source

Figure 9: Traffic Flow (Packets/sec) on MANET Network

X-axis: 1 unit = 2 minutes;
Y-axis: 1 unit = 0.2 packets/second

Scenario-1 (MANET-*Sybil Attack*)

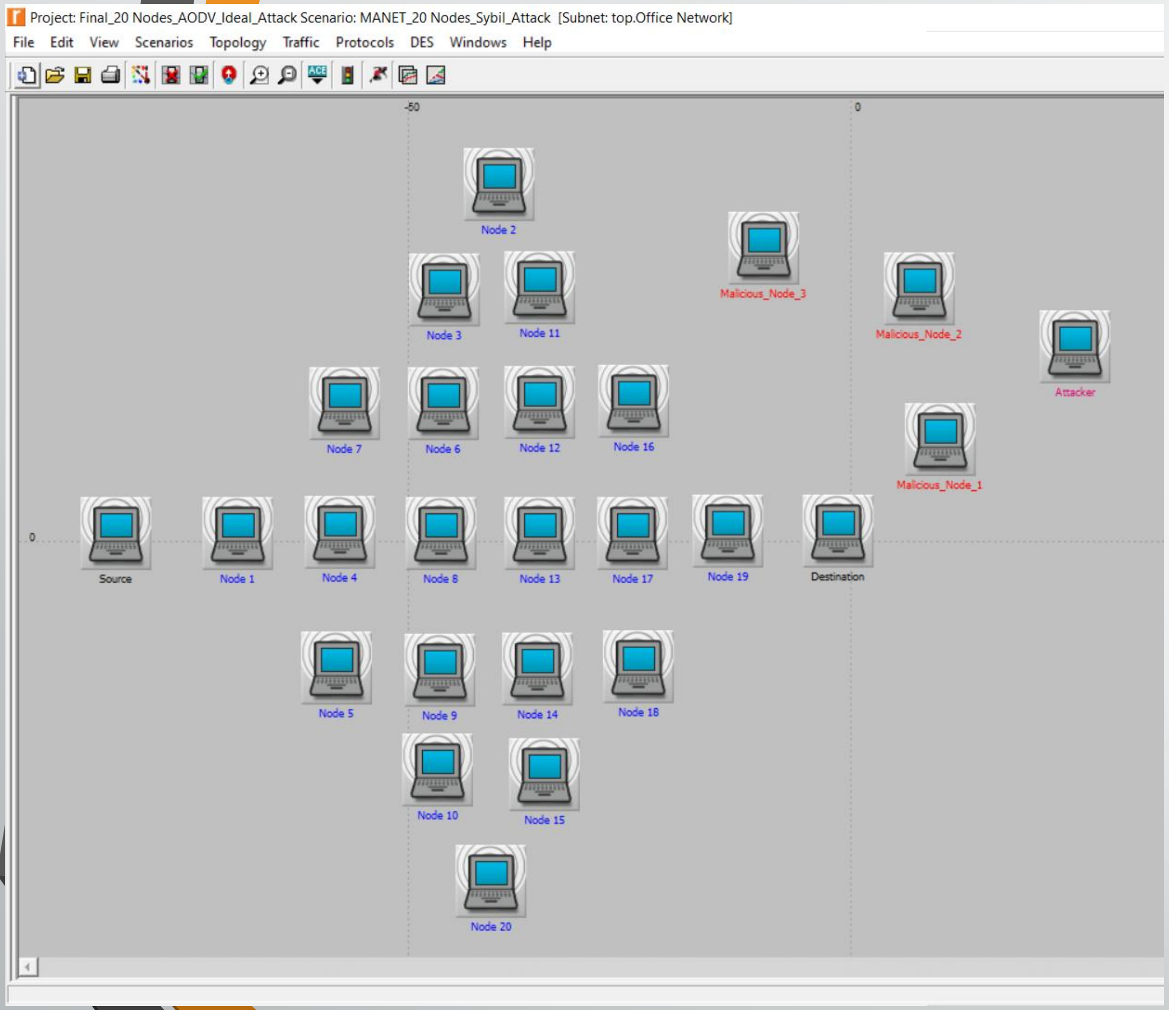
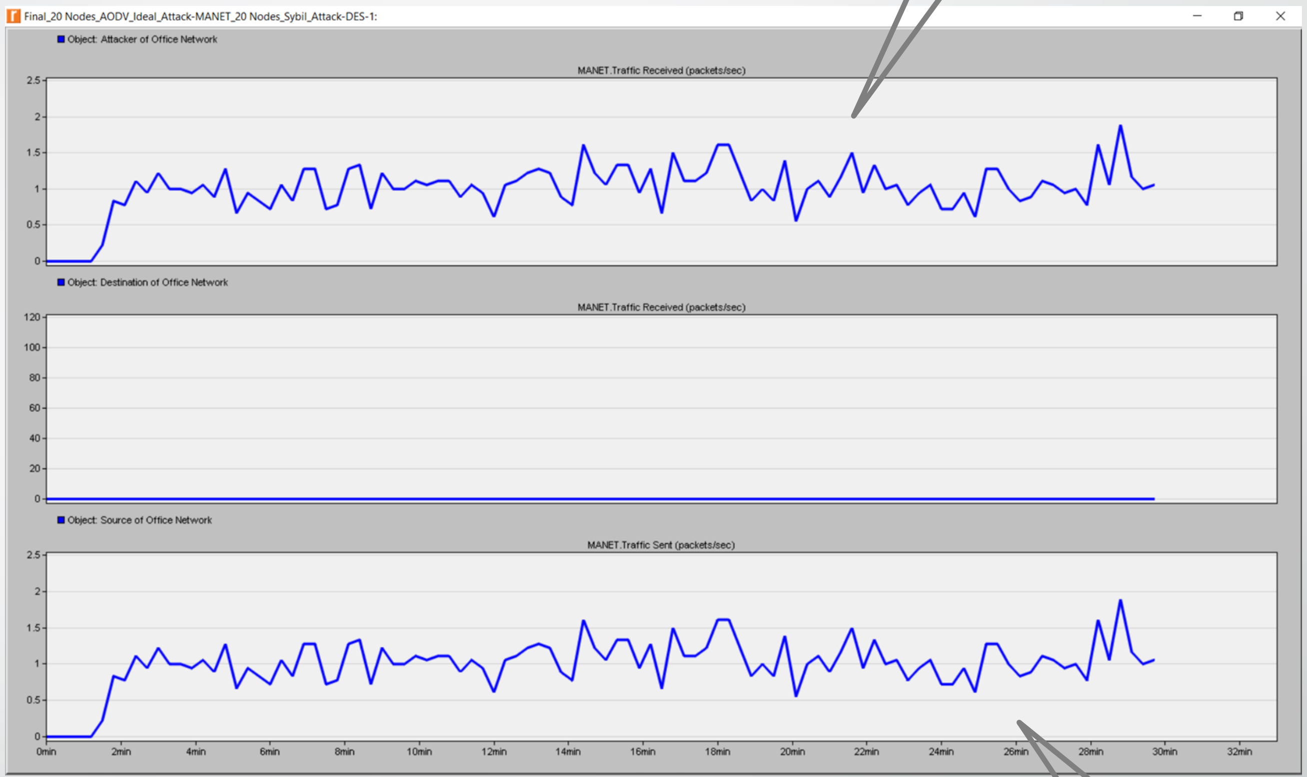


Figure 10: MANET Network with AODV Routing Protocol



Traffic Received at Attacker

Traffic Sent from Source

Figure 11: Traffic Flow (Packets/sec) on MANET Network

- Because of Sybil Attack, all traffic is completely re-routed to the ‘Attacker’ node through the Sybil nodes even though the destination was much closer to the source than the attacker.

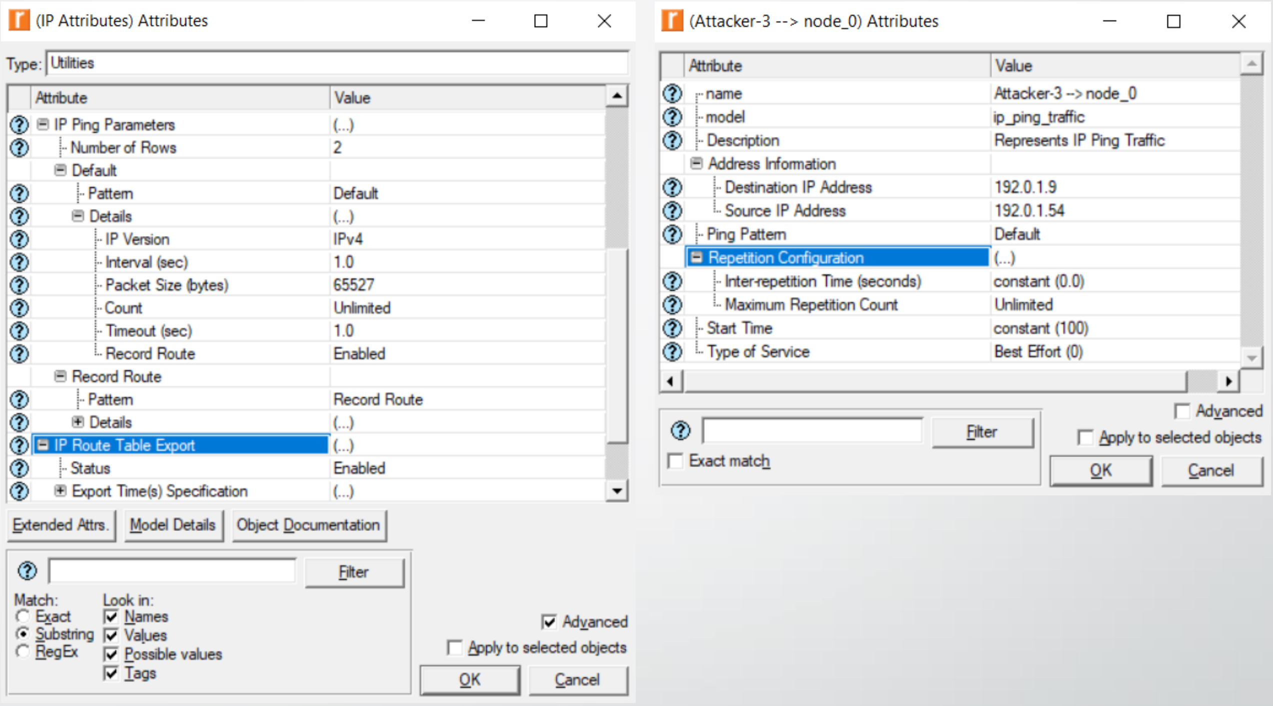
X-axis: 1 unit = 2 minutes;
Y-axis: 1 unit = 0.5 packets/second (bottom), 1 unit = 20 packets/second (middle), 1 unit = 0.5 packets/second (top)

Simulation Criteria and Parameters-II

Scenario-02 to Scenario-05:

- Implemented **AODV, DSR, TORA** routing protocols for 50-node wireless peer to peer network.
- Implemented simulation for **Ideal and DDoS Attack scenarios** for each routing protocol.
- Nodes are arranged in random order and no specific topology is used.
- Statistical data are analyzed based on Load, Media Access Delay, Number of Packets Dropped, and FTP Download Response Time, etc.
- Simulation results for the ideal and the DDoS attack scenarios are compared into a single graph for each of the statistics measured.
- Important Network Parameters for this scenario are:

Simulation Time	1 hour
Routing Algorithm	AODV, DSR, TORA
Number of Nodes	50
Number of Attacker	4
Source Data Rate	1 Mbps
Transmission Power	0.005 W
Traffic Type	FTP
FTP Capacity	High Load
Physical Characteristics	802.11g (Extended Rate PHY)



(IP Attributes) Attributes

Type: Utilities

Attribute	Value
⊟ IP Ping Parameters	(...)
Number of Rows	2
⊟ Default	
Pattern	Default
⊟ Details	(...)
IP Version	IPv4
Interval (sec)	1.0
Packet Size (bytes)	65527
Count	Unlimited
Timeout (sec)	1.0
Record Route	Enabled
⊟ Record Route	
Pattern	Record Route
⊞ Details	(...)
⊟ IP Route Table Export	(...)
Status	Enabled
⊞ Export Time(s) Specification	(...)

Match: ○ Exact ● Substring ○ RegEx

Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

☑ Advanced

□ Apply to selected objects

(Attacker-3 --> node_0) Attributes

Attribute	Value
name	Attacker-3 --> node_0
model	ip_ping_traffic
Description	Represents IP Ping Traffic
⊟ Address Information	
Destination IP Address	192.0.1.9
Source IP Address	192.0.1.54
Ping Pattern	Default
⊟ Repetition Configuration	(...)
Inter-repetition Time (seconds)	constant (0.0)
Maximum Repetition Count	Unlimited
Start Time	constant (100)
Type of Service	Best Effort (0)

□ Advanced

□ Apply to selected objects

□ Exact match

Figure 12: IP Ping Traffic Generation Configurations

- Demonstrated this simulation scenario by using Riverbed Modeler 17.5 academic edition.
- Used ‘IP Ping Traffic Flow’ mechanism, and ‘IP Attribute configuration’ from Riverbed Modeler for implementing DDoS attack.

Scenario-2: 50-Node AODV P2P Network

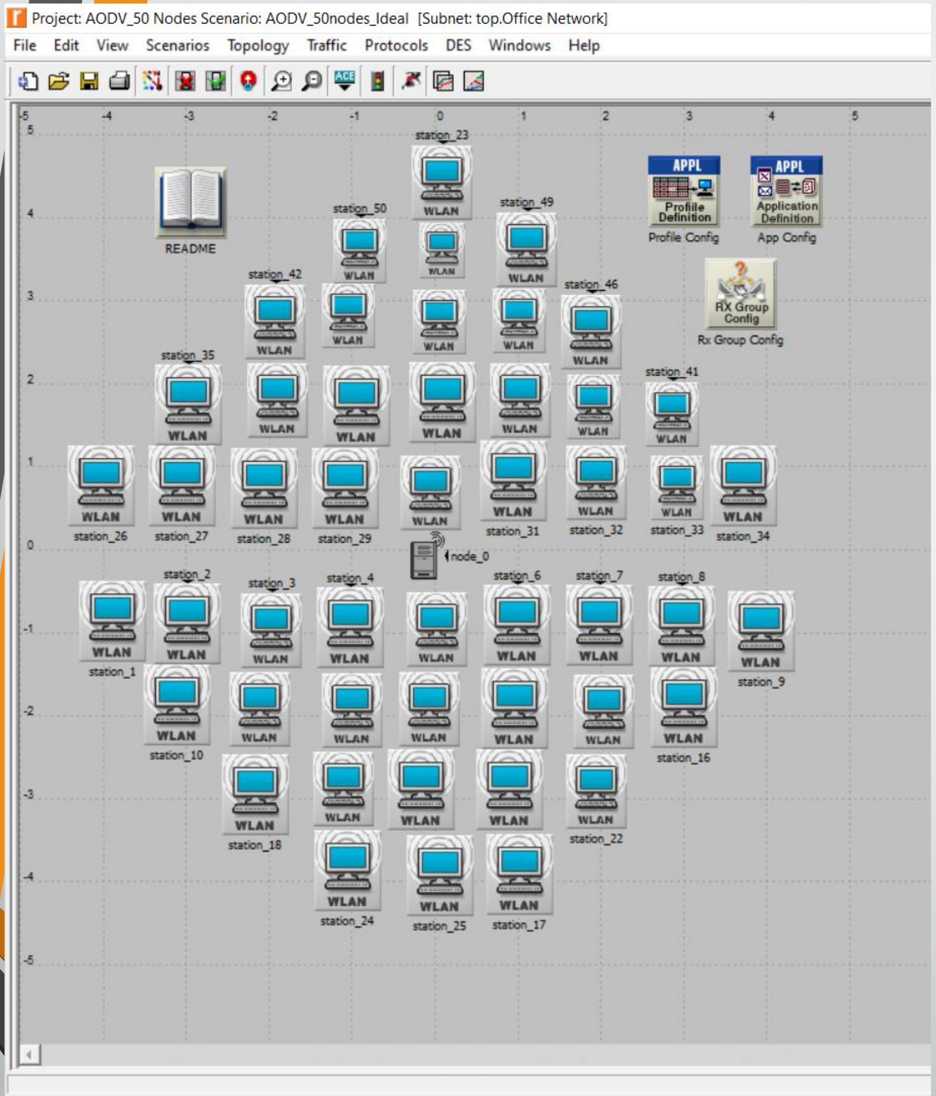


Figure 13: 50 WLAN Nodes AODV Network

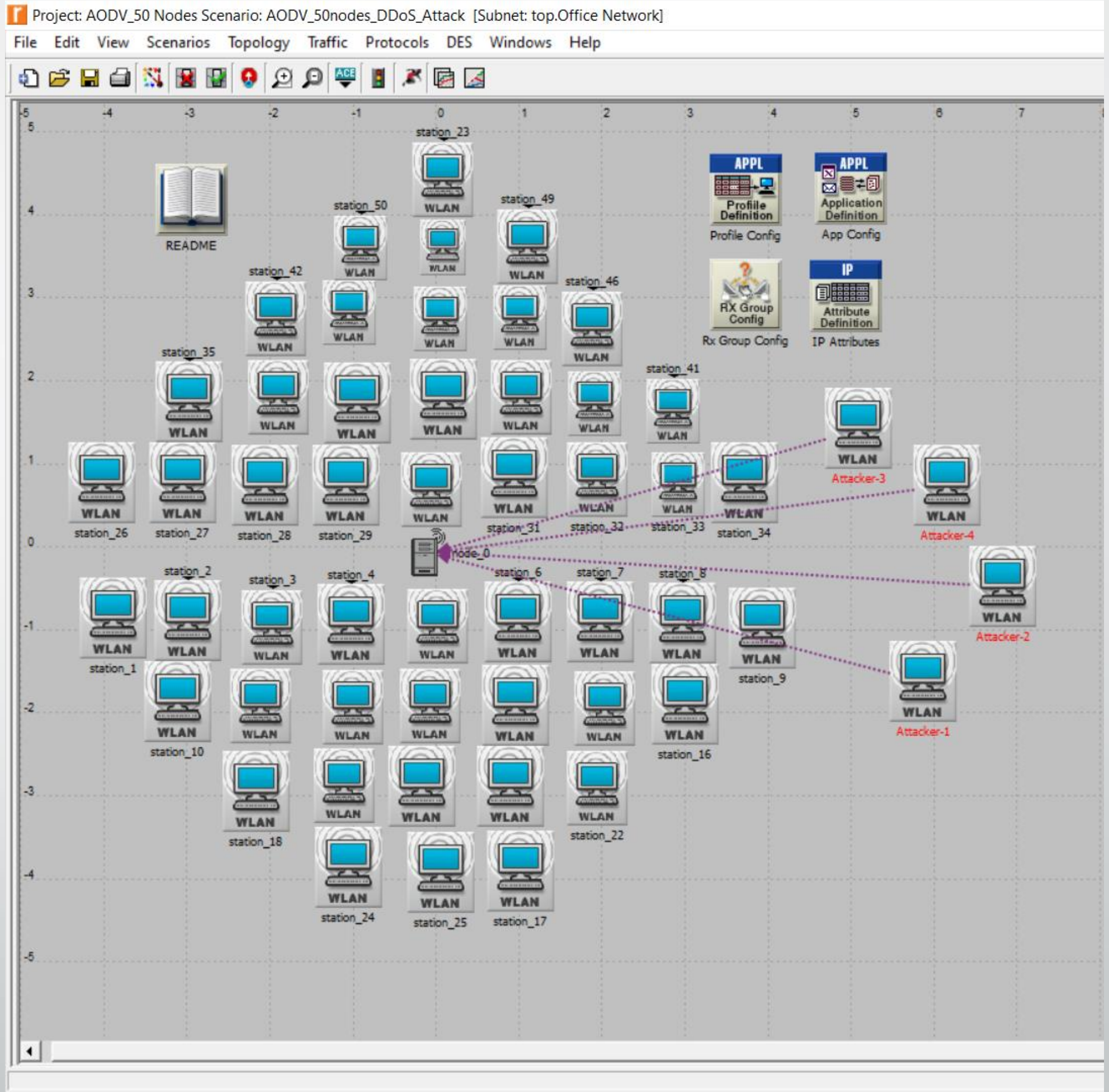


Figure 14: 50 WLAN Nodes AODV Network under DDoS Attack

Scenario-2: 50-Node AODV P2P Network (Contd.)

🔴 Ideal Scenario 🔵 DDoS Attack

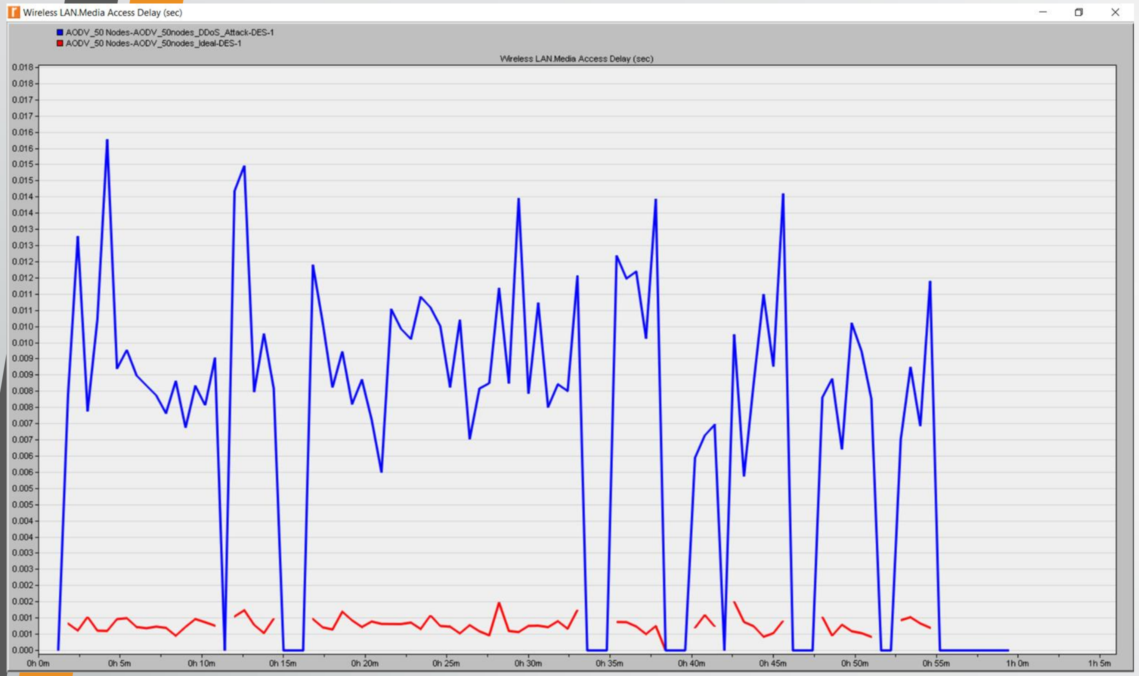


Figure 15: Wireless LAN - Media Access Delay (seconds)

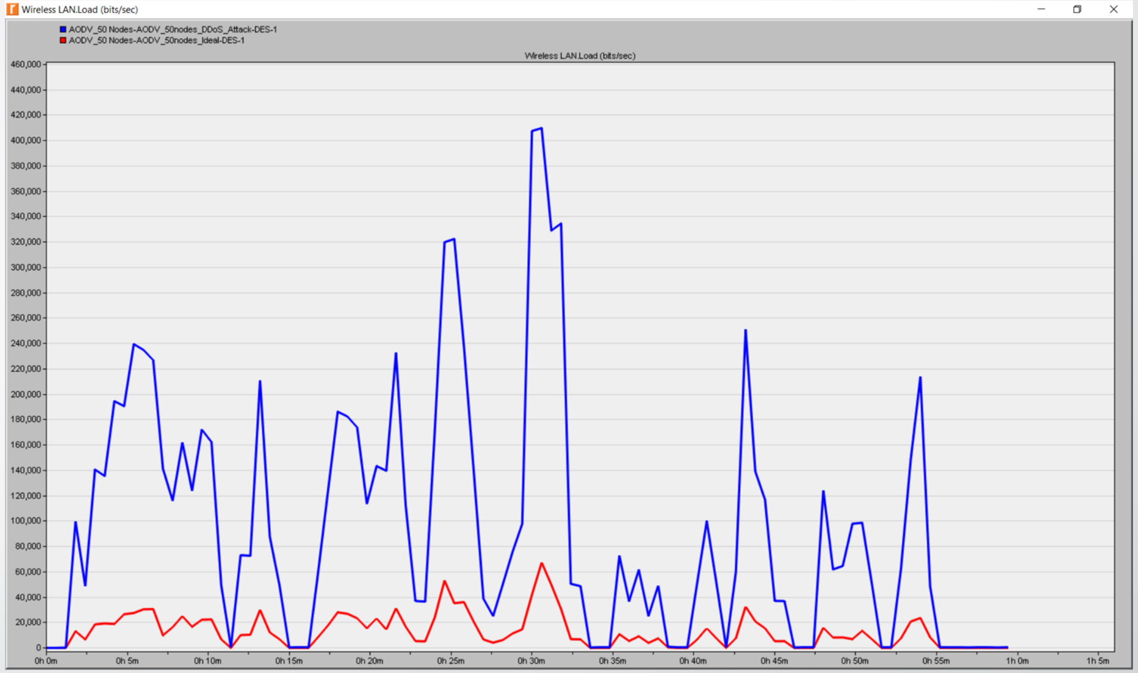


Figure 16: Wireless LAN – Load (bits/sec)

Media Access Delay (seconds): Increased by about 9 times compared to ideal scenario (while performing DDoS attack)

Load (bits/sec): Increased about 10 times more than the ideal network scenario (while performing DDoS attack)

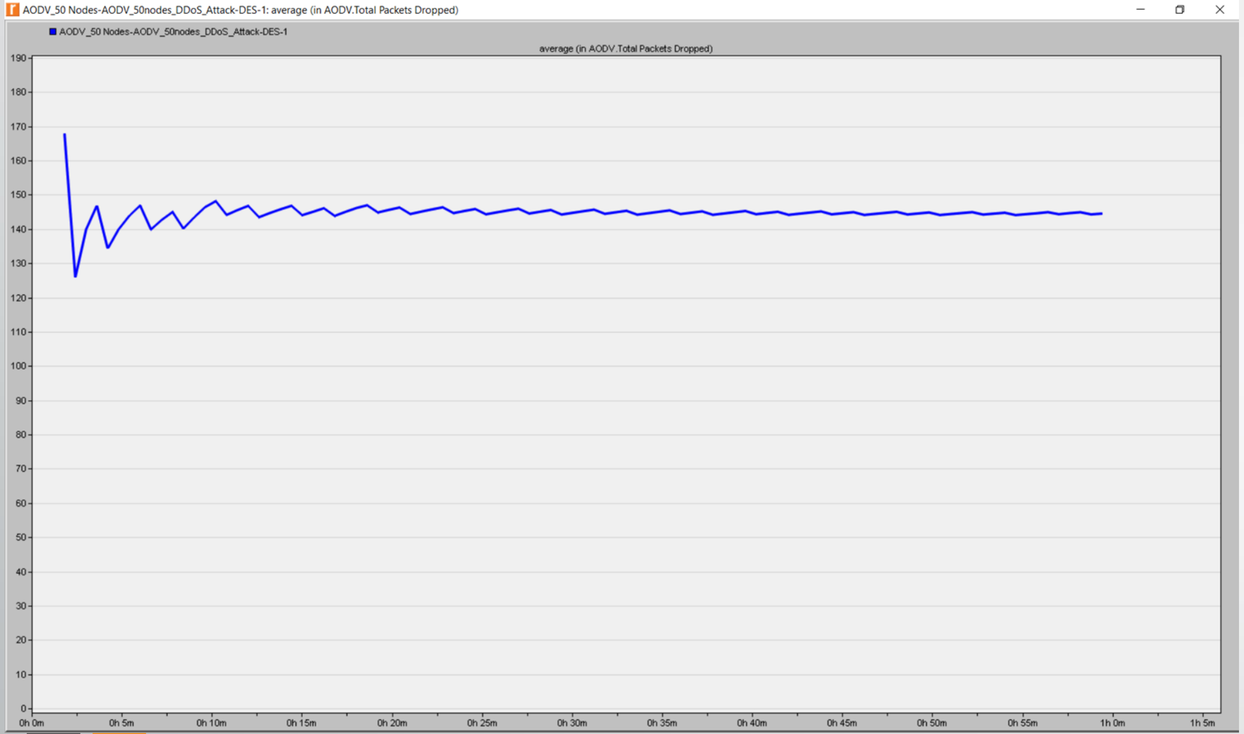
X-axis: 1 unit = 5 minutes
Y-axis: 2 units = 0.001 second

Media Access Delay represents the global statistics for the total of queuing and contention delays of the data, management, delayed Block-ACK and Block-ACK Request frames transmitted by all WLAN MACs in the network. **Load** represents the total load (in bits/sec) submitted to wireless LAN layers by all higher layers in all WLAN nodes.

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 20,000 bits

Scenario-2: 50-Node AODV P2P Network (Contd.)

● Ideal Scenario ● DDoS Attack



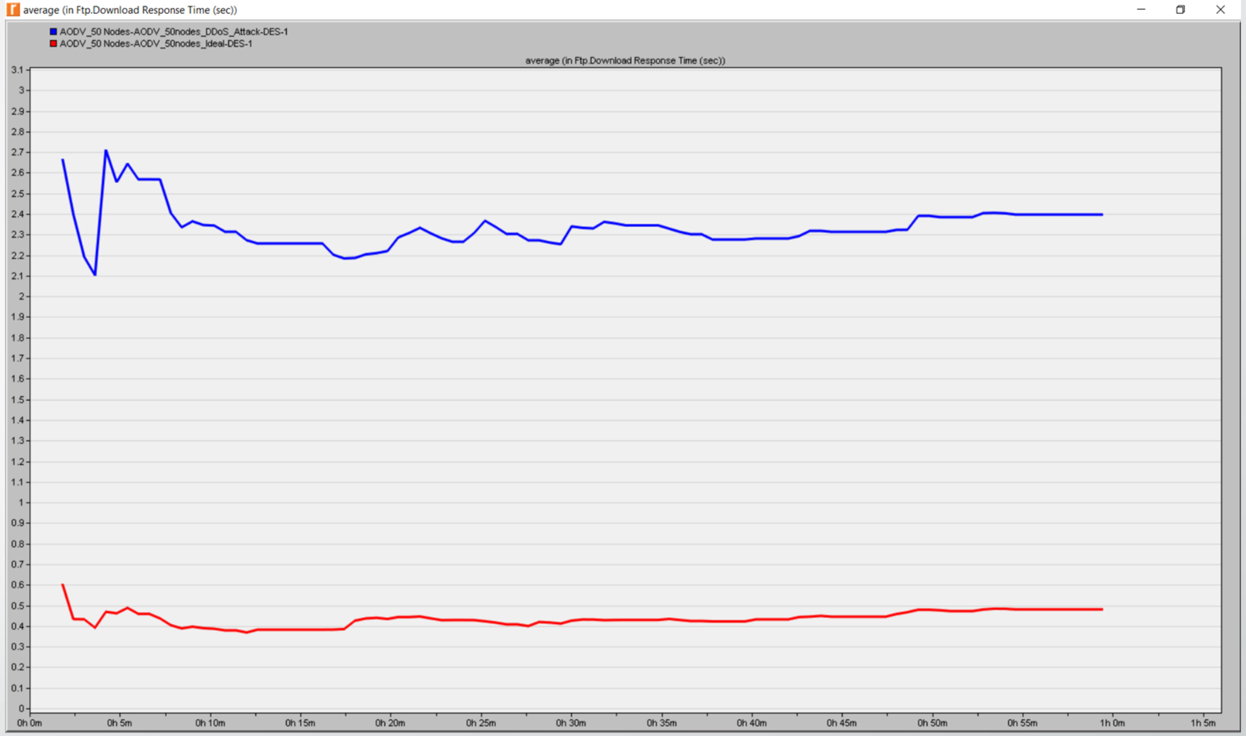


Figure 17: Total Packets Dropped in AODV

Figure 18: Avg. FTP Download Response Time (Seconds)

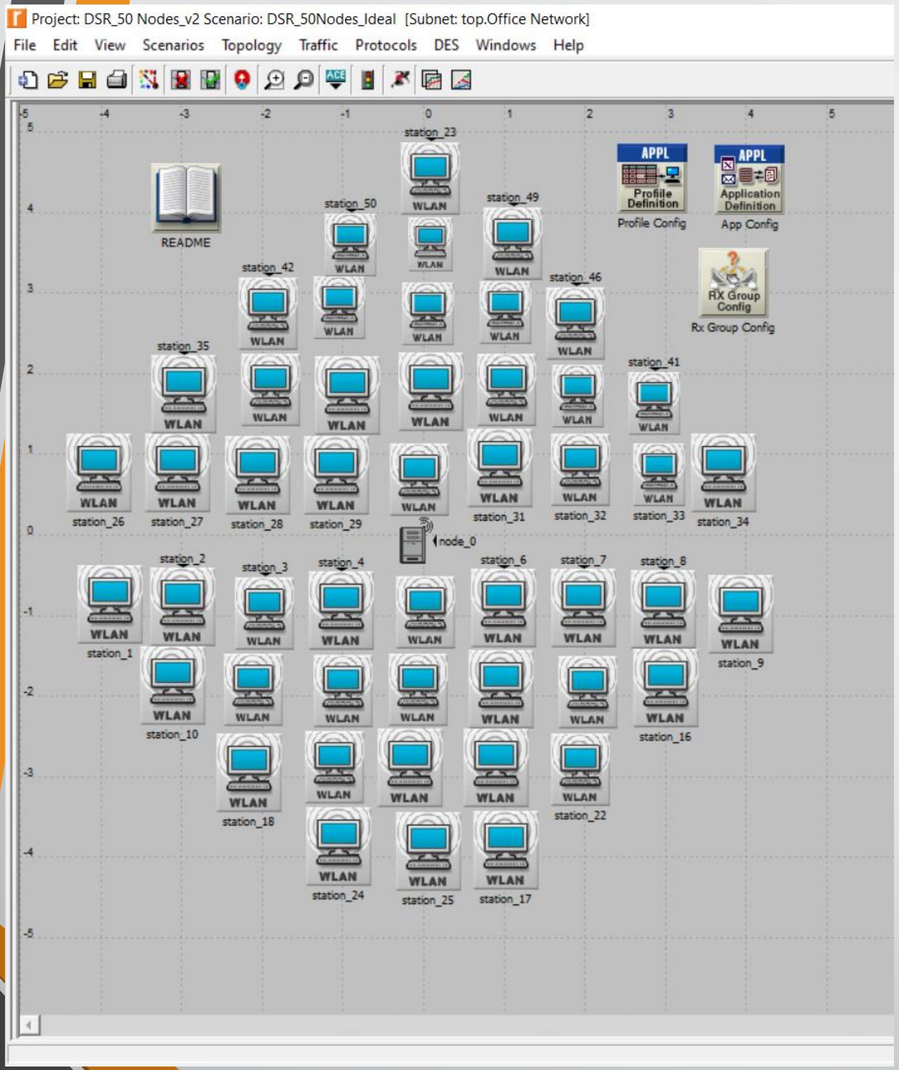
Observed packet drops after DDoS Attack, but No packet drops for ideal scenario

FTP Download Response Time: Increased by more than 9 times compared to the ideal network (while performing DDoS attack)

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 10 packets

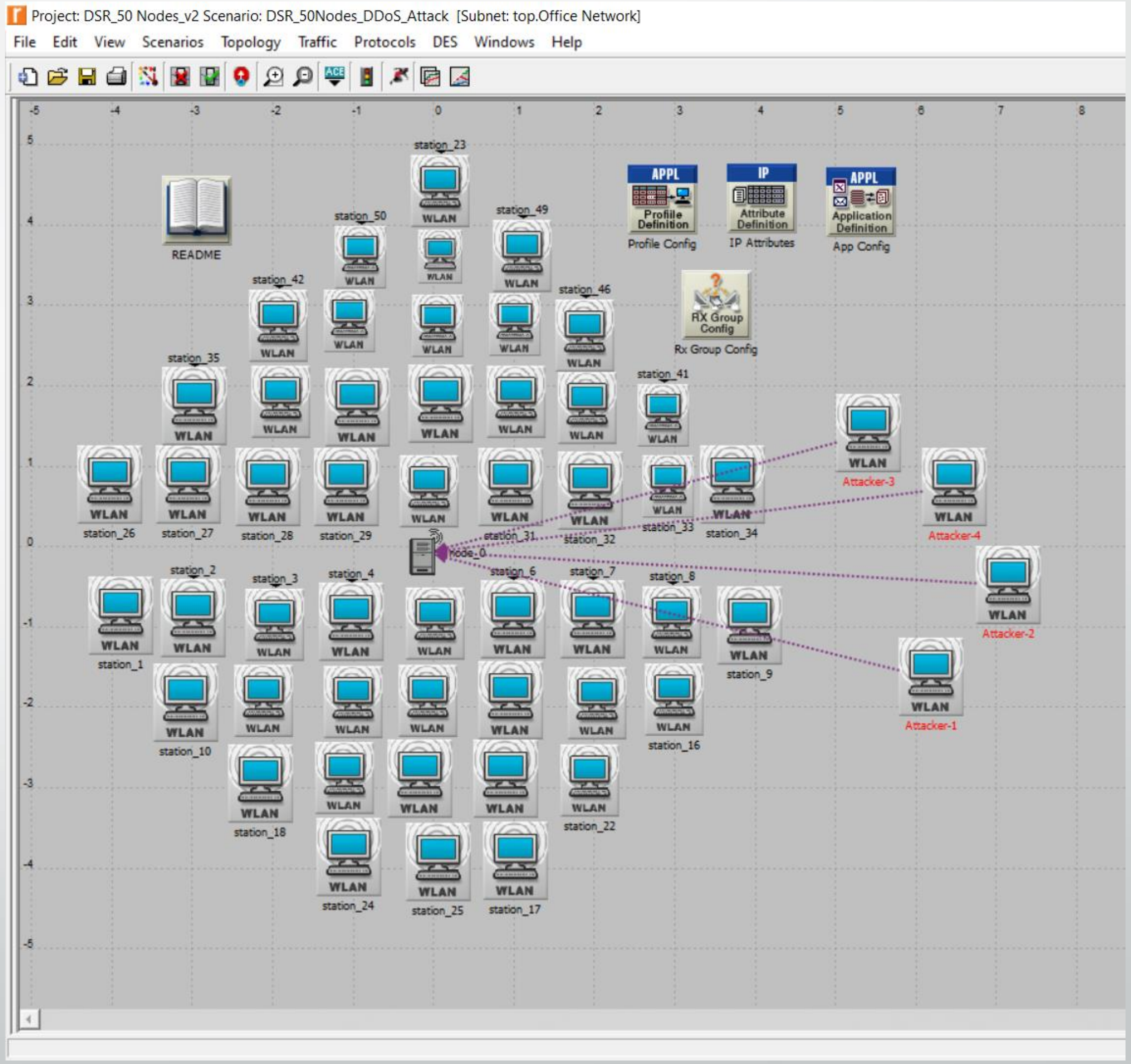
X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 0.1 second

Scenario-3: 50-Node DSR P2P Network



Project: DSR_50 Nodes_v2 Scenario: DSR_50Nodes_Ideal [Subnet: top.Office Network]

Figure 19: 50 WLAN Nodes DSR Network

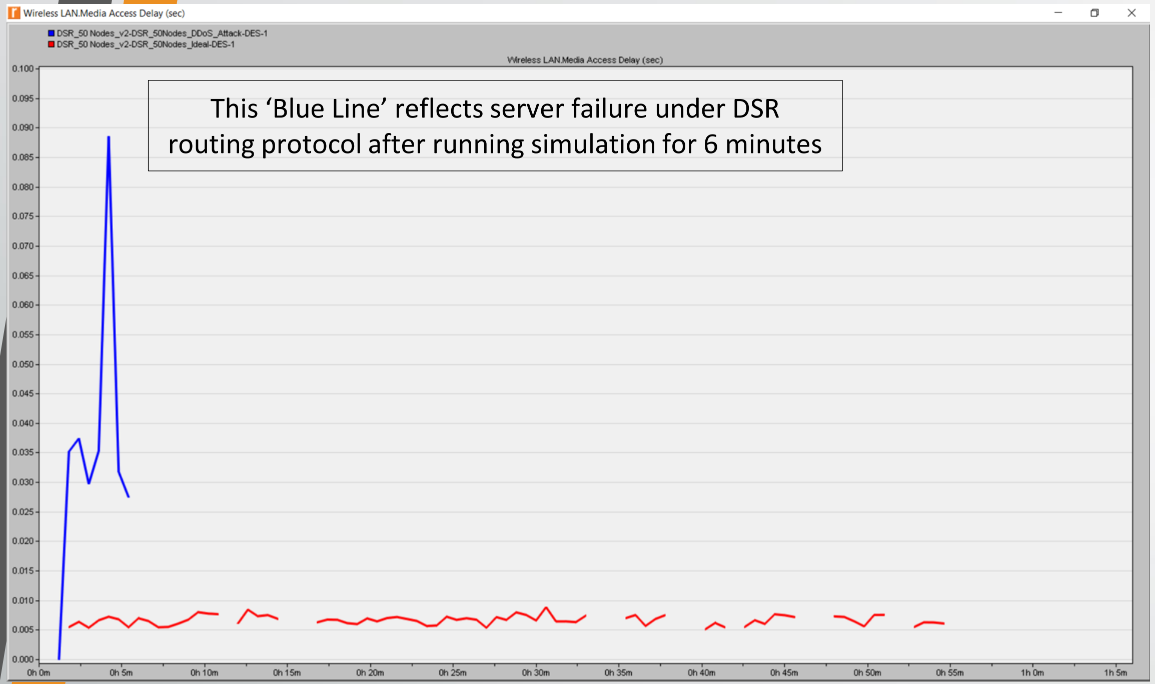


Project: DSR_50 Nodes_v2 Scenario: DSR_50Nodes_DDoS_Attack [Subnet: top.Office Network]

Figure 20: 50 WLAN Nodes DSR Network under DDoS Attack

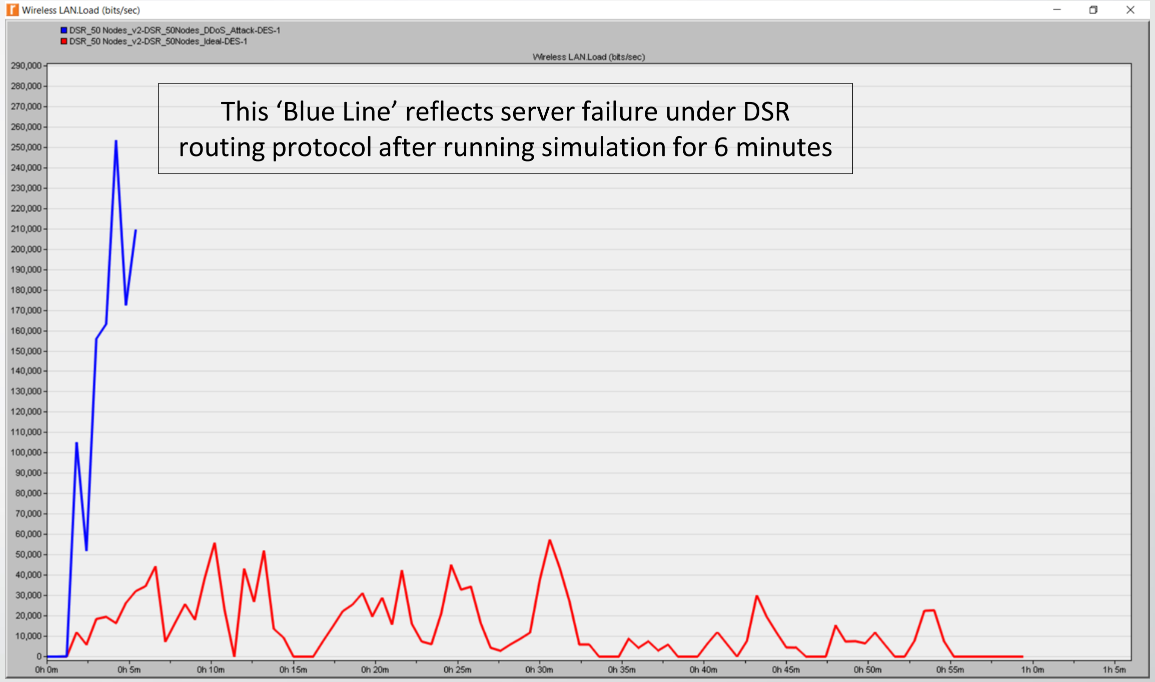
Scenario-3: 50-Node DSR P2P Network (Contd.)

● Ideal Scenario ● DDoS Attack



This 'Blue Line' reflects server failure under DSR routing protocol after running simulation for 6 minutes

Figure 21: Wireless LAN - Media Access Delay (seconds)



This 'Blue Line' reflects server failure under DSR routing protocol after running simulation for 6 minutes

Figure 22: Wireless LAN - Load (bits/sec)

Media Access Delay (seconds): Increased by about 12 times compared to ideal scenario (while performing DDoS attack)

Load (bits/sec): Increased about 10 times more than the ideal network scenario (while performing DDoS attack)

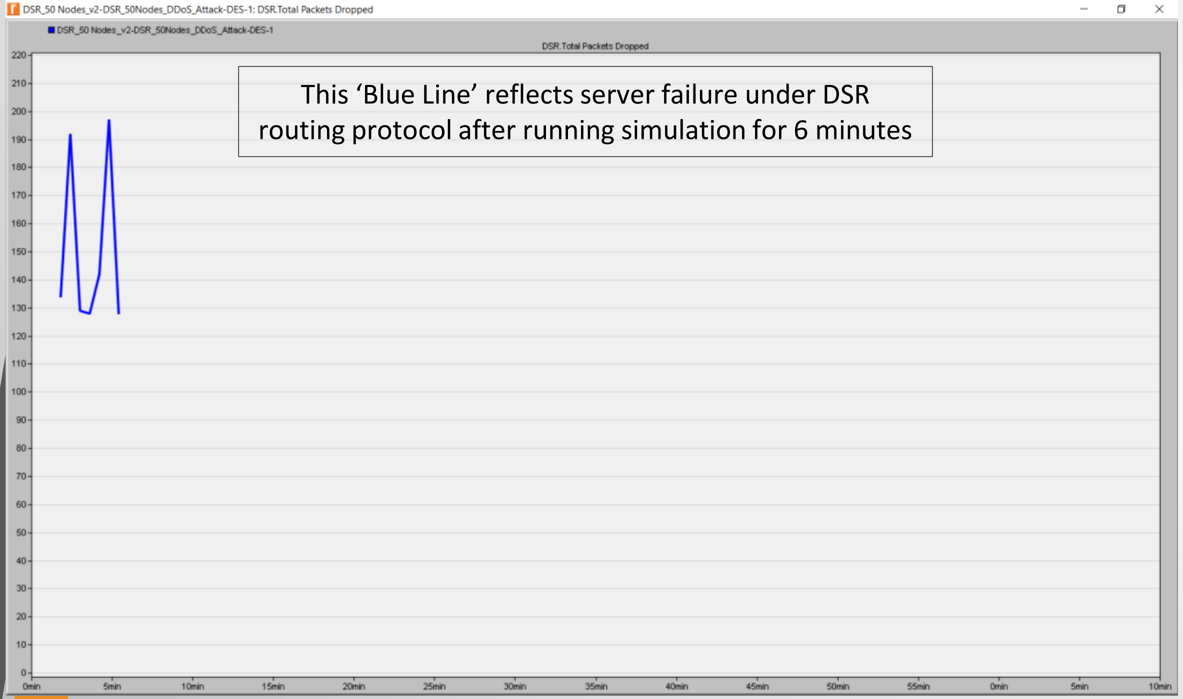
Server with the DSR routing fails after around 6 minutes due to high load from the attacking nodes.

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 0.005 seconds

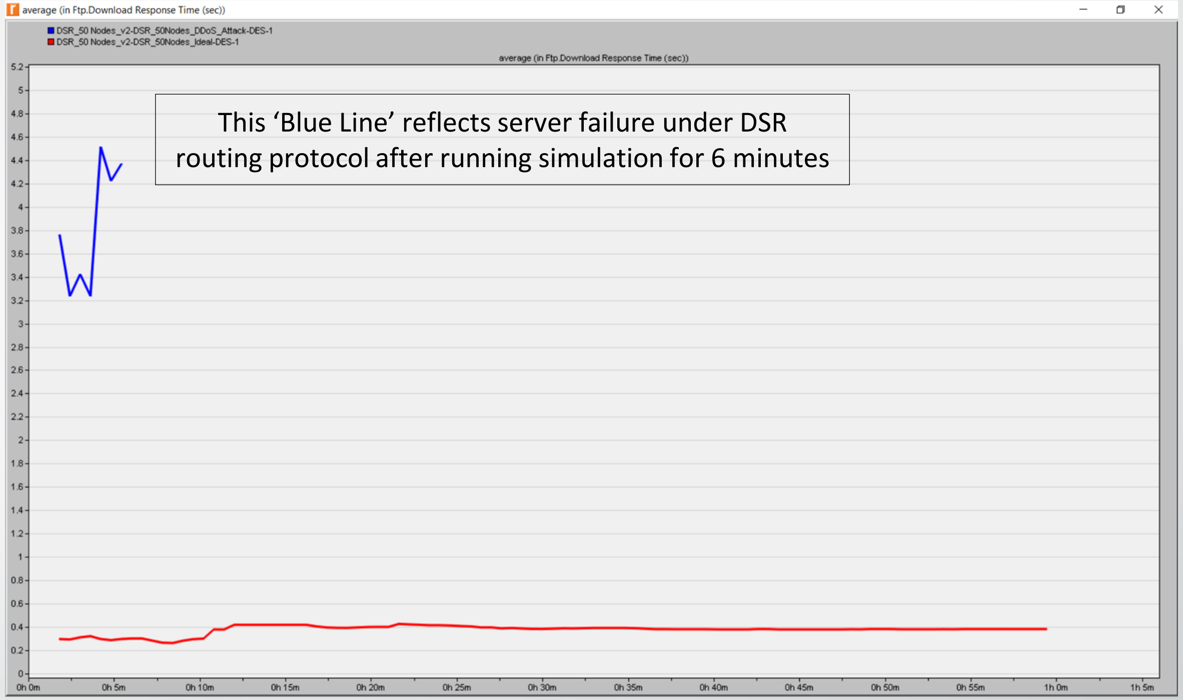
X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 10,000 bits

Scenario-3: 50-Node DSR P2P Network (Contd.)

🔴 Ideal Scenario 🔵 DDoS Attack



This 'Blue Line' reflects server failure under DSR routing protocol after running simulation for 6 minutes



This 'Blue Line' reflects server failure under DSR routing protocol after running simulation for 6 minutes

Figure 23: Total Packets Dropped in DSR

Figure 24: Avg. FTP Download Response Time (Seconds)

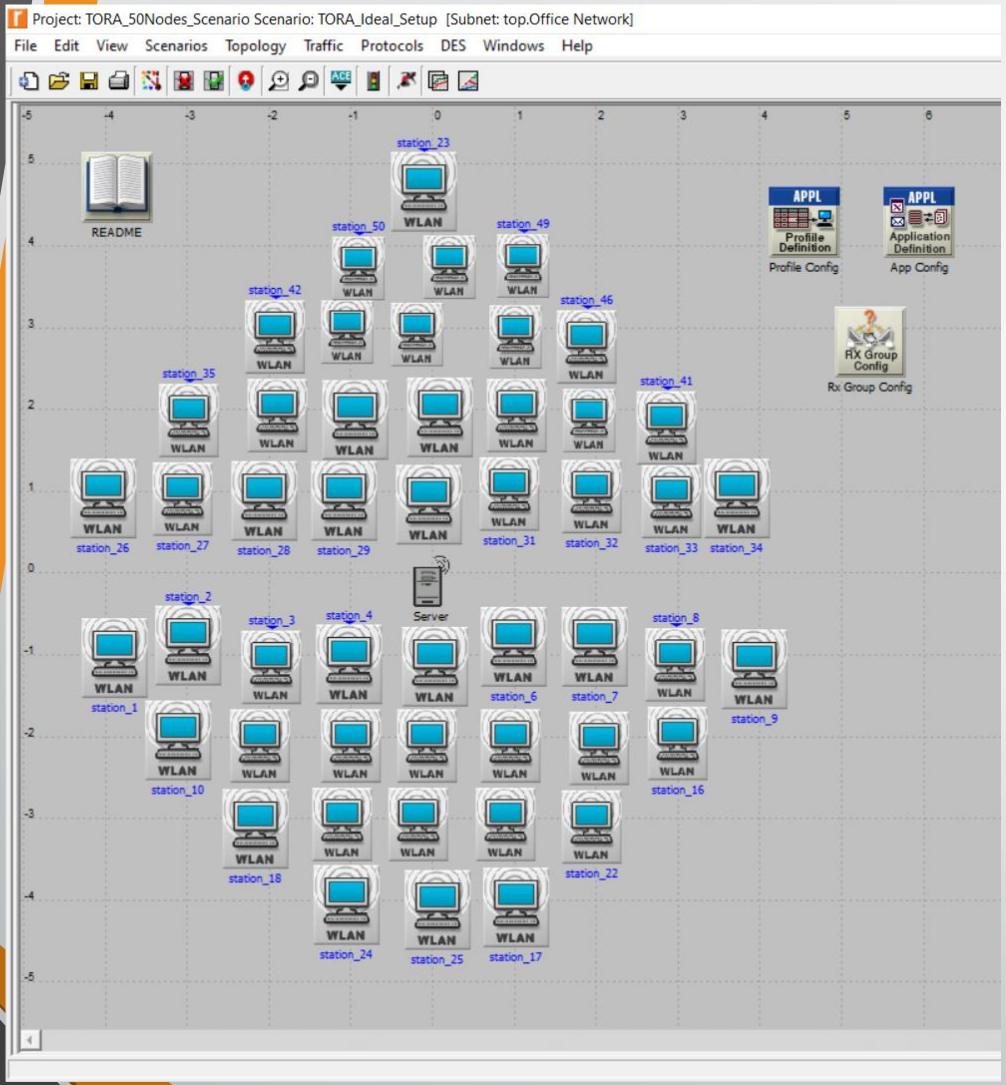
Observed packet drops during DDoS Attack, but No packet drops for ideal scenario.

FTP Download Response Time: Increased significantly (while performing DDoS Attack)

X-axis: 1 unit = 20 seconds
Y-axis: 1 unit = 10 packets

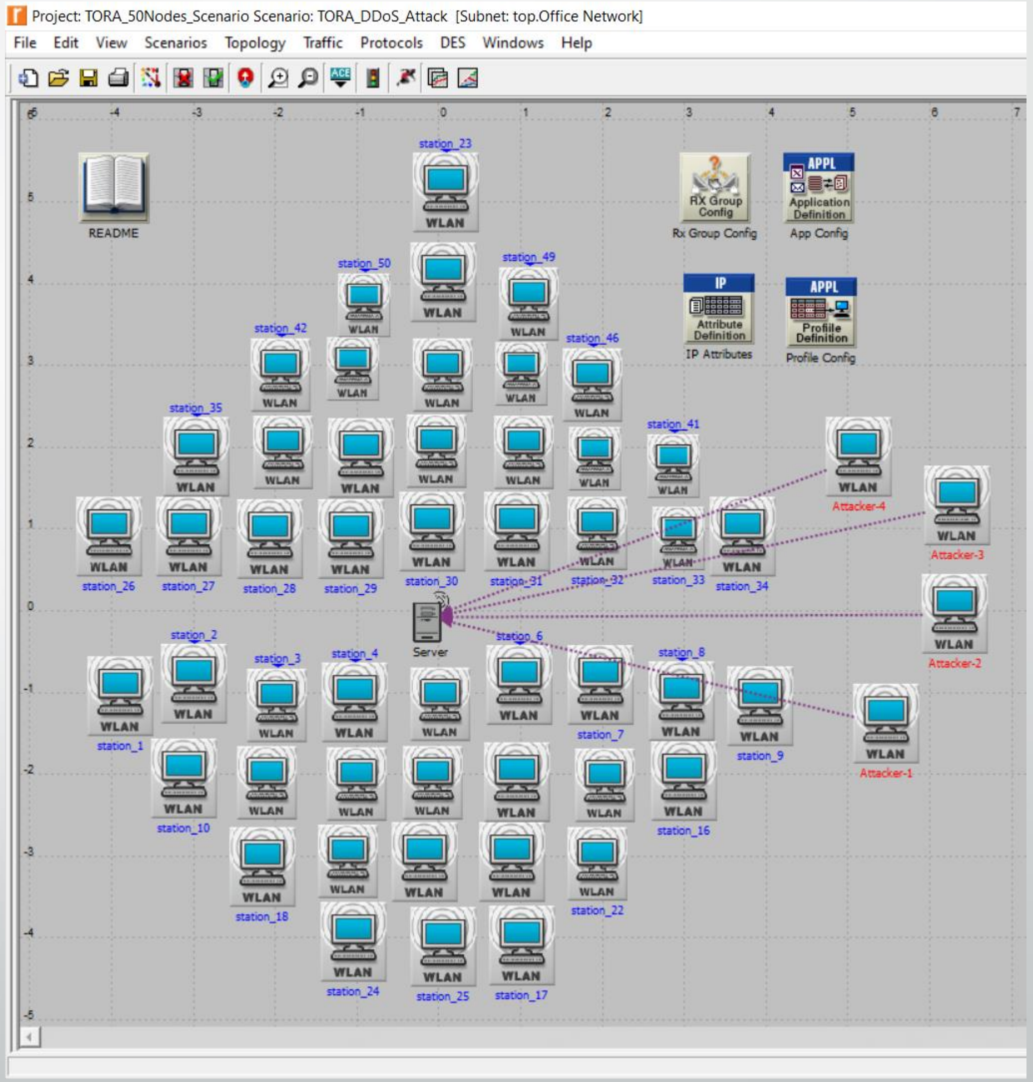
X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 0.2 seconds

Scenario-4: 50-Node TORA P2P Network



Project: TORA_50Nodes_Scenario Scenario: TORA_Ideal_Setup [Subnet: top.Office Network]

Figure 25: 50 WLAN Nodes TORA Network



Project: TORA_50Nodes_Scenario Scenario: TORA_DDoS_Attack [Subnet: top.Office Network]

Figure 26: 50 WLAN Nodes TORA Network under DDoS Attack

Scenario-4: 50-Node TORA P2P Network (Contd.)

🔴 Ideal Scenario 🔵 DDoS Attack

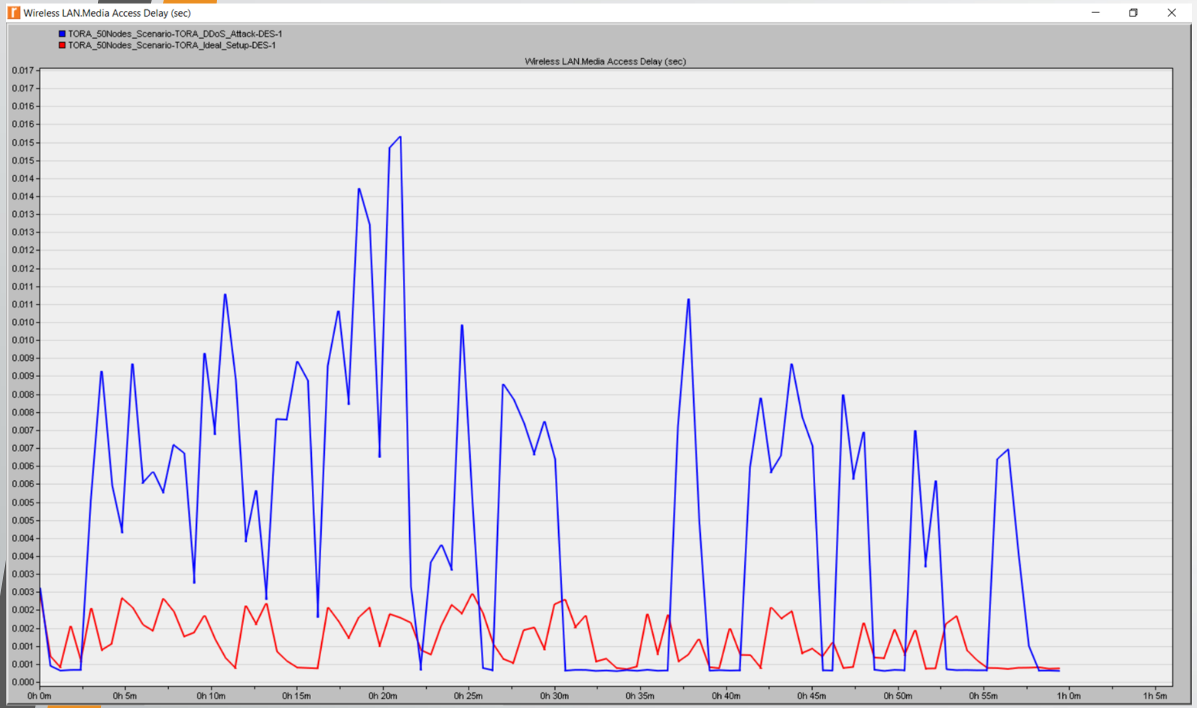


Figure 27: Wireless LAN - Media Access Delay (seconds)

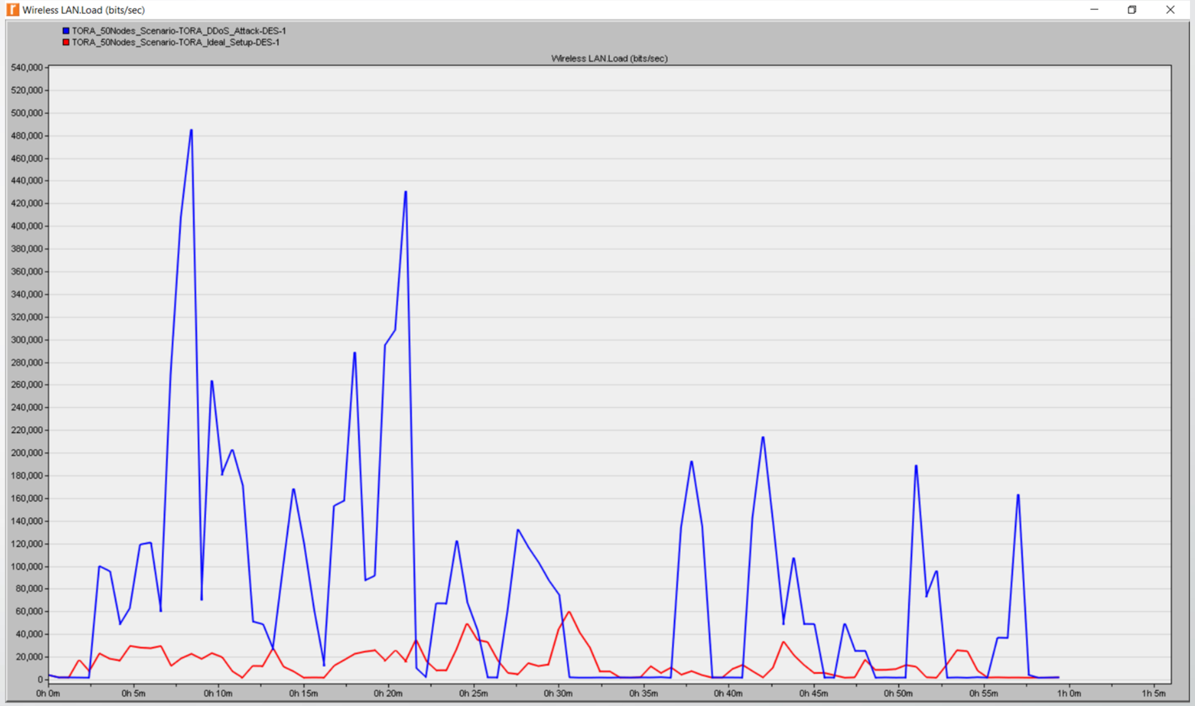


Figure 28: Wireless LAN - Load (bits/sec)

Media Access Delay (seconds): **Highest increased by around 650%** (while performing DDoS Attack)

Load (bits/sec): Increased between 300%-600% (while performing DDoS Attack)

X-axis: 1 unit = 5 minutes
Y-axis: 2 units = 0.001 seconds

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 20,000 bits

Scenario-4: 50-Node TORA P2P Network (Contd.)

🔴 Ideal Scenario 🔵 DDoS Attack

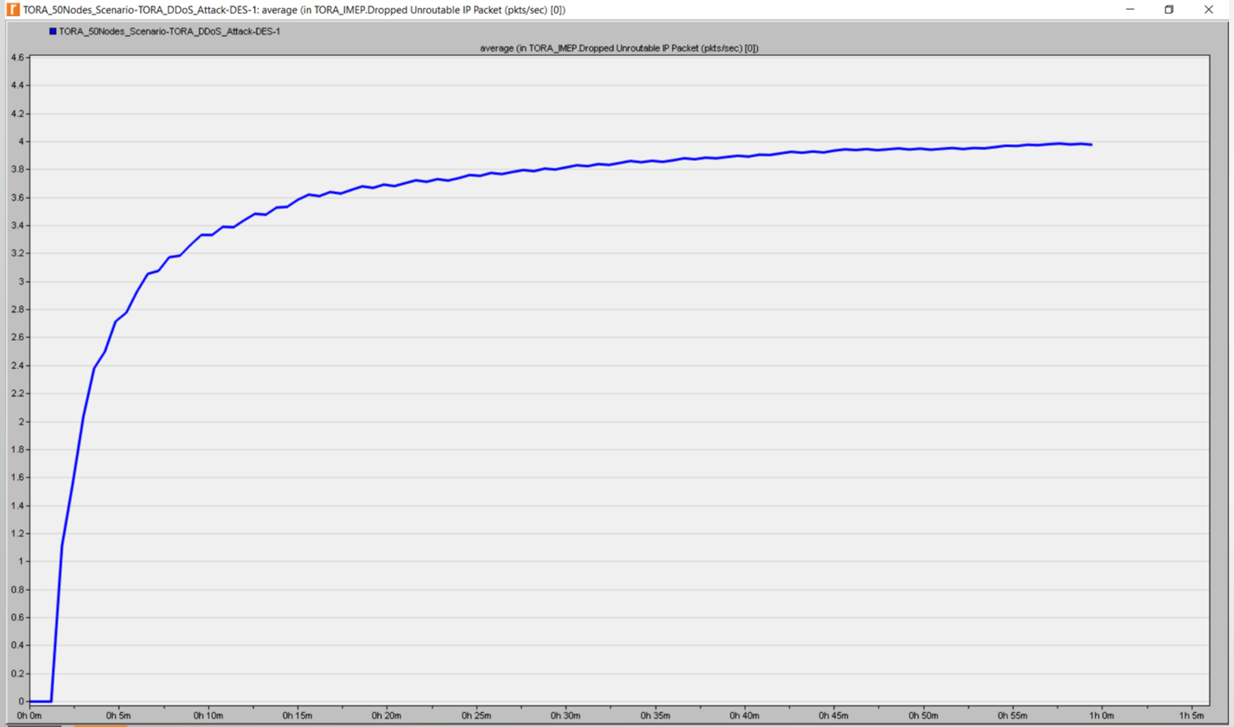


Figure 29: IMEP* Dropped Unroutable IP Packets in TORA

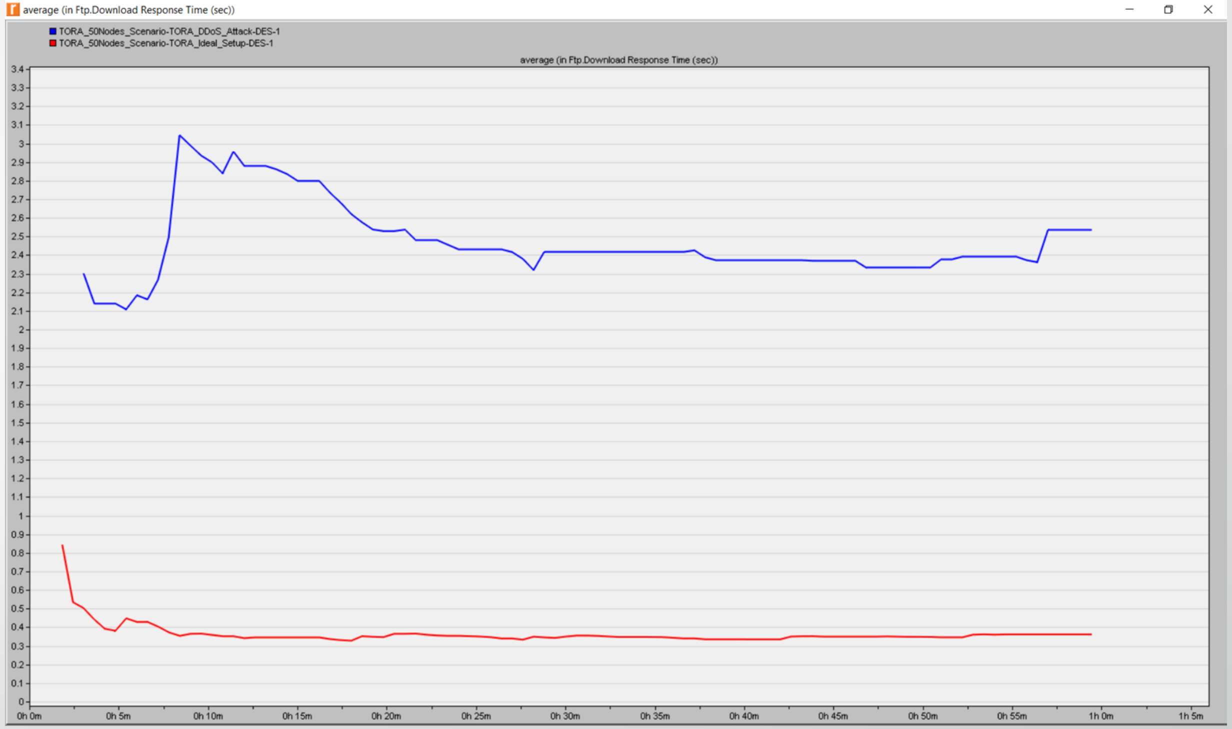


Figure 30: Avg. FTP Download Response Time (Seconds)

Observed unrouted packet drops during DDoS Attack, but not significant amount. No packet drops during ideal condition

FTP Download Response Time: Increased by around 500% (during DDoS Attack)

X-axis: 1 unit = 5 mins
Y-axis: 1 unit = 0.2 packets/sec

*IMEP: Internet MANET Encapsulation Protocol

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 0.1 seconds

Scenario-5: Performance Comparison Between AODV, DSR, and TORA (Ideal Condition)

● DSR ● AODV ● TORA

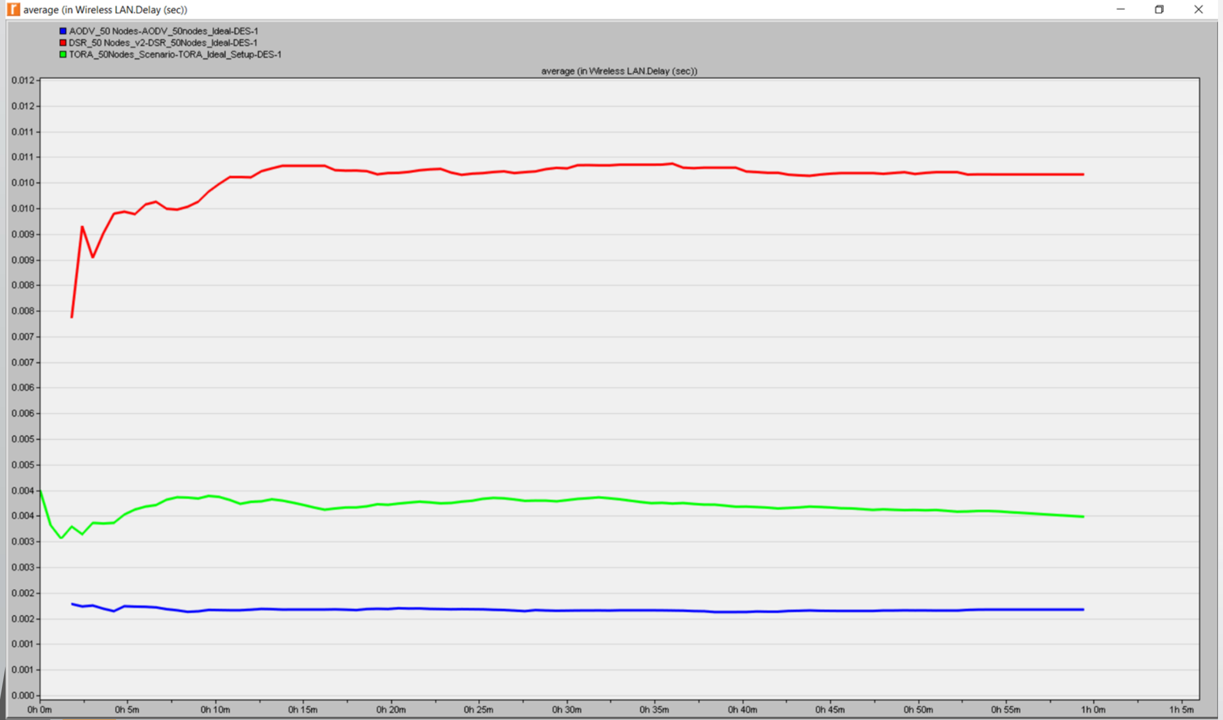

average (in Wireless LAN.Delay (sec))

Figure 31: Avg. Wireless LAN - Delay (seconds)

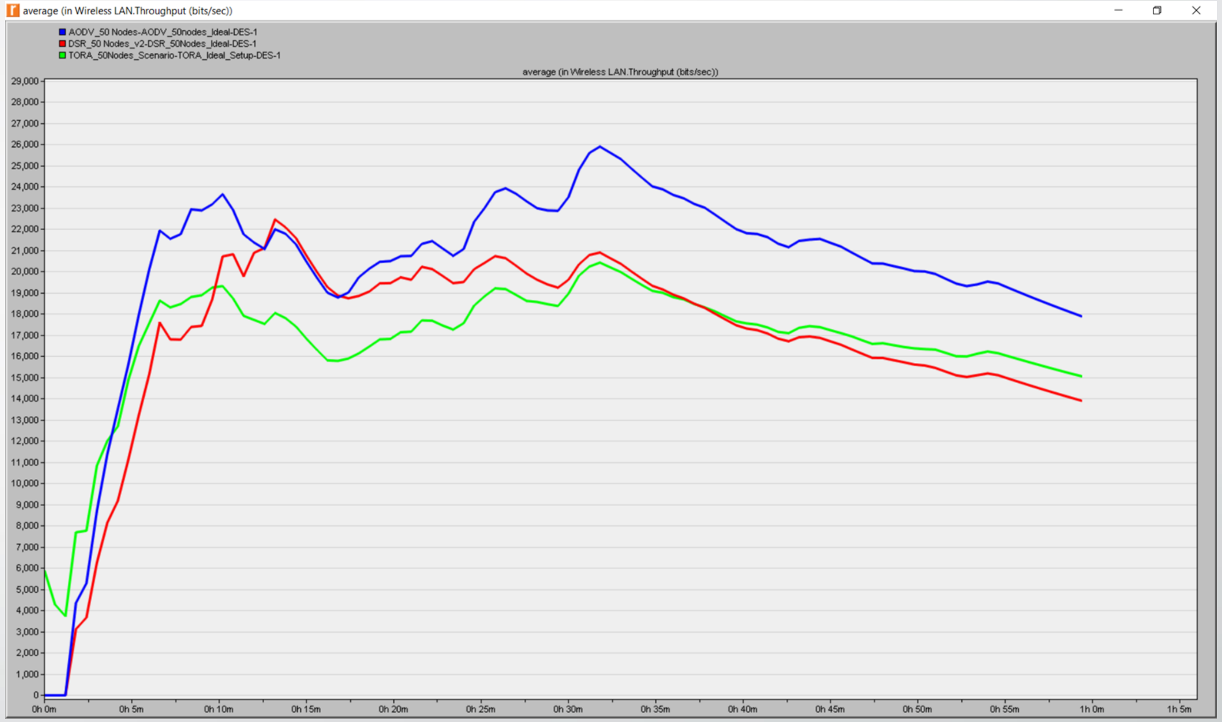

average (in Wireless LAN.Throughput (bits/sec))

Figure 32: Avg. Wireless LAN - Throughput (bits/second)

End-to-End Delay: AODV routing algorithm performs better than DSR & TORA.

Overall, AODV routing algorithm had better **throughput** than DSR & TORA.

X-axis: 1 unit = 5 mins
Y-axis: 2 units = 0.001 sec

Delay represents the end-to-end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer.

Throughput represents the total number of bits forwarded from wireless LAN layers to higher layers in all WLAN nodes.

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 1000 bits/sec

Scenario-5: Performance Comparison Between AODV, DSR, and TORA (DDoS Attack Condition)

● DSR ● AODV ● TORA

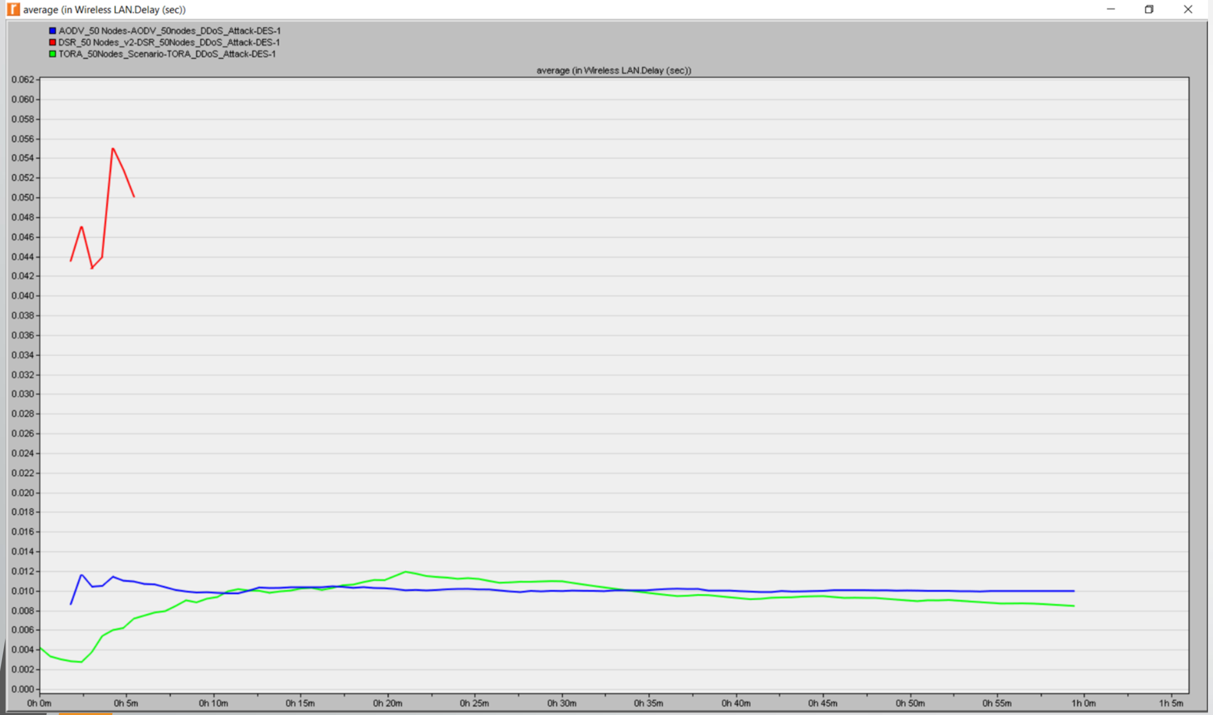


Figure 33: Wireless LAN - Delay (seconds)

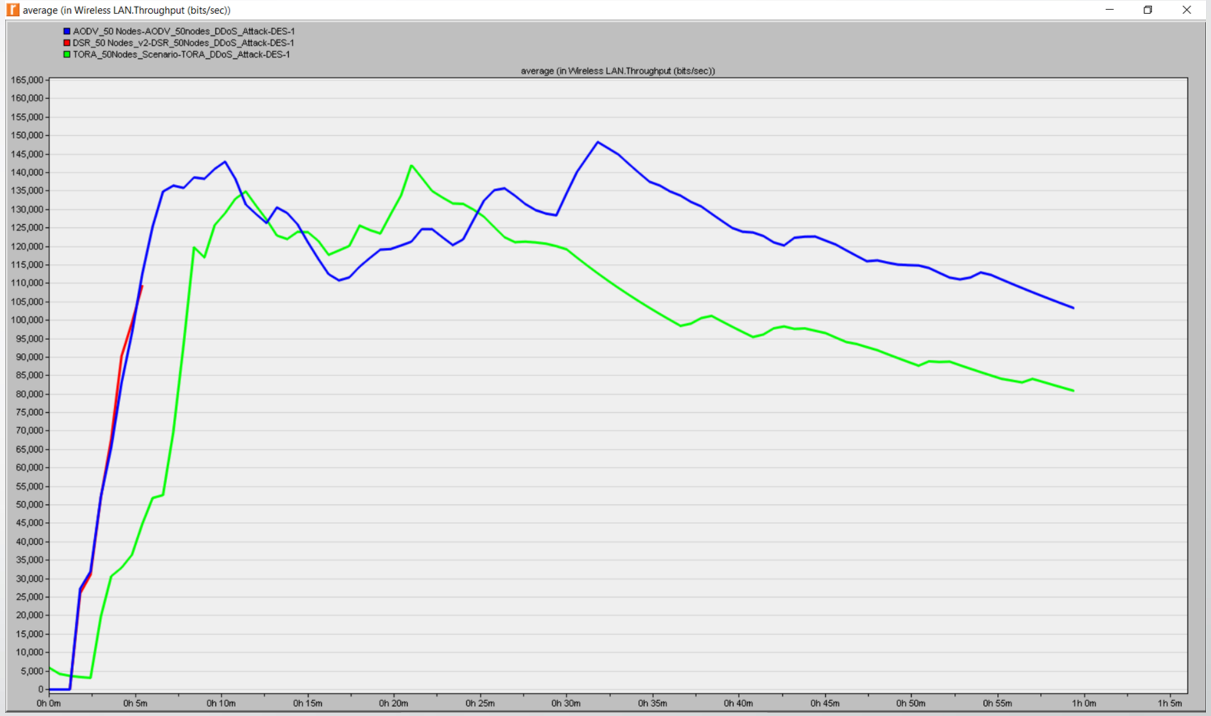


Figure 34: Avg. Wireless LAN - Throughput (bits/second)

X-axis: 1 unit = 5 mins
Y-axis: 1 unit = 0.002 sec

End-to-End Delay: AODV & TORA routing algorithms are performed better than DSR.
Throughput: AODV fairly had better throughput than TORA. But, *DSR had similar throughput trend with AODV* network until shutting down for DDoS attack.

X-axis: 1 unit = 5 minutes
Y-axis: 1 unit = 5000 bits/sec

Conclusion

- As per the goal, we have simulated Sybil attack in MANET network and understood how traffic flow is being affected by Sybil attacker in MANET network.
- We have demonstrated DDoS attack for different routing protocols (AODV, DSR, TORA) in a 50-node wireless peer-to-peer network.
- We have analyzed performance of these peer-to-peer wireless networks based on Delay, Media Access Delay, Load, Throughput, FTP Download Response Time, and Number of Packets Dropped.
- We have seen that AODV & TORA routing protocols are performing much better than DSR routing protocol when executing DDoS attack.
- AODV is preferred as the basic protocol to perform simulations because the AODV protocol can perform well in high mobility and high traffic communication network.
- Though both the DSR & TORA routing algorithms were designed for multi-hop wireless networks, but TORA network is performing better than DSR because the TORA network can efficiently reroute the traffic if there is any link failure.
- The damage due to a DDoS attack may not be huge in our scenarios, but it can be devastating if implemented with many DDoS nodes.

Future Work

Changes in Network Infrastructure:

- Simulate the attack scenarios with increase of number of nodes and configuration changes.
- Introduce mobility concept into the nodes and analyze how the performance can be affected.

Changes in Implementation Process:

- Demonstrate additional routing algorithms with existing or new network setup.

Taking it further:

- Simulate wormhole attack or other attacks in Ad hoc network with the detection and prevention methodologies.
- Demonstrate wormhole attack in Ad hoc network by using Riverbed Modeler 17.5 academic edition.

Reference List

[1] G. Kaur and P. Thakur, "Routing Protocols in MANET: An Overview," *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 2019, pp. 935-941, doi: 10.1109/ICICICT46008.2019.8993294.

[2] N. Gupta and R. Gupta, "Routing protocols in Mobile Ad-Hoc Networks: An overview," *INTERACT-2010*, 2010, pp. 173-177, doi: 10.1109/INTERACT.2010.5706220.

[3] S. Sinha, A. Paul and S. Pal, "The sybil attack in Mobile Adhoc Network: Analysis and detection," *Third International Conference on Computational Intelligence and Information Technology (CIIT 2013)*, 2013, pp. 458-466, doi: 10.1049/cp.2013.2629.

[4] R. Das *et al.*, "Performance analysis of various attacks under AODV in WSN & MANET using OPNET 14.5," *2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2016, pp. 1-9, doi: 10.1109/UEMCON.2016.7777831.

[5] Iftikhar, Waleed & Mahmood, Zunair & Vistro, Daniel. (2020). The Impact Of DDOS And Ping Of Death On Network Performance. International Journal of Scientific & Technology Research. 8. 276-282.

[6] Chhabra, Meghna & Gupta, B B & Almomani, Dr.Ammar. (2013). A Novel Solution to Handle DDOS Attack in MANET. Journal of Information Security. 04. 165-179. 10.4236/jis.2013.43019.

[7] S. A. M. COOK, “DDoS attack statistics, Facts and Trends for 2018-2022,” *Comparitech*, 17-Feb-2022. [Online]. Available: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/. [Accessed: 10-Apr-2022].

[8] Y. Sakurai and J. Katto, "AODV multipath extension using source route lists with optimized route establishment," *International Workshop on Wireless Ad-Hoc Networks, 2004.*, 2004, pp. 63-67, doi: 10.1109/IWWAN.2004.1525542.

THANK YOU

FOR YOUR ATTENTION

ANY QUESTION??