SFU SIMON FRASER UNIVERSITY

ENSC 833: PERFORMANCE OF COMMUNICATION NETWORKS

SPRING 2022

FINAL PROJECT REPORT

Project Title:

Vulnerability Assessment of Ad Hoc Networks under Different Simulation Scenarios

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

Team: 02		
Team Members	**SFU ID**	**SFU Email Address**
Hossain Mohammad Mahbub	301465556	hmm7@sfu.ca
Rohil Malhotra	301472836	rma118@sfu.ca
Md Nawshaad Khan	301448823	nawshaad_khan@sfu.ca

CONTRIBUTIONS OF GROUP MEMBERS

Categories	Hossain Mahbub	Rohil Malhotra	Md Nawshaad Khan
References and literature review	30%	30%	40%
Project website	25%	43%	32%
Simulation scenarios, implementation, analysis, and discussion of simulation results	40%	30%	30%
Project presentation	34%	33%	33%
Written final report	40%	30%	30%

ABSTRACT

An Ad Hoc System is a set of wireless mobile nodes that creates a temporary dynamic network without using any existing network structure or centralized network system. The nodes utilize different routing protocols to communicate with each other, i.e., to forward packets of data to other nodes in the network. There are different classes of wireless ad hoc networks which include mobile ad hoc networks, vehicular ad hoc networks, wireless sensor networks, etc. Nowadays, it is quite challenging to ensure security in ad hoc network due to the lack of centralized privileges and limited resources. DDoS and Sybil attacks are the two most severe security threats in ad-hoc networks. Hence, significant security measures are essential for secured packet delivery operations. In our project, we explore the effects of multiple attacks in mobile ad hoc networks for multiple routing protocols. In the first scenario, we implement sybil attack on 20-node MANET network under AODV routing protocol. From the 2nd scenario to the 4th scenario, we conduct DDoS attack on 50-node wireless peer to peer network for AODV, DSR, and TORA routing protocols. Furthermore, we simulate different scenarios by using the network simulator of Riverbed Modeler Academic Edition 17.5. The performance results of our project work are evaluated based on parameters such as the different number of nodes, load, media access delay, end-to-end delay, number of packets dropped, throughput, FTP download response time, etc. Overall, we present the behavior of performance parameters when there is an attack to assess security vulnerabilities in ad hoc networks in this project.

ACKNOWLEDGEMENTS

We would like to thank the people without whom this project would not have been possible. We extend our gratitude to Dr. Ljiljana Trajkovic, our course instructor, for her guidance throughout the semester, and support during the project, and to the TA, Zhida Li for his valuable suggestions with initial stages of our project.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AODV	Ad hoc On Demand Vector
DSR	Dynamic Source Routing
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IMEP	Internet MANET Encapsulation Protocol
MANET	Mobile Ad Hoc Network
P2P	Peer-to-Peer
RREP	Route Reply
RREQ	Route Request
TORA	Temporally Ordered Routing Algorithm

CHAPTER 1: INTRODUCTION

After the invention of the internet in the 1970's the road to new technological advancements hasn't stopped. With the newfound popularity of the internet using Local Area Networks there was a need for wireless networks that can be accessed without the need for physical cables. The progress of wireless networks and accessibility of wireless devices is what made wireless networks so popular. This progress in wireless communication has brought new technologies like satellites, Infrared Communication & Bluetooth Technology just to name a few.

An Ad-Hoc Network is a collection of communication devices that want to communicate among themselves, but have no pre-defined communication links or fixed infrastructure available. The main idea is that not all nodes are able to communicate with each other so each node has to relay packets on behalf of other nodes to send the data forward [1].

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) and many more. For our project we will focus on Mobile Ad Hoc Network (MANET) [2].

A Mobile Ad Hoc Network (MANET) is a type of decentralized network where data is flowed using the participating nodes in the network where, each node is used to forward data to the next node and this decision of determination is done dynamically by looking at the routing algorithm in use and network connectivity [3]. MANET is a type of Ad Hoc network which has special characteristics like dynamic topology, distributed network, fast and quick implementation and hop-by-hop communications.

A MANET network device is free to go in any direction and due to that changes its link to other devices often. A MANET has significant advantages over a traditional system, as a MANET does not have a structure with a base station and is therefore not affected as such when there are base station failures causing connectivity outages, a MANET can be routed through multiple paths thus reducing the risk significantly, but such an ability reduces the security of the network. Large scale use of MANET is hard due to the desire to route packets through each node, need to maintain real-time routing data, has to share the bandwidth, is unaware of other's needs.

Security in MANET is an important component for the main functions like routing and packet forwarding. Network operations can be put at risk if countermeasures are not put in place in the design structure of the network. The Ad-Hoc network is not like other networks with dedicated packet switching, forwarding and network management nodes; in the Ad Hoc network the functions are followed by all the available nodes [1].

This paper focuses on the exploration of the effects of Sybil, DDoS attacks in mobile ad hoc networks for different routing protocols under different simulation scenarios.

CHAPTER 2: LITERATURE REVIEW

2.1 Classification of Major Attacks:

In this section, we will try to illustrate a brief background on the major types of attacks in the Ad hoc Networks.

2.1.1 Blackhole Attack

It is a type of attack in which an attacker invades into the forwarding routes to intercept data packets of the connection. After this the attackers drop some or all of the data packets which it intercepted rather than send it to the next node in the routing path. This type of attack leads to a very low packet delivery ratio [4].

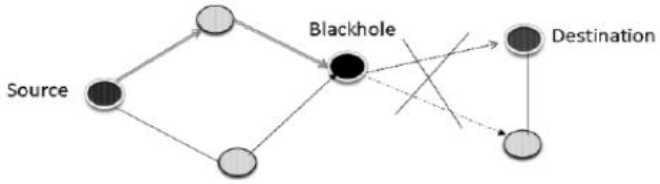


Figure 2.1.1: Blackhole Attack

Bhattacharyya, Aniruddha & Banerjee, Arnab & Bose, Dipayan & Saha, Himadri & Bhattacharyya, Debika. (2011). "Different types of attacks in Mobile ADHOC Network."

2.1.2 Jellyfish Attack

It is a passive type of attack which is very similar to the blackhole attack but the difference is that it can either drop the data packets or change the order of the packets and can also cause some sort of delay in it. In addition, the attacker can also change the order of the packets, reorder and send them to their destination [4].

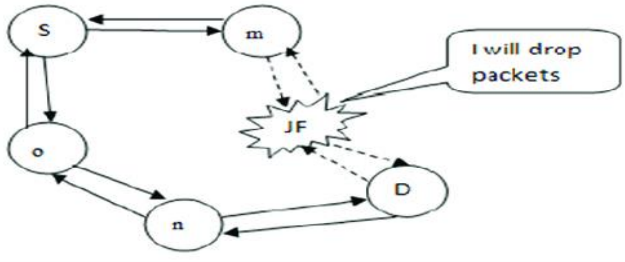


Figure 2.1.2: JellyFish Attack

Doss, Srinath & Nayyar, Anand & G., Suseendran & Tanwar, Sudeep & Khanna, Ashish & Son, Le & Pham, Thong. (2018). APD-JFAD: Accurate Prevention and Detection of JellyFish Attack in MANET. IEEE Access. 10.1109/ACCESS.2018.2868544.

2.1.3 Wormhole Attack:

A malicious node records packets at one location of the network and then tunnels them to another location [5]. Due to the fault routing information the malicious node can then disrupt routes in the network.

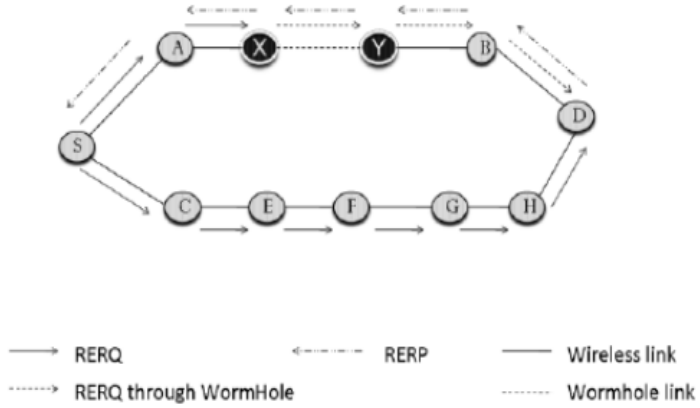


Figure 2.1.3: Wormhole Attack

Bhattacharyya, Aniruddha & Banerjee, Arnab & Bose, Dipayan & Saha, Himadri & Bhattacharyya, Debika. (2011). "Different types of attacks in Mobile ADHOC Network."

2.1.4 Sybil Attack

In this attack, the attacker can gain influence on the network by forging multiple false identities of trusted nodes and gain influence in the network. Due to an absence of authority in the network and the process in which the nodes in the established network can vouch for the other nodes, the sybil nodes can generate a chain of trust with the malicious nodes therefore compromising all identities in the network [6].

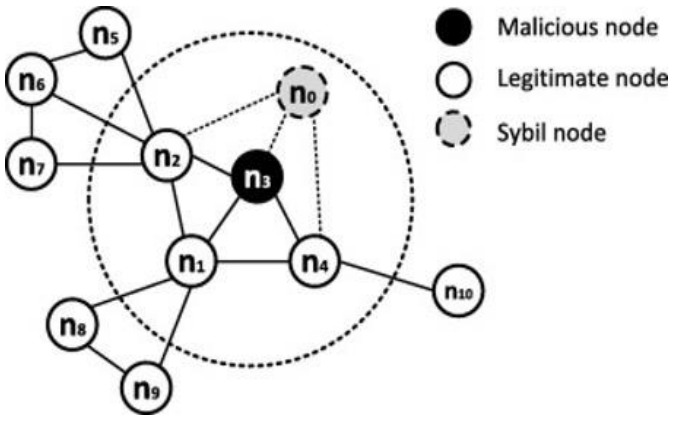


Figure 2.1.4: Sybil Attack

Panagiotis Sarigiannidis, Eirini Karapistoli, Anastasios A. Economides, Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information, Expert Systems with Applications, Volume 42, Issue 21, 2015,Pages 7560-7572, ISSN 0957-4174

2.1.5 DDoS Attacks

In this attack, the attacker can decrease the quality or fully break down the victim's network connectivity. 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 [7].

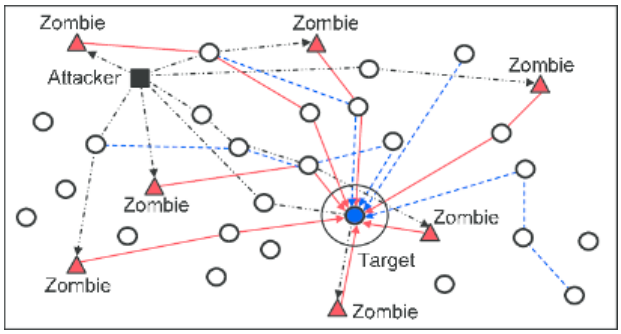


Figure 2.1.5: DDoS Attack

Stojanovic, Mira & Acimovic-Raspopovic, V & Timcenko, Valentina. (2012). The impact of mobility patterns on MANET vulnerability to DDoS attacks. Elektronika ir Elektrotechnika. 1392-1215. 10.5755/j01.eee.119.3.1358.

2.2 Routing Protocols in Mobile Ad hoc Networks

Routing protocols in MANET are classified based on the procedure of routing information acquisition and maintenance by network nodes, utilized metrics for path creation and information routing. Generally, these protocols are divided into three broad categories- proactive, reactive and hybrid which are further subdivided as following [8]:

2.2.1 Proactive Routing Protocols:

This is a table-driven process where routers in the network exchange information periodically to update their own routing table. Delays and risk of loops decreases while plenty of routing information creates burden on the nodes. Feasible for smaller networks comprising about 50 nodes hence it has reduced scalability.

2.2.2 Reactive Routing Protocols:

This a demand-based approach where routes are explored, and routing information is updated depending on necessity. The process is initiated when there is a change in the topology and the source needs to send a packet to the destination. Lesser traffic is generated in comparison to proactive routing protocol.

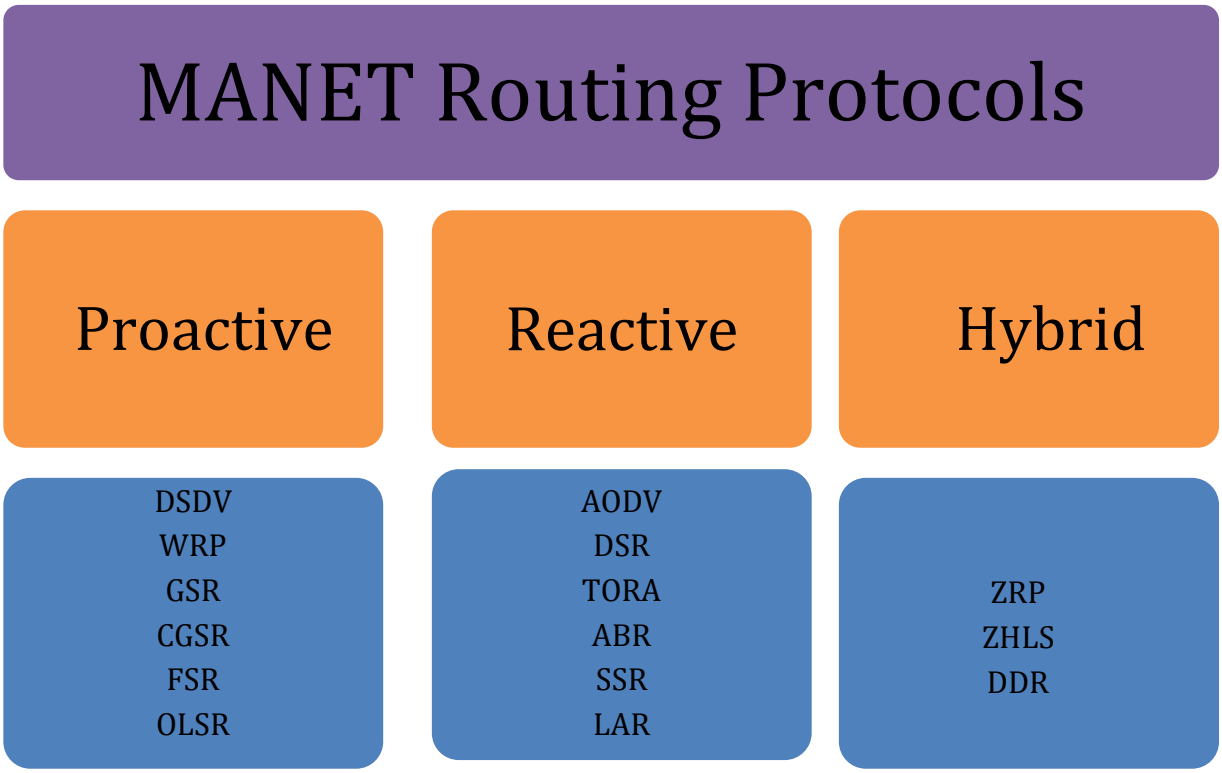


Figure 2.2: MANET Routing Protocols

For this project AODV, DSR and TORA protocols have been used, which are briefly explained below:

2.2.2.1 AODV:

AdHoc On-Demand Vector is a reactive routing protocol where the route is constructed based on demand and individual nodes do not have to maintain total real time network topology information. Route request (RREQs), Route reply (RREPs) and Route errors (RRERs) are the types of messages used in this protocol. Query and reply to cycles are the basis of route exploration. A Unicast RREQ message is sent to inquire about a node and a reply is received. When any node is not linked anymore an error message is raised and other nodes are notified.

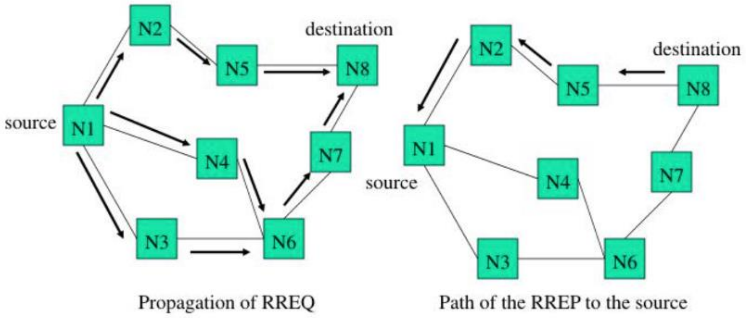


Figure 2.2.2.1: AODV

2.2.2.2 DSR:

Dynamic Source Routing is another type of reactive routing where periodic messages like AODV are not required thus network bandwidth and battery usage is reduced. It is specially designed for multi hop wireless ad hoc networks consisting of mobile nodes. Complete source to destination routing information is carried in each packet and multiple routes are allowed. Two mechanisms called Route Discovery and Route Maintenance are used in this routing protocol [8]. There is less possibility of count to infinity complication and DSR is also efficient in terms of route discovery and maintenance.

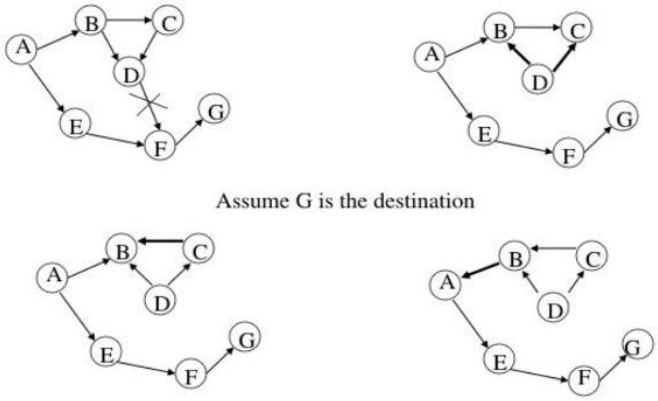


Figure 2.2.2.2: DSR

2.2.2.3 TORA:

Temporarily Ordered Routing Algorithm is a source initiated multipath routing protocol based on three functions- creation, maintenance, and erasure of nodes. Control messages within the network are localized and distributed based on topology. Adaptive link reversal and node coordination allows the prevention of count to infinity complication [8].

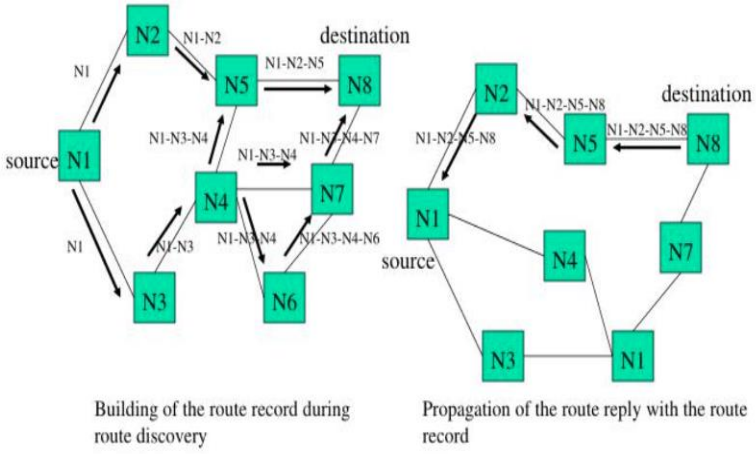


Figure 2.2.2.3: TORA

2.2.3 Hybrid Routing Protocols:

This approach utilizes properties from both proactive and reactive protocols to stabilize the network. Proactive routing is used within small clusters within the network while reactive routing is used for creating optimal path to destination. Rebroadcast of the same information is reduced and route exploration is limited among a few selected numbers of nodes.

CHAPTER 3: RELATED WORK

Following papers are closely related to our project and have been studied to develop a deeper understanding of the relevant topics.

S. Sinha et. al. (2013), "The sybil attack in Mobile Adhoc Network: Analysis and detection" discussed different types of security attacks in MANET with emphasis on the Sybil attack and proposed a new approach to detect Sybil attack based on clustering and resource testing [9].

R. Das et al. (2016), "Performance analysis of various attacks under AODV in WSN & MANET using OPNET 14.5" introduced an algorithm to design a Mobile Ad-hoc network (MANET), Wireless Sensor Network (WSN) and compares the effect of different network and physical layer attacks [10]. Various attacks are also simulated 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" discussed several scenarios and demonstrated DOS and DDoS attacks on Riverbed Modeler [11].

M. Chhabra et. al. (2013), "A Novel Solution to Handle DDoS Attack in MANET" recommended a novel solution to handle DDoS attacks in mobile ad hoc networks (MANETs) [12].

CHAPTER 4: SIMULATION SCENARIOS & RESULTS

An effective analysis of a DDoS attack requires it to be implemented on a network simulation tool. The selection of a network simulation tool is a challenge, and it totally depends on the characteristics of a specific experiment. The riverbed modeler is the leading network simulation tool in the industry and has a good graphical user interface for analyzing the results of an experiment [13]. In this chapter, we have implemented different routing protocols in the Ad hoc Network environment, and we have studied the Sybil attack and DDoS attack in the Ad hoc network. For this simulation, the Academic edition of Riverbed Modeler 17.5 is used. This simulation software is user-friendly, and it has a good number of features to work on.

Section 4.1 illustrates initial validation process of our project ideas, and we have successfully able to implement DDoS attack in Riverbed Modeler. Section 4.2 discusses necessary simulation parameters for different scenarios which we have used to perform our simulations. Section 4.3 explains about simulation methodology of 20-Node MANET network scenario and its simulation results. Section 4.4 discusses about simulation methodology of 50-node AODV network scenario and its simulation results. Section 4.5 describes about simulation methodology of 50-node DSR network scenario and its simulation results. Section 4.6 describes about simulation methodology of 50-node TORA network scenario and its simulation results. Moreover, Section 4.7 provides comparison data between three routing protocols (AODV, DSR, TORA) for multiple parameters.

4.1 Project Validation Process

4.1.1 Simulation Methodology

After choosing the simulation tool, an experimental network topology is first created for our project. When the network topology is formed, some parameters are set. Once the parameters are set, we run the simulation for a specified period of time. After running the simulation successfully, we can verify necessary validation process of our created network topology.

First, we have implemented the topology in a small campus network, and from the Figure 4.1.1(a), we can see the original network is free from any kind of attackers. It simply shows two nodes that are named as ‘College of Engineering (CE)’ and ‘College of Arts and Sciences (CAS)’ connected to a single server over a wireless network. The wireless network is created using a switch which is further connected to a Cisco router, and then linked to an internet connection. Similarly, the server is connected to a Cisco router and then provided internet access. The ‘Application_Config' and ‘Profile_Config’ are implemented to configure specific network properties. The ‘College of Engineering’ is a simple Ethernet workstation which supports a profile that is created using ‘Profile_Config’. Similarly, the ‘College of Arts and Sciences’ supports a profile that is also created using the ‘Profile_Config’. The internet connection for the entire scenario is provided using an “ip32_cloud” model available in the riverbed. The server that is connected on the other

side of the network is configured to support all kind of services that are sent to the server. The two profiles created using “Profile_Config” are CE, and CAS profiles. Routers connected to the internet is completed using the PPP_DS1 cables, while the rest of the network is connected using simple 10Base LAN cables [14].

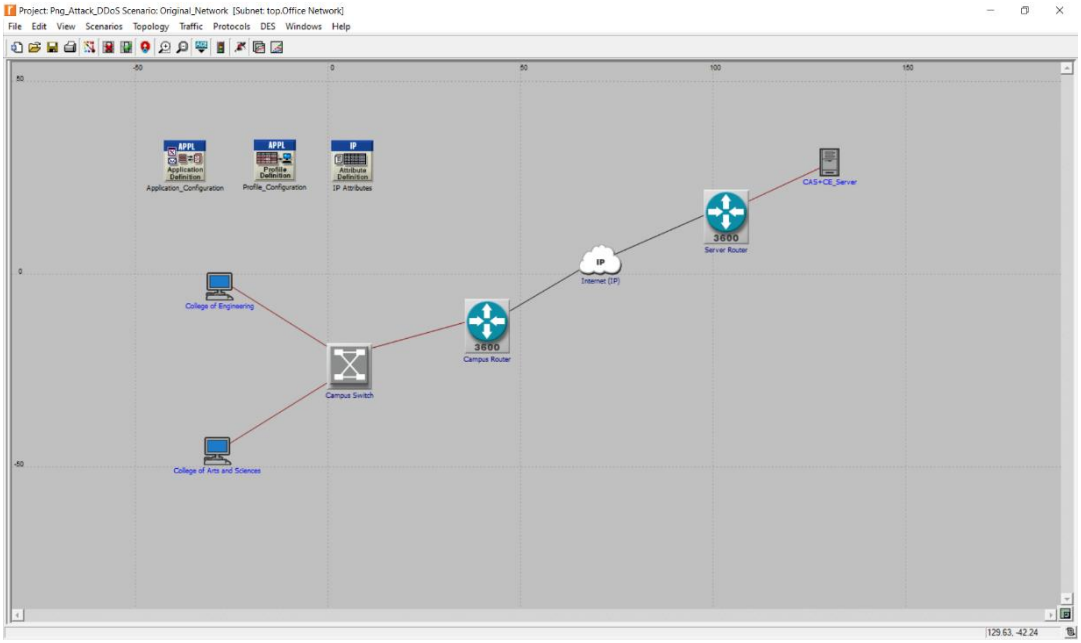


Figure 4.1.1(a): First Scenario - Original Network

To implement the DDoS attack, ‘IP Attribute’ is really vital to be set accordingly. The figure below displays the configuration of IP attributes. The important attribute is the Packet size and is set as 65527 bytes with an unlimited count [14]. So, attacker node sends unlimited requests to the server.

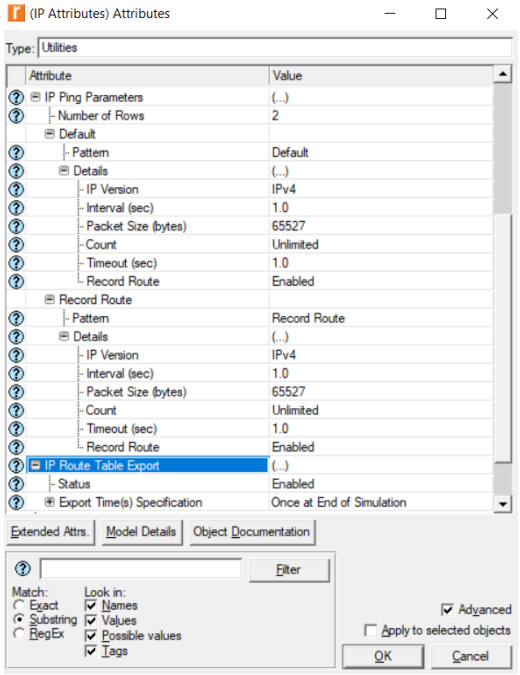


Figure 4.1.1(b): IP Attribute Configuration

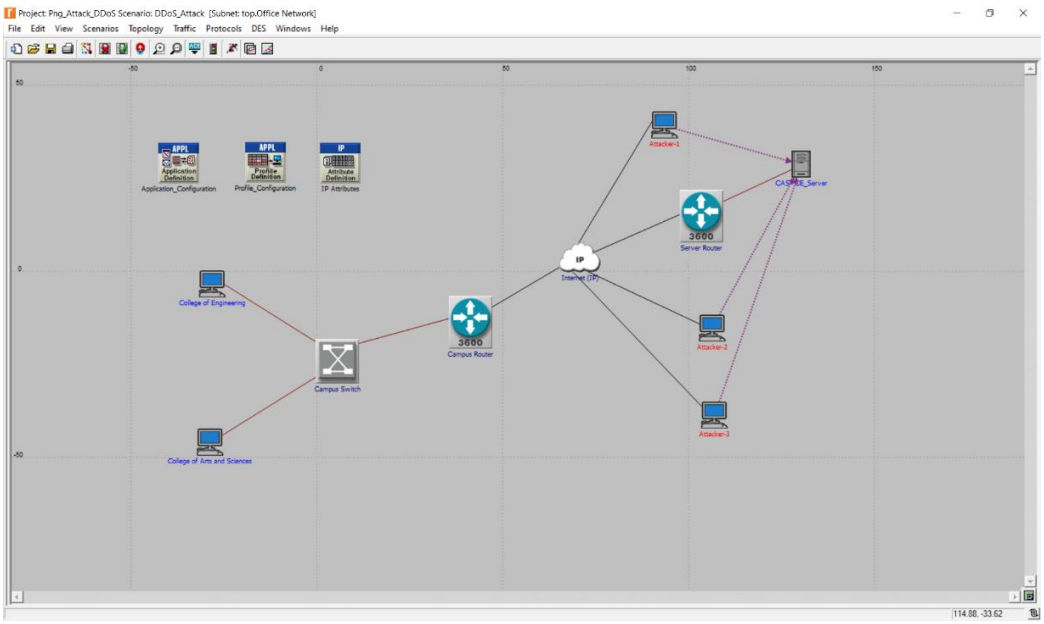


Figure 4.1.1(c): Second Scenario - DDoS Attack

The second scenario is the DDoS attack setup in the original network. The number of attackers is three (3) and it is what happens in a typical Distributed denial of service attack. This attack is well-defined as more dangerous and is typically difficult to predict [14].

4.1.2 Simulation Results

We run this simulation for 2 hours. After running the simulation, we have recorded DB Query Response Time, Traffic Sent, and Traffic Received for original and DDoS attack networks.

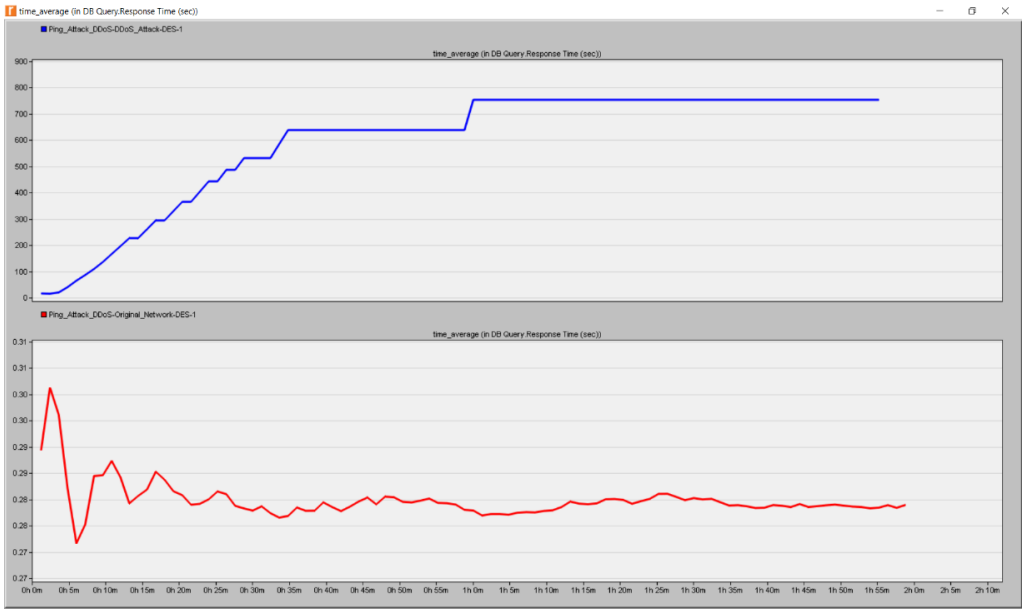


Figure 4.1.2(a): Average DB Query Response Time (Sec)

From the Figure 4.1.2(a), we observe that the DB query response time of the original network, which is shown by the red line, is undoubtedly better as compared to the DB query response time of the DDoS attack network, which is displayed by the blue line.

Additionally, we have observed ‘Traffic Sent’ and ‘Traffic Received’ statistics from following two graphs. We have seen that packet transmission is significantly dropped due to DDoS attack on the original network (Figure 4.1.2(b)).

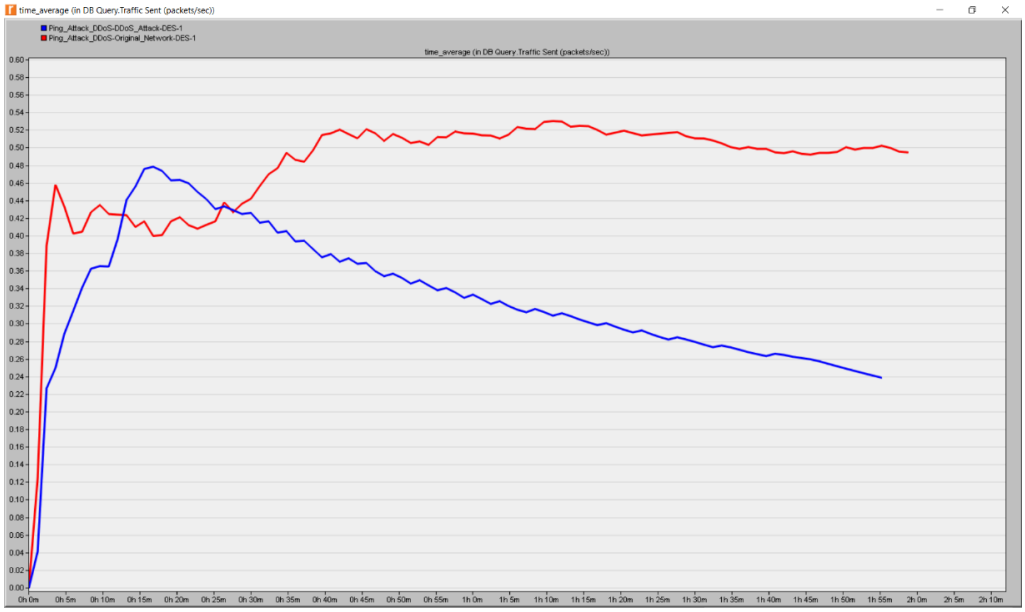


Figure 4.1.2(b): Traffic Sent (packets/sec)

We have also seen that the rate of received packets has dropped significantly due to DDoS attack compared to original network scenario (Figure 4.1.2(c)).

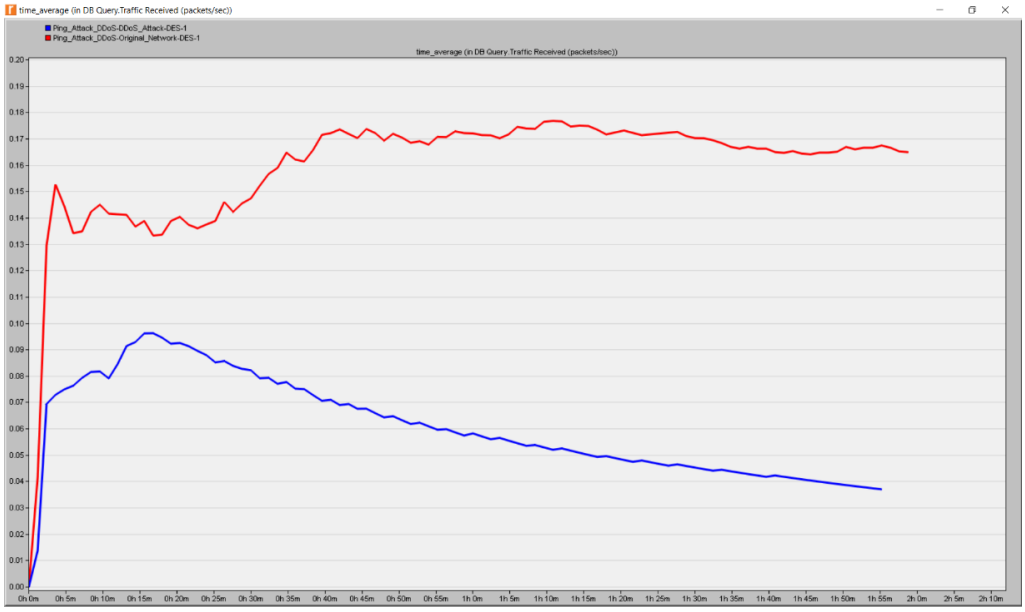


Figure 4.1.2(c): Traffic Received (packets/sec)

This comparison explains that the involvement of DDoS attacks on the network has significantly reduced the performance of the entire network. Hence, the validation process of this network topology is completed successfully based on given network configurations and parameters.

4.2 Simulation Criteria and Parameters

4.2.1 Parameters Part-I *(MANET Network Scenario/Scenario-01)*

We followed this set of parameters for only Scenario-01. We have implemented the AODV routing protocol for a 20-node wireless MANET network. We have executed simulations for both ideal and Sybil attack scenarios [15]. Nodes are arranged in random order and no specific topology is used. We demonstrated this simulation scenario by using Riverbed Modeler 17.5 academic edition. **In this scenario, packets sent and received are analyzed.** Important network parameters for this scenario are attached below in a tabulated form:

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)

Table 4.2.1 Network Parameters-I

4.2.2 Parameters Part-II *(Scenario-02 to Scenario-05)*

We followed this set of parameters for Scenario-02 to Scenario-05. We have implemented AODV, DSR, TORA routing protocols for 50-node wireless peer to peer network. We executed simulations for ideal and DDoS attack scenarios for each routing protocol. We demonstrated this simulation scenario by using Riverbed Modeler 17.5 academic edition. Nodes are arranged in random manner and no specific topology is followed. **Data are analyzed based on load, media access delay, and number of packets dropped, etc.** We have used 'IP Ping Traffic Flow' mechanism, and 'IP Attribute configuration' from Riverbed Modeler for implementing DDoS attack [14]. We have attached important network parameters for this scenario in a tabulated form:

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)

Table 4.2.2 Network Parameters-II

4.3 MANET Network Scenario *(Scenario-01)*

4.3.1 Simulation Methodology

For the first scenario, a 20-node wireless MANET network is implemented. The nodes are arranged in random order without following any specific topology. Figure 4.3.1(a) shows the design of the MANET network which is used in the first scenario.

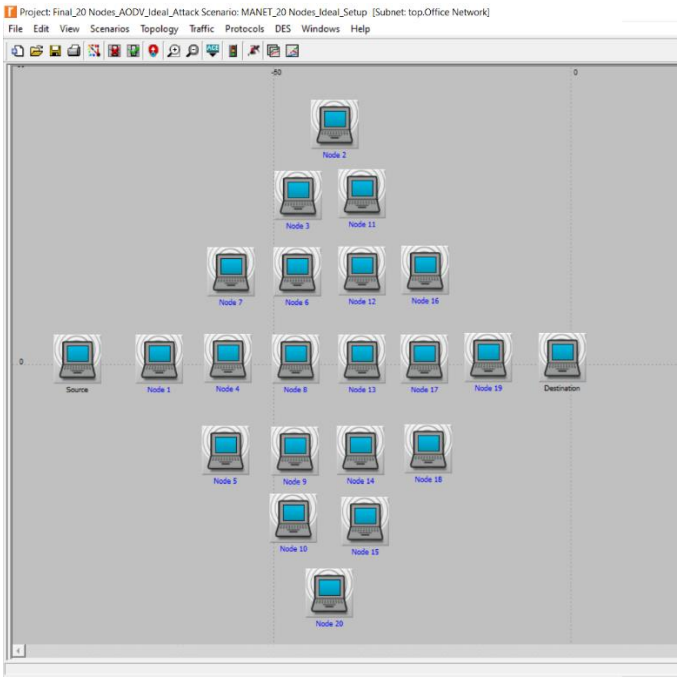


Figure 4.3.1(a): 20-Node MANET using AODV Routing Protocol

The most vital network configurations are made in the MANET traffic generation parameters at the source node [15]. The destination IP is specified in the configuration of the source node, where traffic is generated. This is shown in Figure 4.3.1(b).

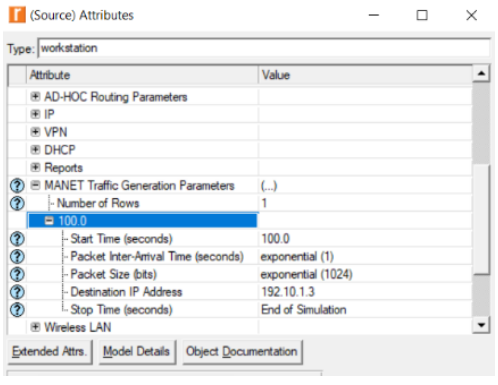


Figure 4.3.1(b): MANET Traffic Generation Parameters at Source Node

Apart from MANET parameters, there are certain configuration settings related to the routing protocol and the destination IP host configurations needs to be setup. Figure 4.3.1(c) and (d) displays the AODV protocol parameters at the source, and at the destination nodes respectively.

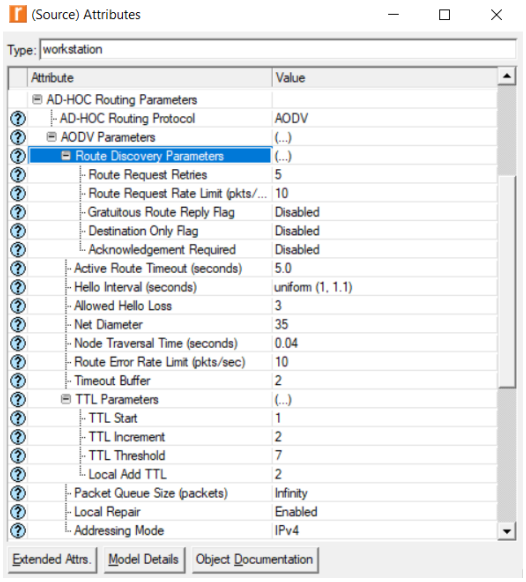


Figure 4.3.1(c): AODV Routing Parameters at Source Node

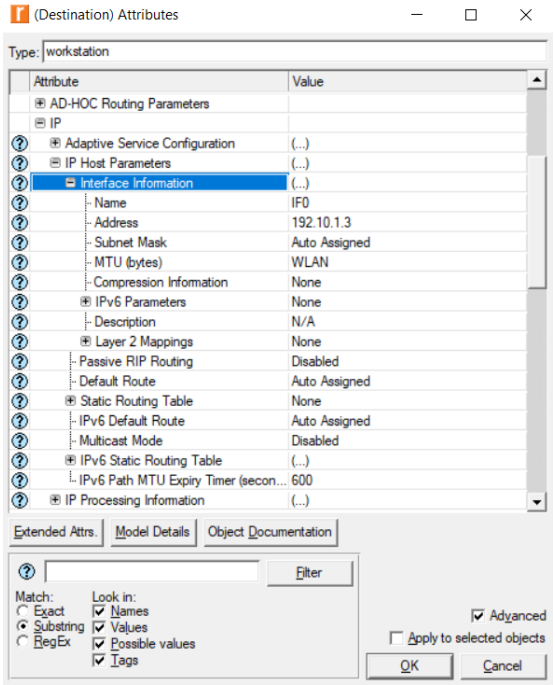


Figure 4.3.1(d): AODV Routing Parameters at Destination Node

The next part of the scenario works with the Sybil attack setup and simulation on AODV routing protocol. Related to the ideal scenario, the network scenario does not change a lot, only with the

addition of a few malicious nodes (attackers) as part of the Sybil network on AODV routing protocol as displayed in Figure 4.3.1(e). Mainly, the Sybil attack reroutes the packet traffic, that is on route to the destination, to the attacker node [15]. The simulation is performed for 30 minutes.

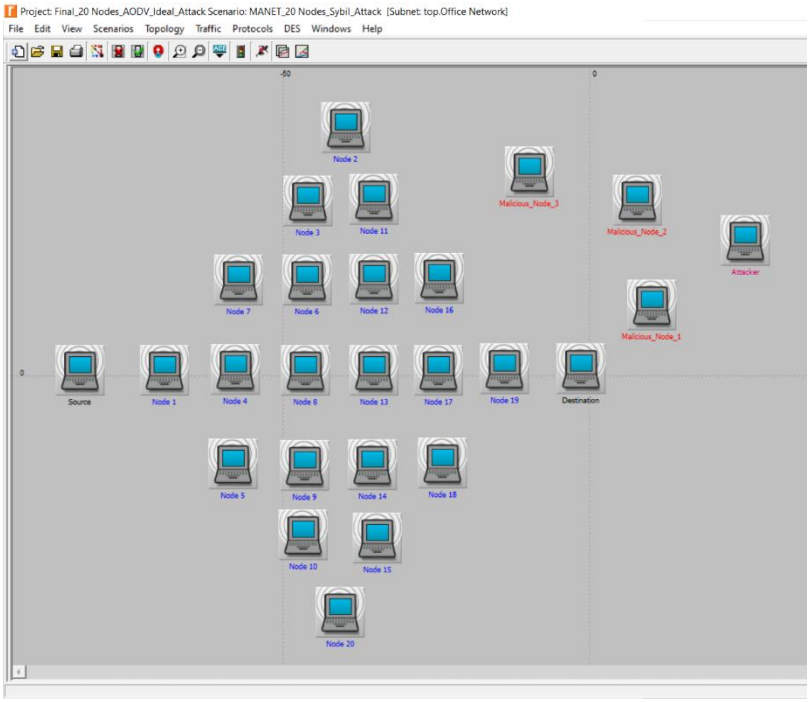


Figure 4.3.1(e): Sybil Attack Scenario on AODV Routing Protocol

4.3.2 Simulation Results

Both the scenarios are ready to simulate, and we are running the simulation to observe the traffic flow. We have already included simulation parameters at Section 4.2.1 from Chapter 4. At the first scenario, traffic will flow from the source node to destination node, whereas the traffic flow from the source to destination will be interrupted because of Sybil attack at the second scenario. Figure 4.3.2(a) demonstrates the simulation results of the ideal scenario.

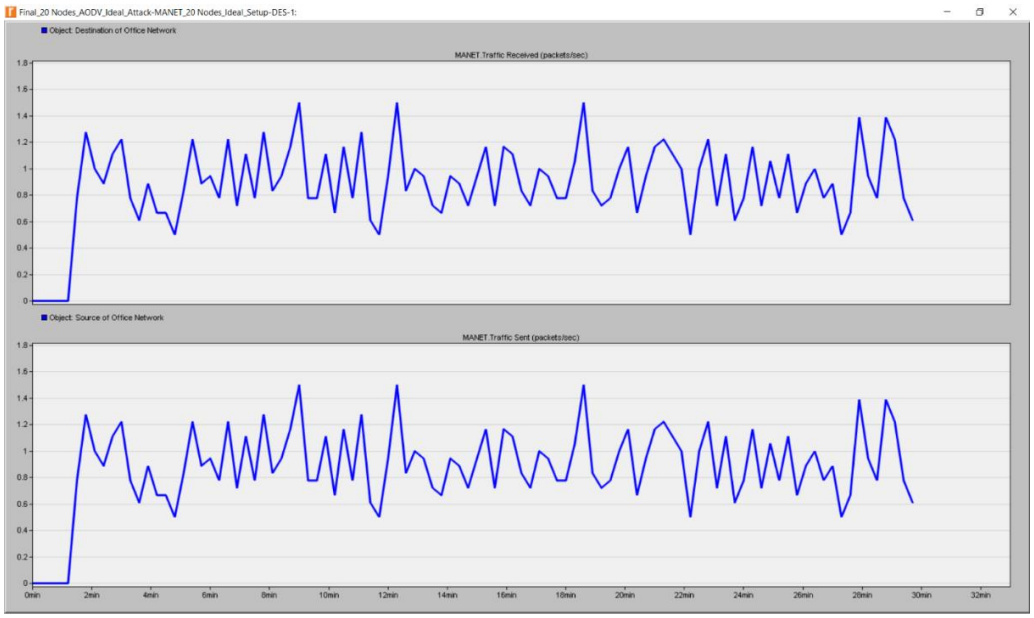


Figure 4.3.2(a): Traffic Flow from Source to Destination (Packets/Sec)

Without any significant modification in the network configurations of source and destination or any intermediate nodes in the first scenario, comparing to the graph of the ideal scenario with the scenario of Sybil attack. From figure 4.3.2(b), we have observed that because of Sybil attack, all traffic is completely re-routed to the 'Attacker' node through the Sybil nodes even though the destination node was much closer to the source than the attacker node.

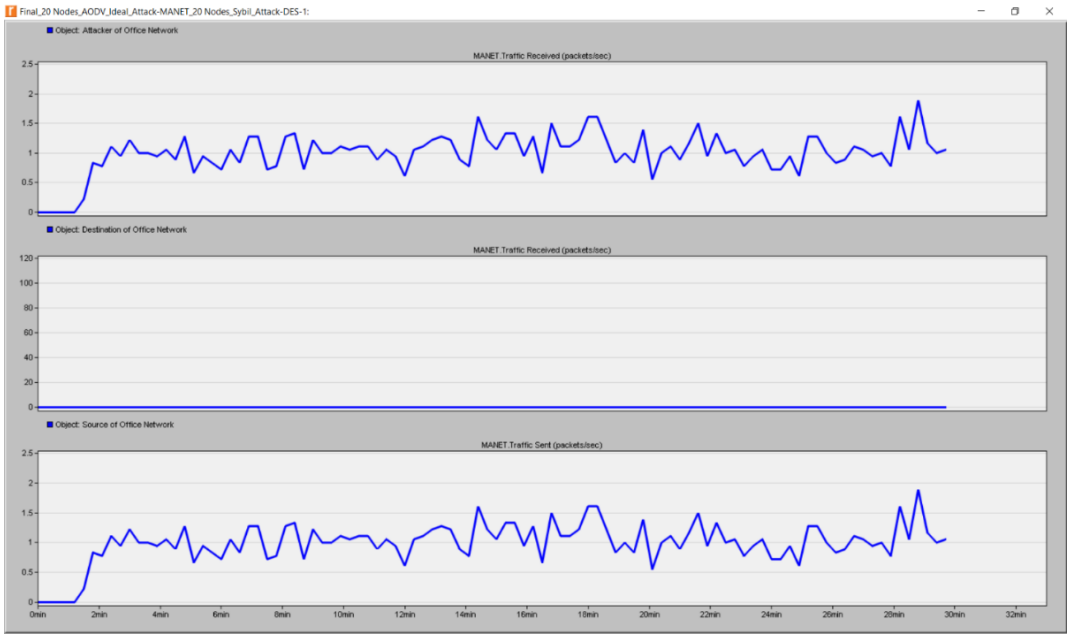


Figure 4.3.2(b): Traffic Flow from Source to Destination & Attacker (Packets/Sec)

4.4 50-Node AODV Network Scenario *(Scenario-02)*

4.4.1 Simulation Methodology

For the first phase (ideal case), a 50-node wireless peer to peer network is executed on AODV routing protocol. The nodes are arranged in random order and no specific topology is followed. All nodes in the network are configured to perform AODV and multiple FTP sessions. Additionally, WLAN data rate is 1Mbps, and simulation is performed for 1 hour. Figure 4.4.1(a) shows the design of the 50-node P2P network used with default parameters on AODV protocol.

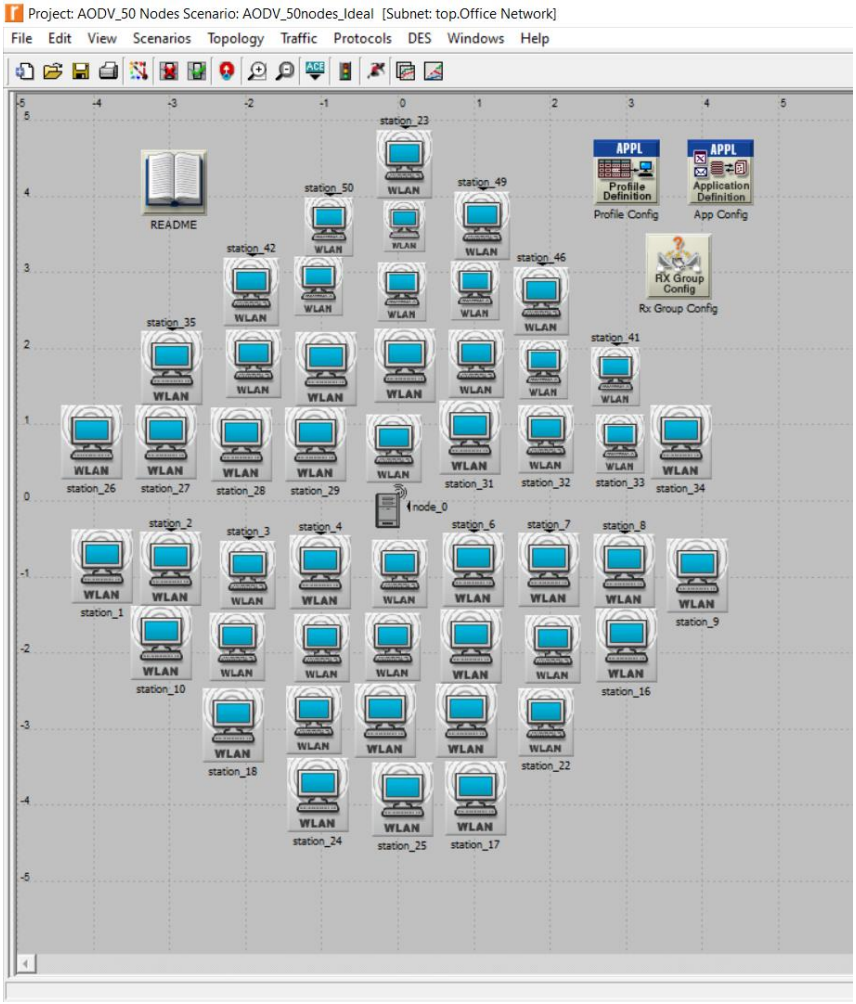


Figure 4.4.1(a): 50-Node AODV Network

For the second phase, a 50-node wireless P2P network is implemented on AODV protocol with DDoS attack. All nodes in the network are configured to run AODV and multiple FTP sessions with high load. We have added 4 attackers in the network, and we have connected those attackers to the server via ‘IP Ping Traffic Flow’ link. We have used ‘IP Attribute’ for implementing DDoS attack in this network. The vital attribute is the Packet size and is set as 65527 bytes with an unlimited count [14]. So, any attacker node can transmit continuous packets to the server.

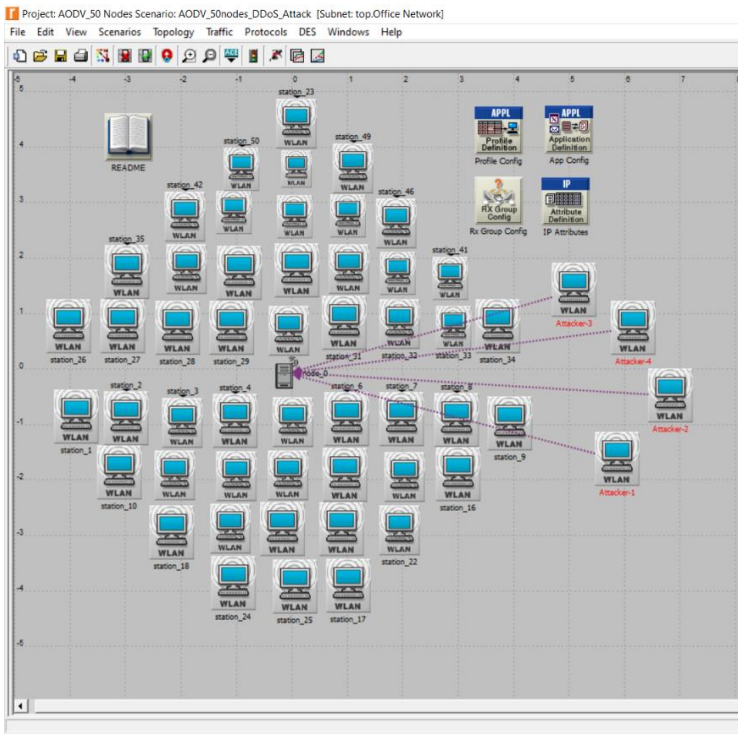


Figure 4.4.1(b): 50-Node AODV Network with DDoS Attack

4.4.2 Simulation Results

The simulation results for the ideal and the DDoS attack scenarios are compared into a single graph for each of the statistics measured. In this section, we measure media access delay, the load on the network, total number of packets dropped, and average FTP download response time.

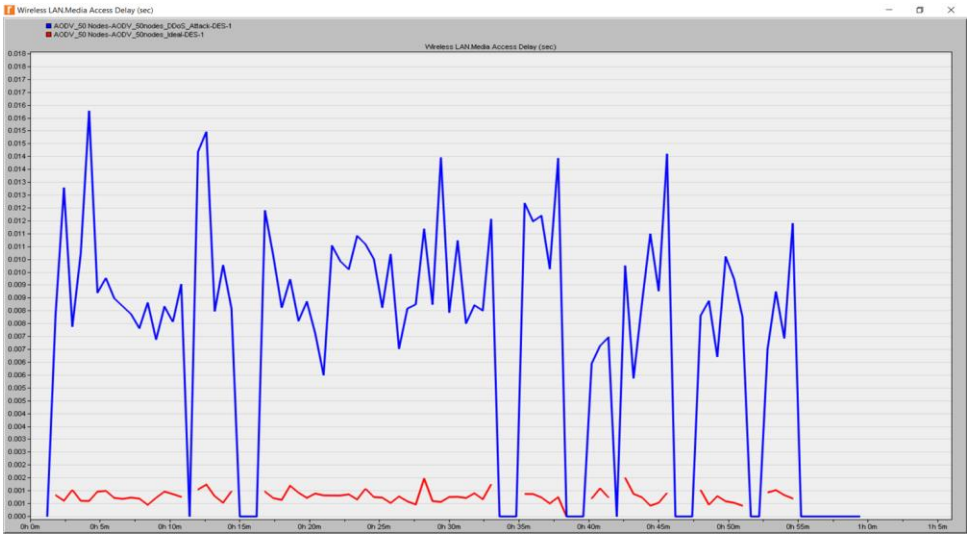


Figure 4.4.2(a): Wireless LAN - Media Access Delay (Seconds)

From the graphs above we understand that in the case of DDoS attack, the media access delay is increased by almost 9 times compared to ideal scenario in AODV protocol. Here, 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.

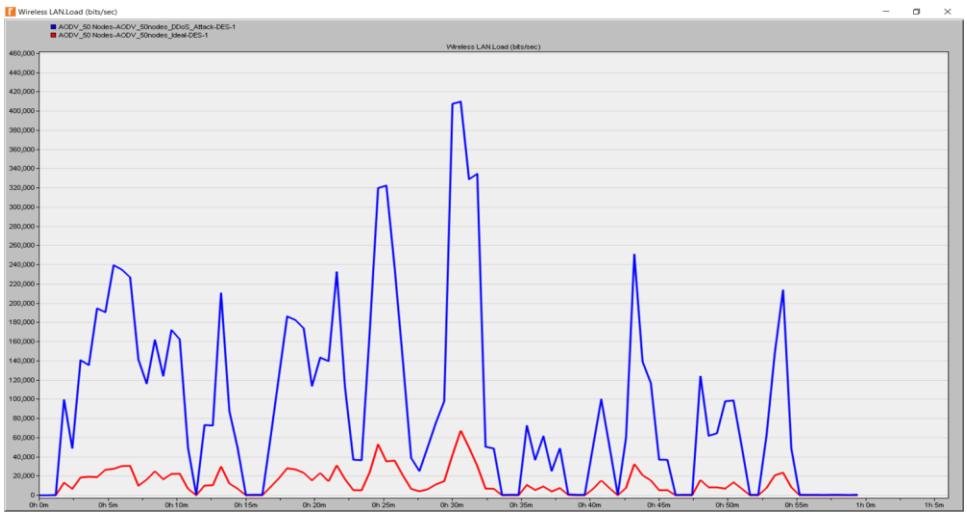


Figure 4.4.2(b): Wireless LAN – Load (bits/sec)

Here, Load on the network represents the total load (bits/sec) submitted to wireless LAN layers by all higher layers in all WLAN nodes. From the above graph, we have observed that the number of bits transferred each second because of DDoS attack is about 10 times more than the ideal network scenario. When there is high traffic load on the network because of DDoS attack, we can expect more packets drop. Figure 4.4.2(c) displays the packets dropped in the AODV network due to the high traffic load by attackers. The average packets dropped is around 150 packets per second.

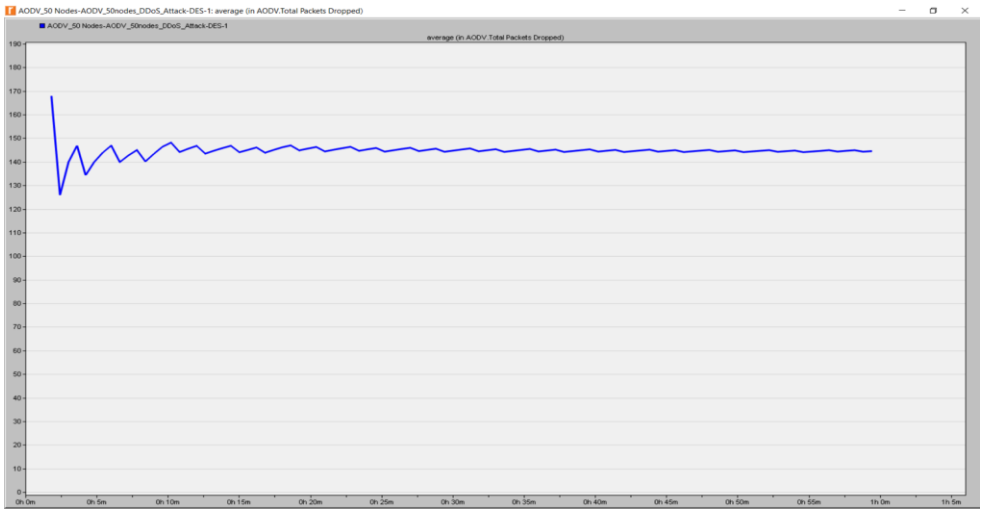


Figure 4.4.2(c): Total Packets Dropped in AODV

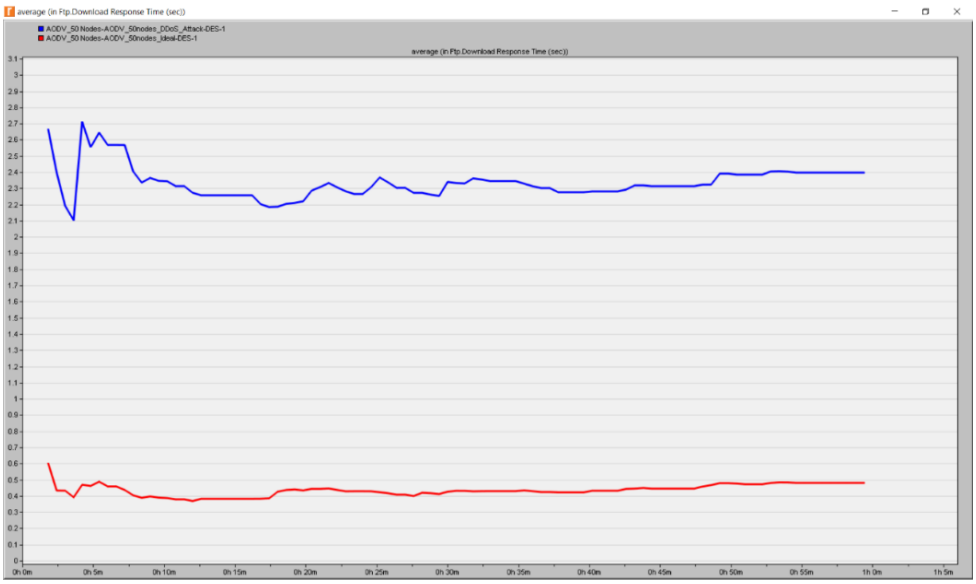


Figure 4.4.2(d): Avg. FTP Download Response Time (seconds)

From the above graph, we can deduce that the average FTP download response time (in seconds) because of DDoS attack has increased by more than 9 times compared to the ideal network.

4.5 50-Node DSR Network Scenario *(Scenario-03)*

4.5.1 Simulation Methodology

For the first phase, a 50-node wireless peer to peer network is implemented on DSR routing protocol. The nodes are organized in random manner and no specific topology is followed. All nodes in the network are configured to perform DSR and multiple FTP sessions. Moreover, WLAN data rate is 1Mbps, and simulation is performed for 1 hour. Figure 4.5.1(a) shows the design of the 50-node P2P network used with default parameters on DSR routing protocol.

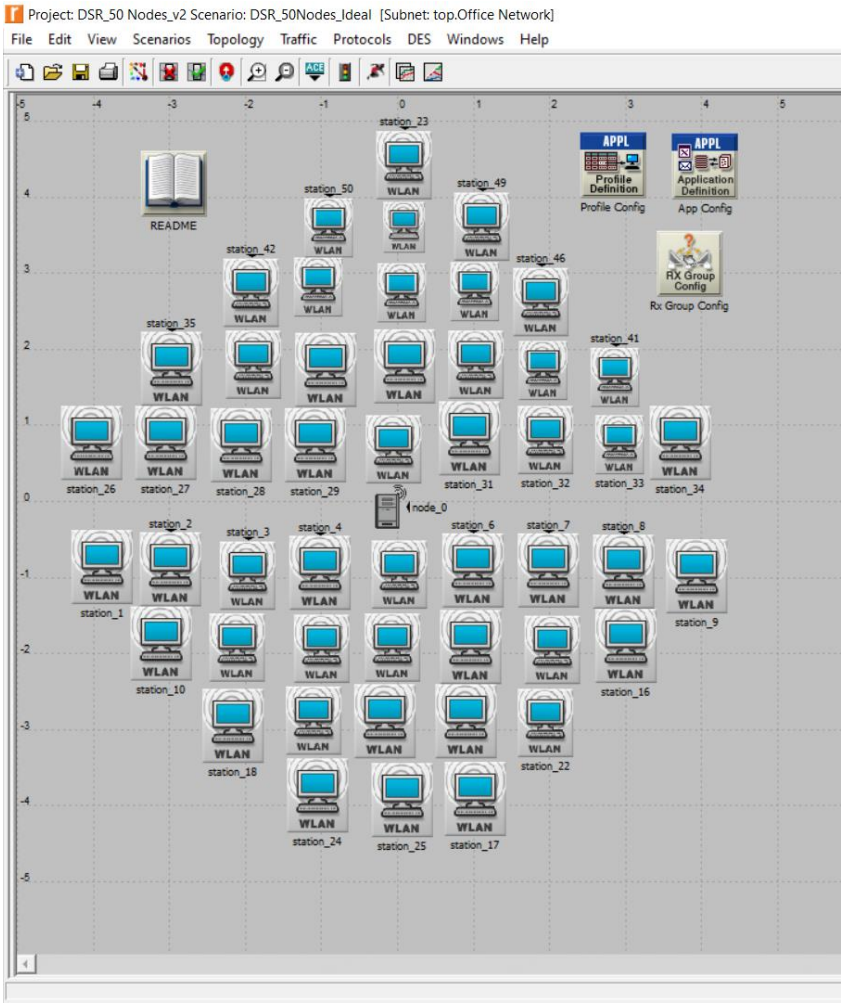


Figure 4.5.1(a): 50-Node DSR Network

For the second phase, a 50-node wireless P2P network is executed over DSR routing protocol with DDoS attack. All nodes in the network are configured to run DSR and multiple FTP sessions with high load. We have added 4 attackers in this network, and we have connected those attackers to the server via 'IP Ping Traffic Flow' mechanism. We have used 'IP Attribute' for implementing DDoS attack in the network. The important attribute is the 'Packet Size' and is set as 65527 bytes with an unlimited count [14]. So, attackers would be able to generate continuous traffic for server. Moreover, we have attached snapshots of different configurations (Figure 4.5.1(b), Figure 4.5.1(c), Figure 4.5.1(d)) in this section which we have followed for this simulation section.

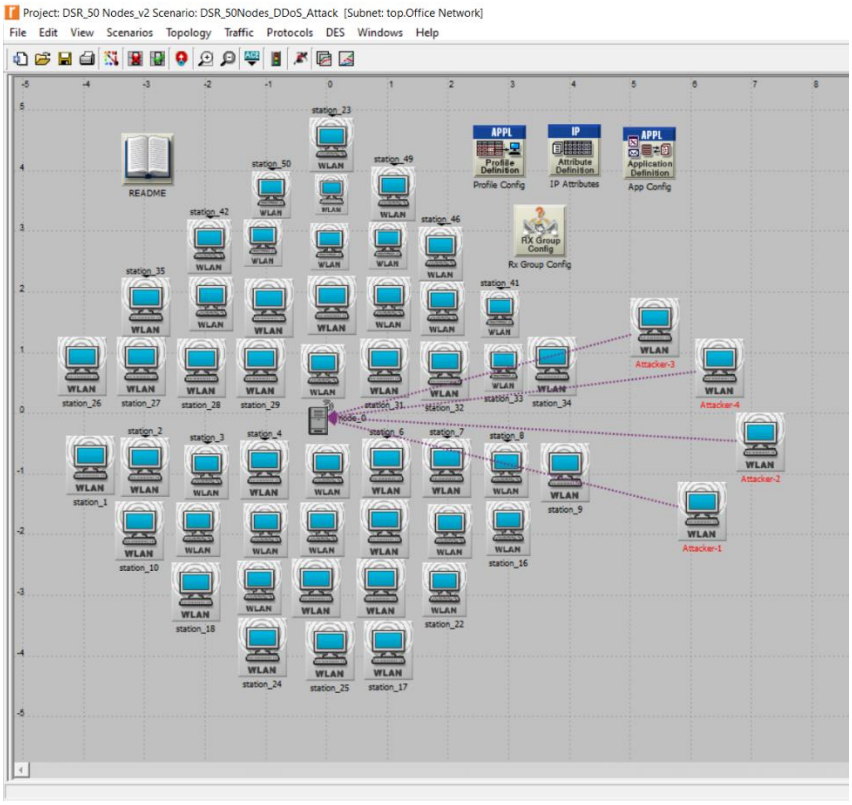


Figure 4.5.1(b): 50-Node DSR Network with DDoS Attack

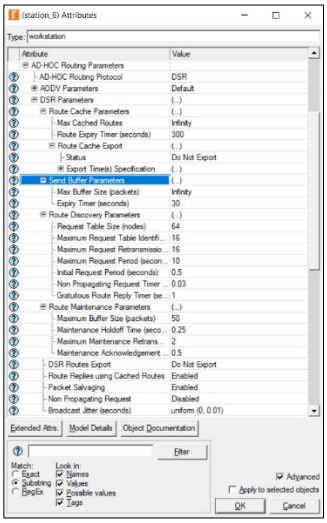


Figure 4.5.1(c)

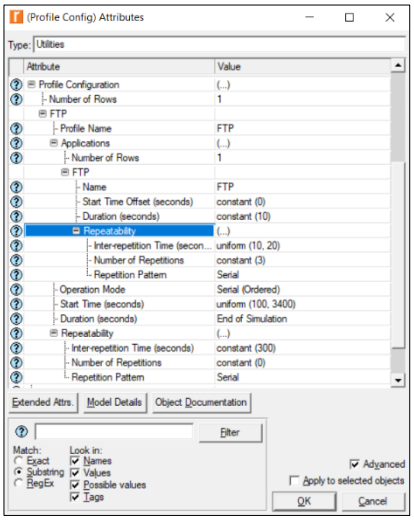


Figure 4.5.1(d)

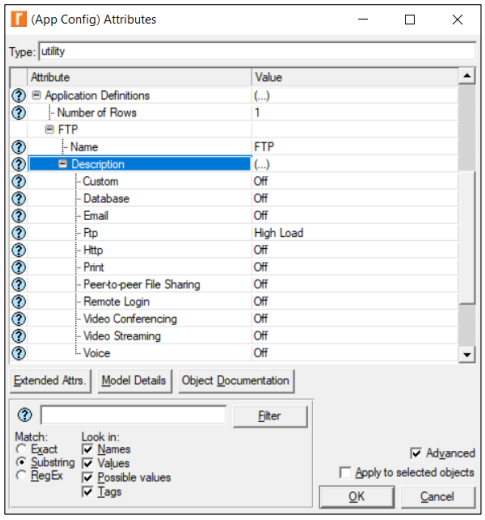


Figure 4.5.1(e)

Figure 4.5.1 (c): DSR Node Configuration; Figure 4.5.1 (d): Profile Configuration; 4.5.1(e): Application Configuration

4.5.2 Simulation Results

In this section, we have measured media access delay, the load on the network, total number of packets dropped, and average FTP download response time between ideal and DDoS attack scenarios for DSR routing protocol. We know that in the case of DDoS attack, the media access delay is increased by almost 12 times compared to the ideal scenario in DSR network. The Server with the DSR routing protocol fails after approximately 5.5 minutes due to high load from the attacking nodes.

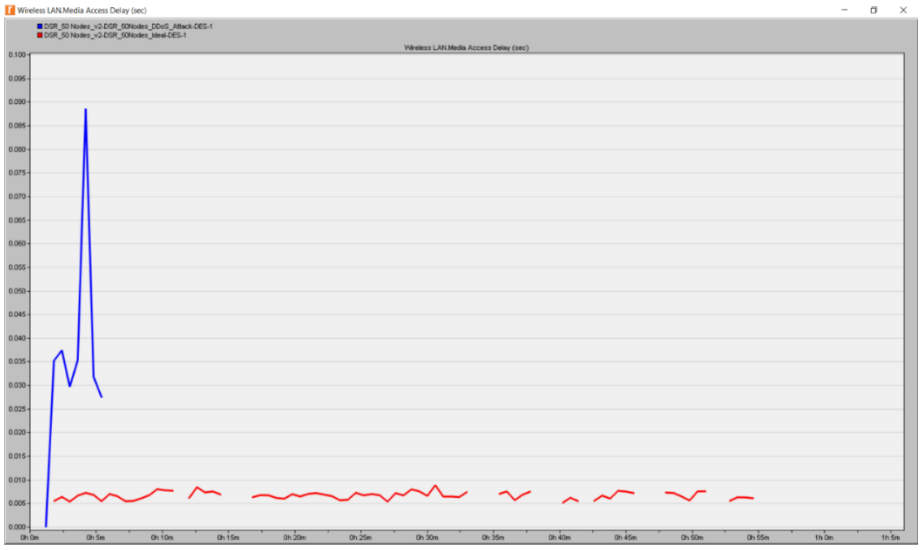


Figure 4.5.2(a): Media Access Delay (seconds) – DSR Network

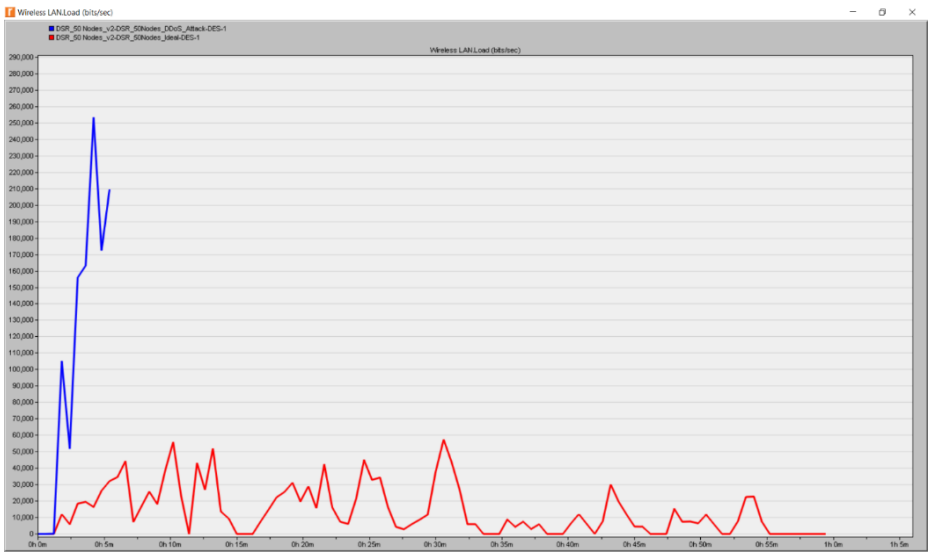


Figure 4.5.2(b): Load (bits/sec) – DSR Network

From the Figure 4.5.2(b), we can illustrate that the number of bits transferred each second because of DDoS attack is more than 10 times than the ideal network scenario. It means server of the network was getting tremendous amount of traffic or packets from those attackers. After 5.5 minutes of simulation, the server crashed by which it stopped carrying any traffic.

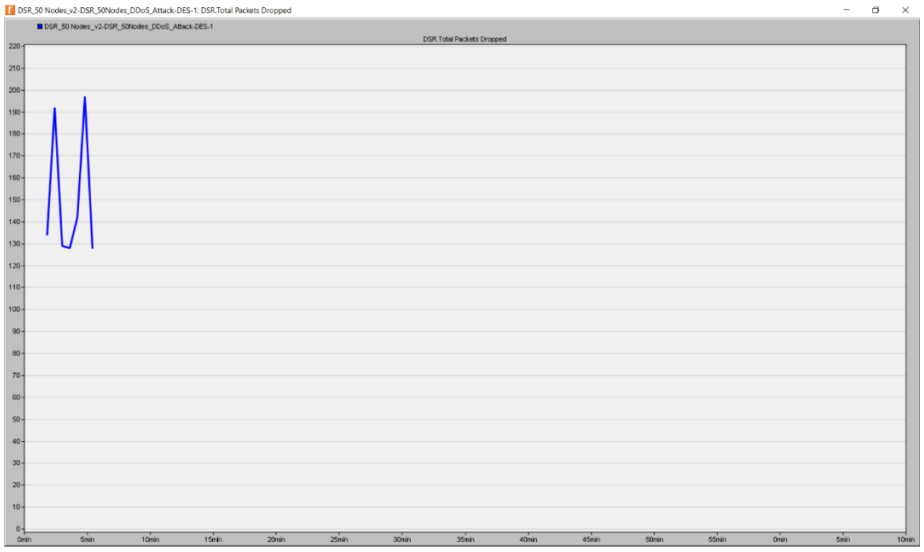


Figure 4.5.2(c): Total Packets Dropped in DSR

Figure 4.5.2(c) displays the packets dropped in the network due to the high load by the attacker, and we can say that there were not any packets dropped during the ideal scenario. The packets dropped reaches around 200 packets an instant, at one point of the simulation for DSR protocol.

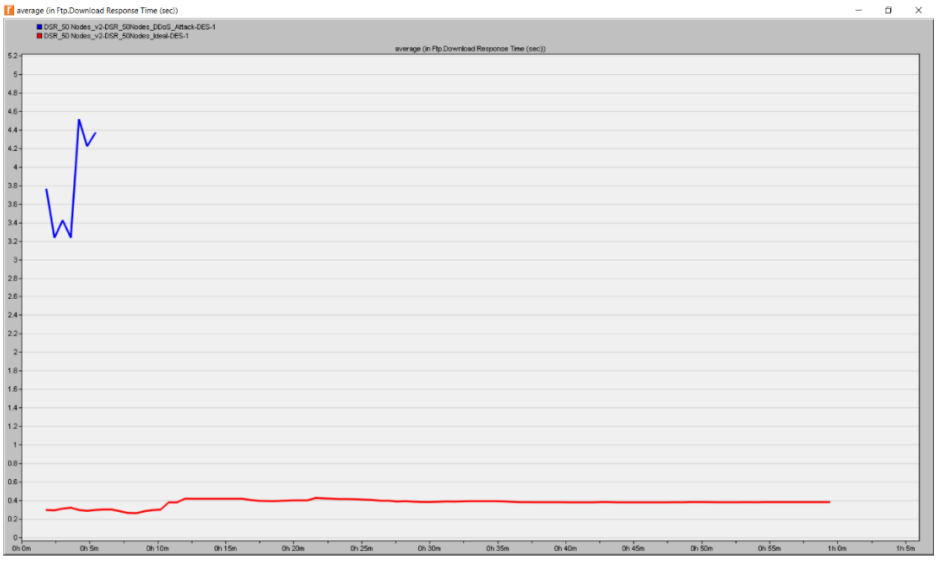


Figure 4.5.2(d): Average FTP Download Response Time in DSR

From the above graph, we can say that average FTP download response time (in seconds) due to DDoS attack has increased by around 14 times compared to the ideal scenario for DSR protocol.

4.6 50-Node TORA Network Scenario *(Scenario-04)*

4.6.1 Simulation Methodology

For the first phase, a 50-node wireless peer to peer network is implemented on TORA routing protocol. The nodes are organized in random style and no specific topology is followed. All nodes in the network are configured to perform TORA and multiple FTP sessions. Moreover, WLAN data rate is 1Mbps, and simulation is performed for 1 hour. Figure 4.6.1(a) shows the design of the 50-node P2P network used with default parameters on TORA routing protocol.

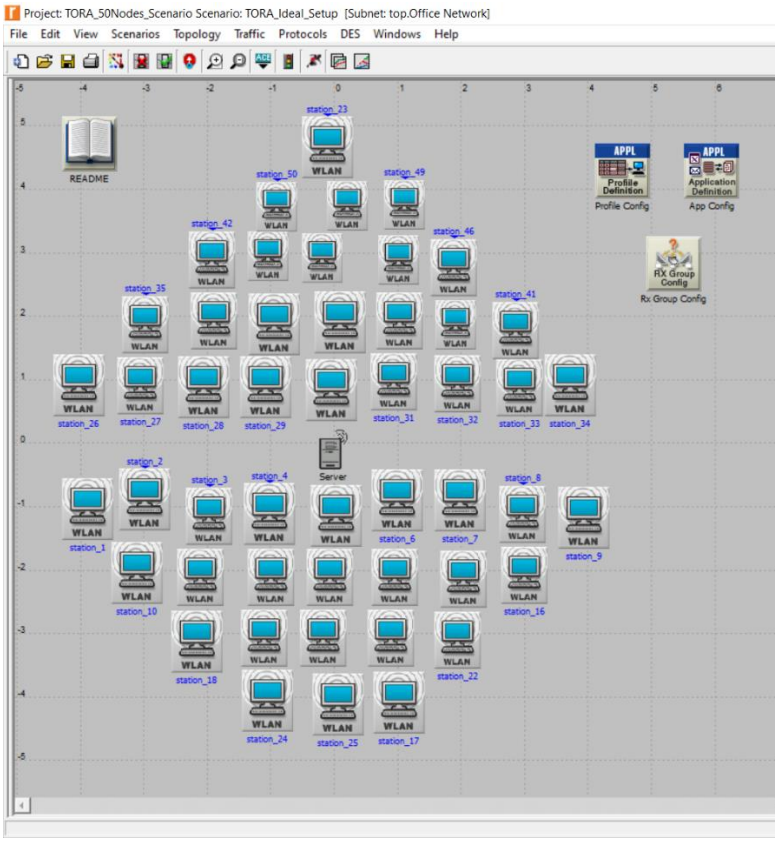


Figure 4.6.1(a): 50-Node TORA Network

For the second phase, a 50-node wireless P2P network is executed over TORA routing protocol with DDoS attack. All nodes in the network are configured to run TORA and multiple FTP sessions with high load. We have implemented 4 attackers for this network, and we have connected those attackers to the server via ‘IP Ping Traffic Flow’ link. We have used ‘IP Attribute’ for implementing DDoS attack in the network. The important attribute is the ‘Packet Size’ and is set

as 65527 bytes with an unlimited count [14]. Moreover, we have attached snapshots of different configurations (Figure 4.6.1(c), Figure 4.6.1(d)) in this section which I followed for the simulation.

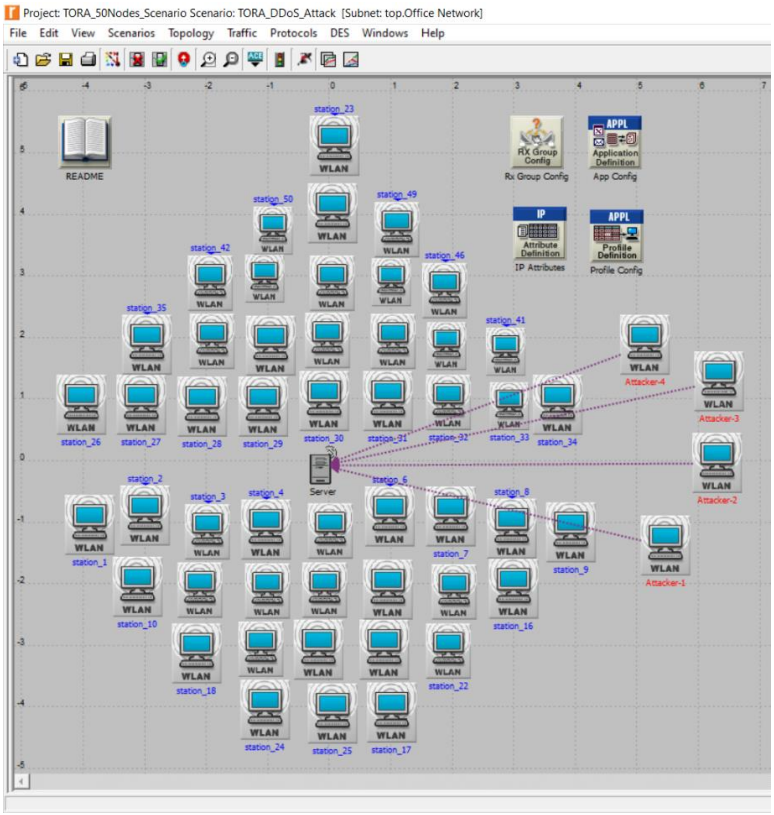
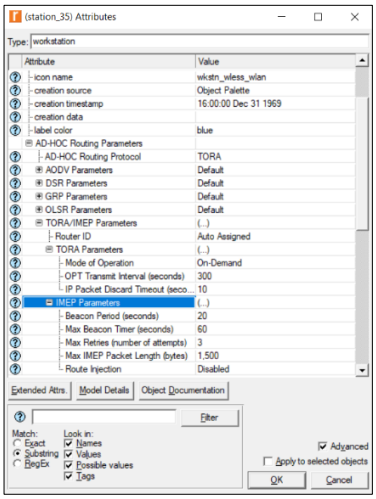


Figure 4.6.1(b): 50-Node TORA Network with DDoS Attack



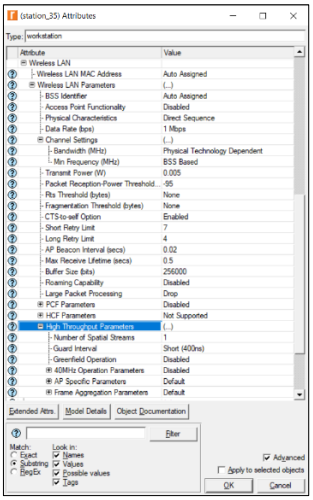


Figure 4.6.1(c) Figure 4.6.1(d)

Figure 4.6.1(c): TORA Configuration; Figure 4.6.1(d): WLAN Configuration

4.6.2 Simulation Results

In this section, we have analyzed media access delay, the load on the network, average IMEP dropped unroutable IP packets, and average FTP download response time between ideal and DDoS attack scenarios for TORA routing protocol. We know that in the case of DDoS attack, the media access delay is increased by 10 times compared to ideal scenario in TORA network.

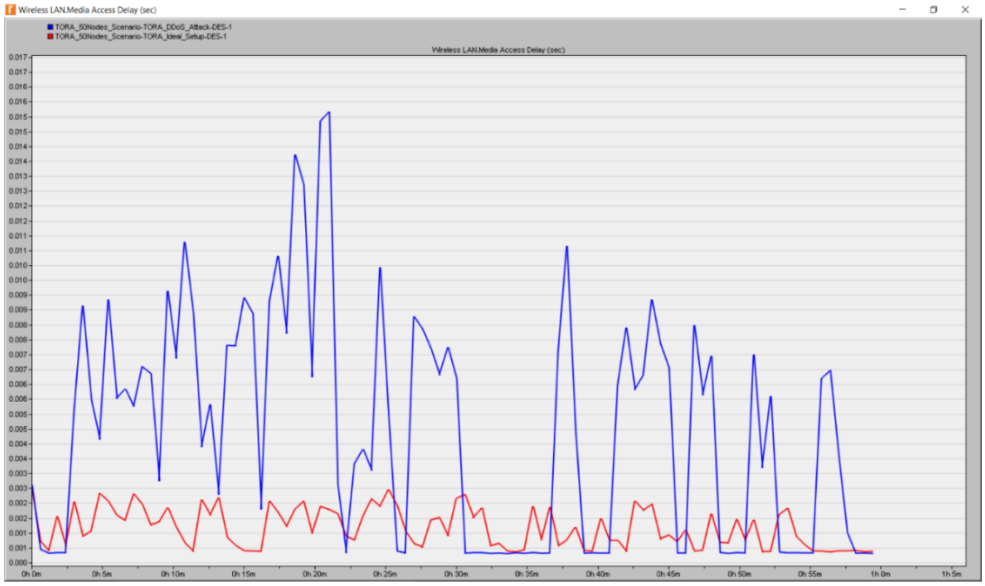


Figure 4.6.2(a): Media Access Delay (Seconds) – TORA Network

From the below graph, we can say that the network server is taking more load of packets due to DDoS attack, and it is highest about 12 times more compared to the ideal network at some point.

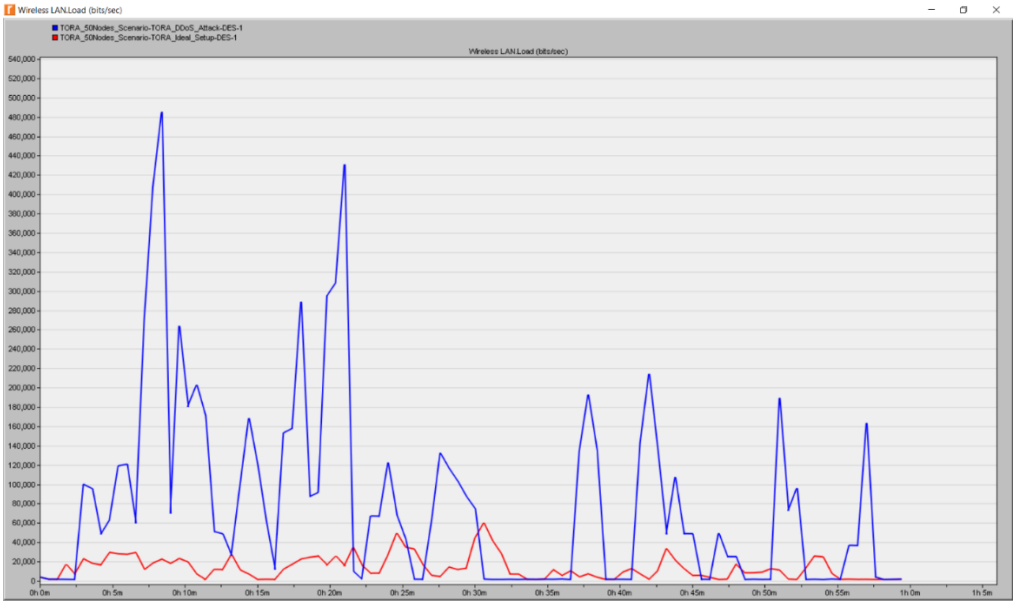


Figure 4.6.2(b): Load (bits/sec) – TORA Network

Figure 4.6.2(c) displays the IMEP dropped unroutable IP Packets in the network for TORA routing protocol. IMEP is known as Internet MANET Encapsulation Protocol.

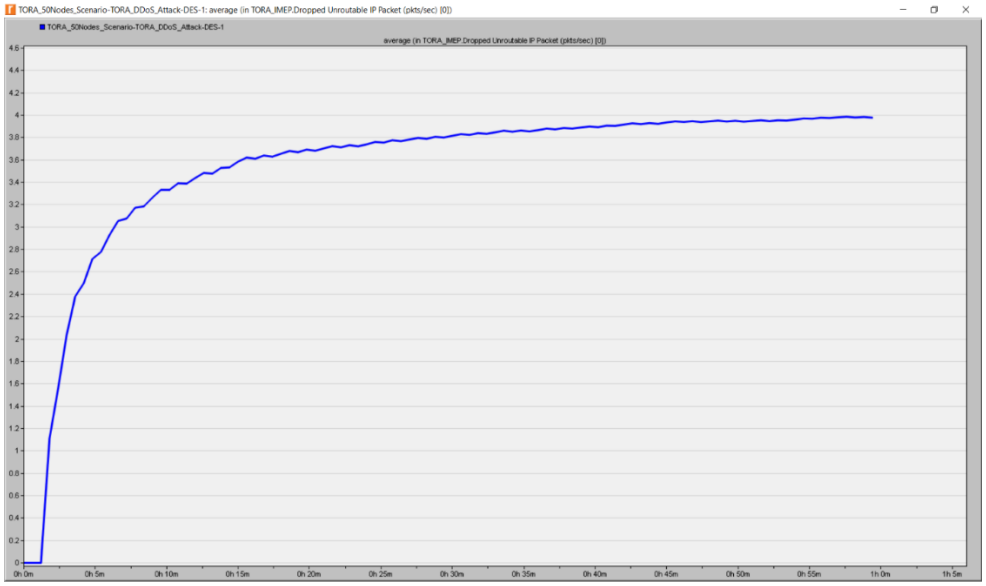


Figure 4.6.2(c): IMEP Dropped Unroutable IP Packets

From the below graph, we can say that average FTP download response time due to DDoS attack has raised by 13 times at some point of the simulation compared to the ideal scenario for TORA routing protocol. So, network server was taking longer time to process FTP download response.

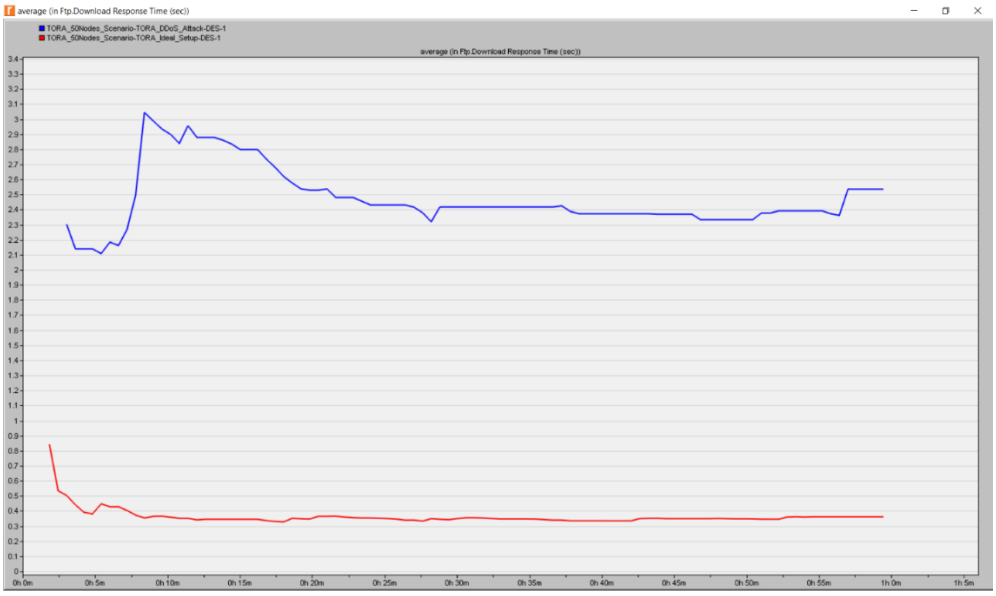


Figure 4.6.2(d): Avg. FTP Download Response Time (seconds)

4.7 Comparison between AODV, DSR, and TORA *(Scenario-05)*

4.7.1 Original Network (Ideal Scenario)

Our original network is a 50-node wireless peer to peer network, and which is implemented on AODV, DSR, and TORA routing protocols. We have followed similar network topology for all three protocols, and we have ensured all basic configurations of the network remain same. We have performed simulation for 1 hour and the simulation results for the ideal scenario are compared into a single graph between different routing protocols (e.g., AODV, DSR, TORA).

Figure 4.7.1(a) shows us the end-to-end delay performance for all three routing protocols (AODV, DSR, TORA) in an ideal condition of the network. This '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. So, AODV routing algorithm performed better than DSR & TORA.

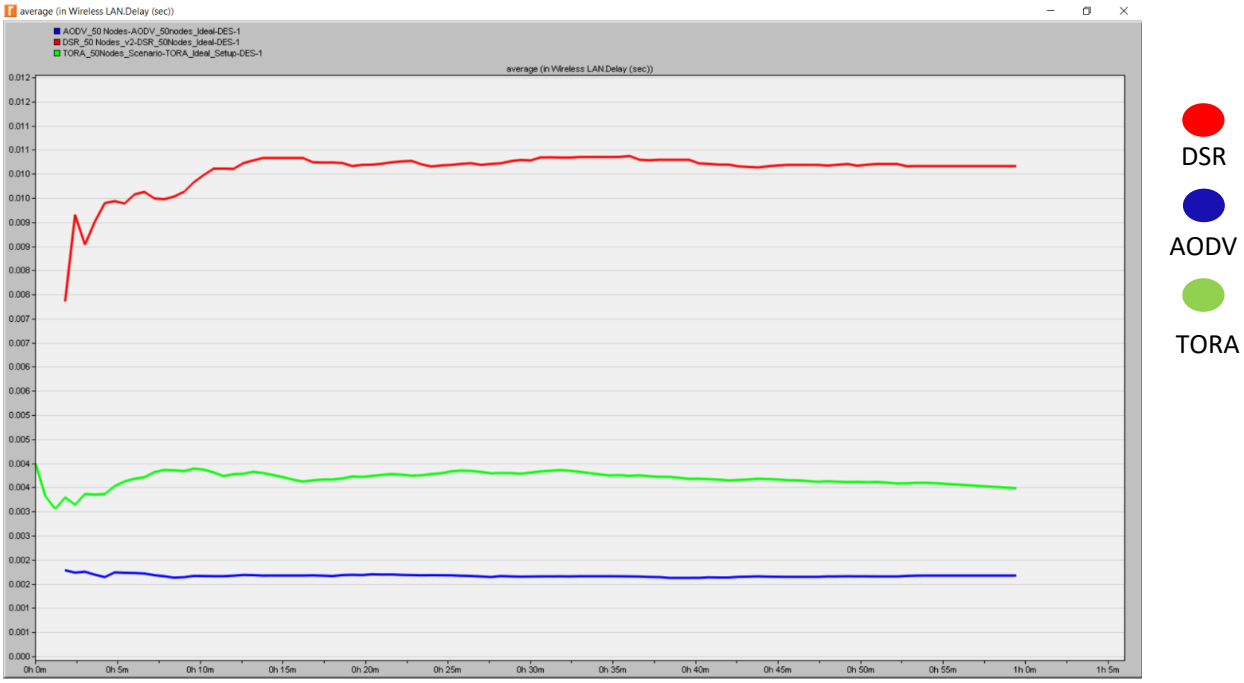


Figure 4.7.1(a): Avg. Wireless LAN - Delay (seconds)

Figure 4.7.1(b) shows us the throughput performance for all three routing protocols (AODV, DSR, TORA) in an ideal condition of the network. This 'throughput' represents the total number of bits forwarded from wireless LAN layers to higher layers in all WLAN nodes. So, AODV routing algorithm performed better than DSR, and TORA routing algorithms.

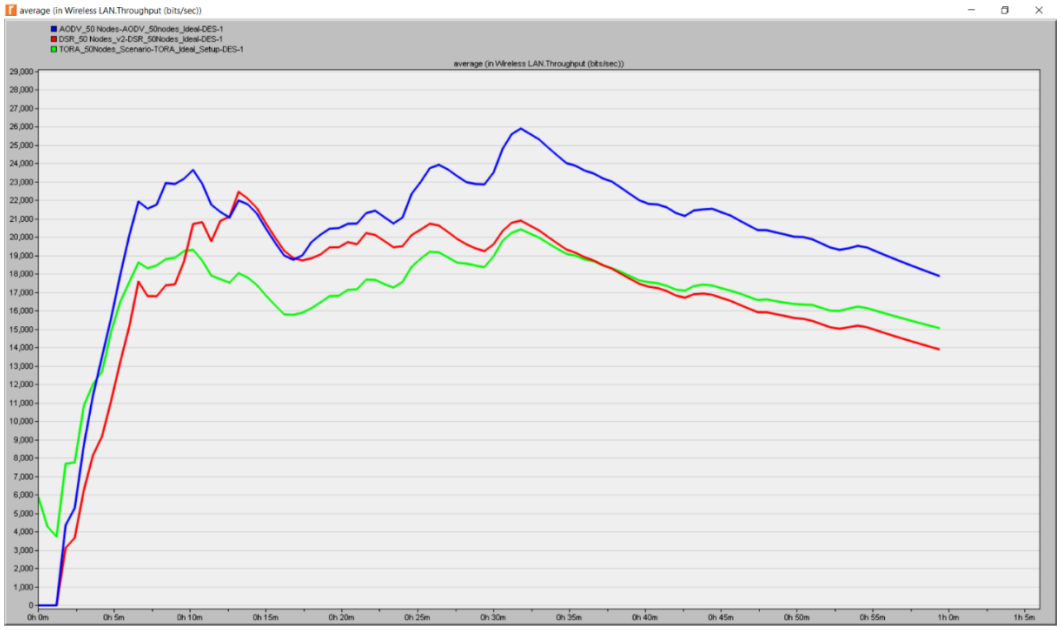


Figure 4.7.1(b): Avg. Wireless LAN - Throughput (bits/second)

4.7.2 DDoS Attack Scenario

We implemented DDoS attack scenario in a 50-node wireless P2P network, which is implemented on AODV, DSR, and TORA routing protocols. We have followed similar network topology for all three protocols, and we have ensured all basic configurations of the network remain same.

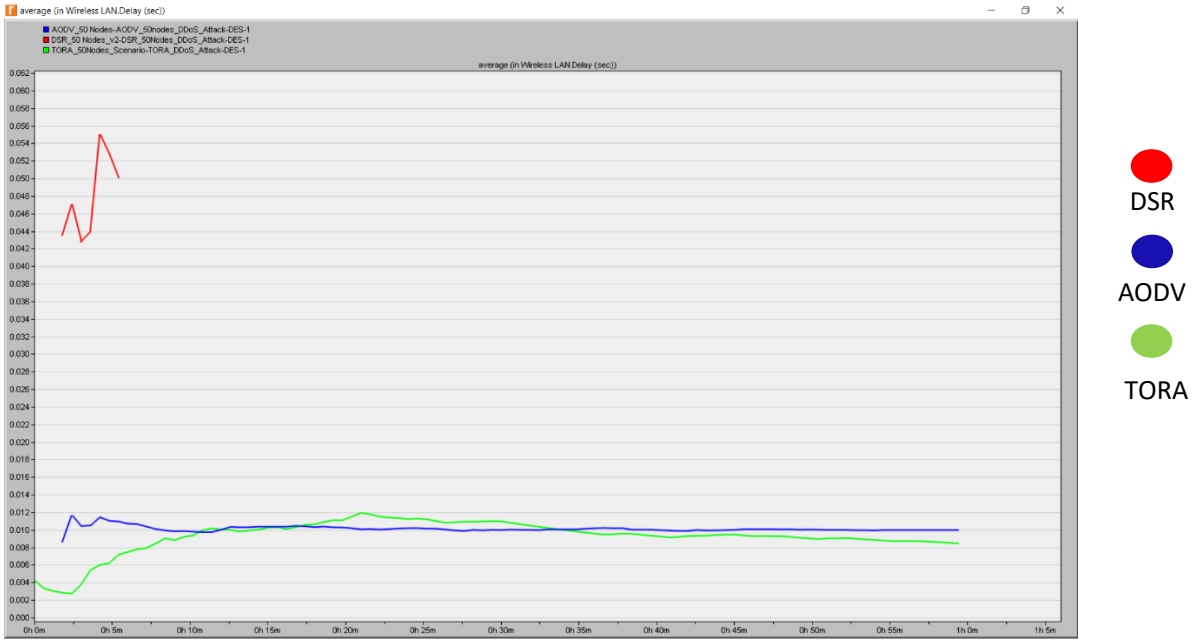


Figure 4.7.2(a): Avg. Wireless LAN - Delay (Seconds) - DDoS

We used 4 attacker nodes in our network, and IP Attribute for attackers remain same all over the network. We have performed simulation for 1 hour, and the simulation results for the DDoS attack

scenario are compared into a single graph between different routing protocols. Figure 4.7.2(a) shows us the end-to-end delay performance for all three routing protocols (AODV, DSR, TORA) in DDoS attack condition. Overall, AODV & TORA routing algorithms are performing better than DSR protocol.

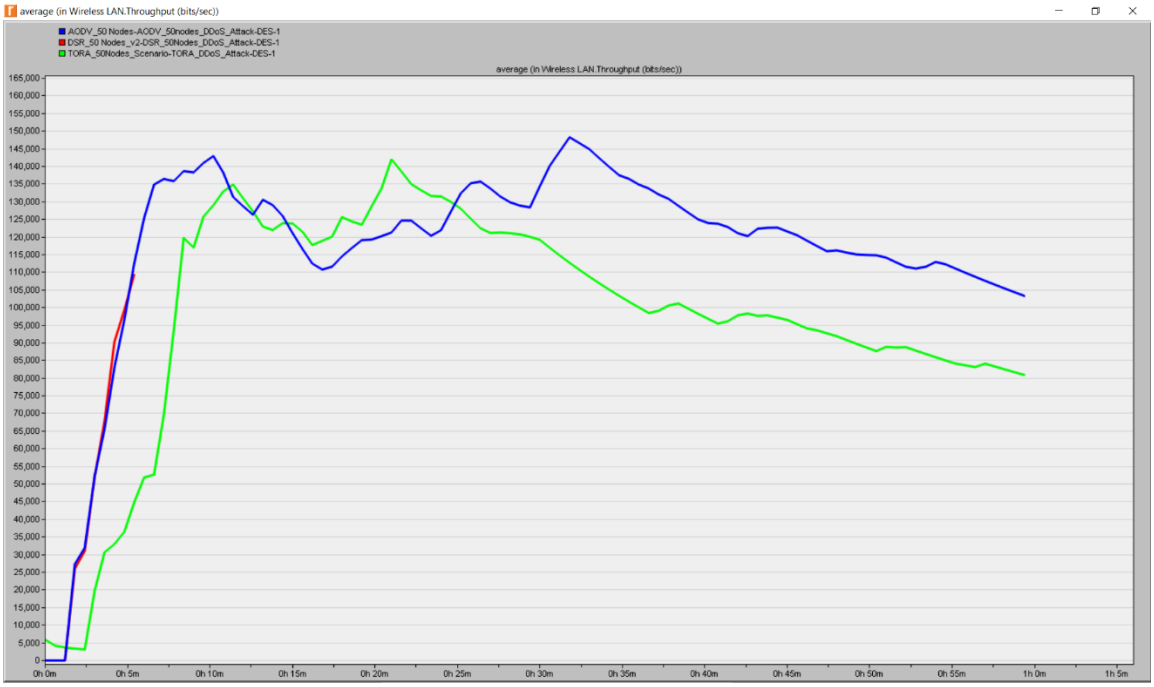


Figure 4.7.2(b): Avg. Wireless LAN - Throughput (bits/second) – DDoS

Figure 4.7.2(b) displays us the throughput performance for all three routing protocols (AODV, DSR, TORA) in a DDoS attack scenario. So, AODV fairly had better throughput than TORA over the whole simulation time. Moreover, DSR protocol network had similar throughput trend with AODV protocol network until DSR network is shutting down for DDoS attack.

4.8 Miscellaneous

We have used different routing algorithms for different network setup as well as performed multiple simulations under different attacks (such as Sybil & DDoS attacks). A couple of network simulations ran for 30 minutes. The remaining six network simulations ran for 1 hour. In the following table, we have included the simulated time for all these network simulations which we have performed in Riverbed Modeler 17.5 academic edition. After running these simulations in Riverbed Modeler, simulation execution window shows the ‘Elapsed Time (or Simulated Time)’.

Routing Algorithm	Scenario Type	Simulation Time	Elapsed Time (Simulated Time)
AODV: 20 Nodes	Ideal	30 Minutes	1 second
AODV: 20 Nodes	Sybil Attack	30 Minutes	1 second
AODV: 50 Nodes	Ideal	1 hour	1 second
AODV: 50 Nodes	DDoS Attack	1 hour	3 seconds
DSR: 50 Nodes	Ideal	1 hour	3 seconds
DSR: 50 Nodes	DDoS Attack	1 hour	1 second
TORA: 50 Nodes	Ideal	1 hour	3 seconds
TORA: 50 Nodes	DDoS Attack	1 hour	4 seconds

Table 4.8: Simulation Execution Time in Different Scenarios

Moreover, we have attached a couple of snapshots from simulation execution windows after running simulation for a couple of network topologies under TORA routing protocols.

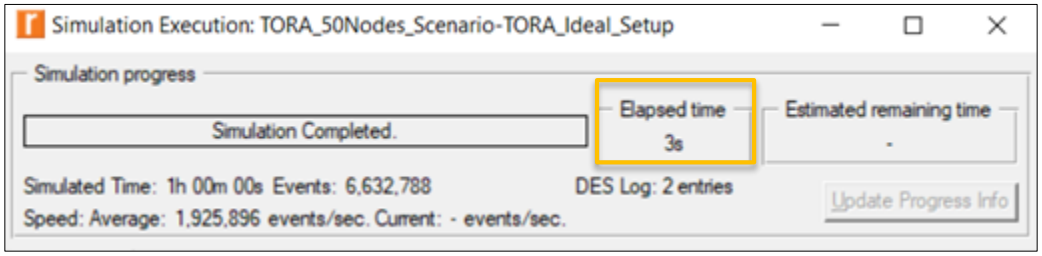


Figure 4.8(a): Simulation Execution Window – TORA Network

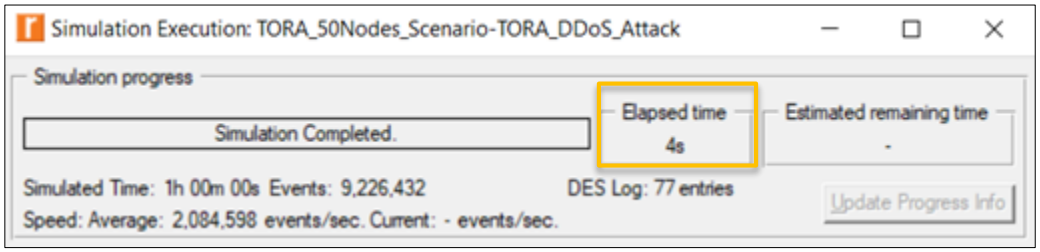


Figure 4.8(b): Simulation Execution Window – TORA DDoS Network

CHAPTER 5: DISCUSSION

5.1 Challenges and Limitations

The first challenge was to become familiar with the various functions of the Riverbed Modeler and then determine what type of attacks are possible to simulate using this software because the Academic Edition of the Riverbed Modeler has limited features. Initially it was difficult to understand how to implement the Sybil attack and the DDoS attack. Due to limited time and bindings in the software it was not possible to develop attack scenarios from scratch in different routing protocols without using the example scenarios.

5.2 Future Works

There are several extension opportunities for the project. Firstly, network infrastructure can be changed and attack scenarios can be simulated with increased number of nodes and different configurations can be tested. Mobility concept can be introduced into the nodes and the effect on the performance can be observed. Furthermore, implementation process can be changed such as using additional routing algorithms with existing or new network setup. In addition, different types of attacks such as wormhole attack can be simulated with detection and prevention functions.

CHAPTER 6: CONCLUSION

Though simplicity, portability, and infrastructure less operability of ad hoc networks is enabling it to gain popularity in various sectors, its security is not yet out of question as ad hoc networks are still prone to various types of attacks and no routing protocol is fully sufficient to counter all sorts of attacks [16]. We have implemented several scenarios in Riverbed Modeler to assess vulnerability of mobile ad hoc networks. Firstly, we used AODV routing protocol in ideal and Sybil attack scenario and observed the effect on traffic flow. In this case the total traffic was routed to the Sybil node bypassing the actual destination. Then 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, and TORA routing protocols are performing much better than DSR routing protocol when executing DDoS attack. Though both the DSR & TORA routing algorithms were designed for multi-hop wireless networks, but TORA network performed better than DSR because it can efficiently reroute the traffic if there is any link failure. Overall, it is found that AODV is the best routing protocol as it can perform well in high mobility and high traffic communication network.

After completion of this project, we have obtained valuable knowledge about various routing protocols and attack scenarios in MANET. In addition, we compared the performance among the routing protocols used in the project. Most importantly we have developed practical insights on the vulnerability of mobile ad hoc networks through the simulation environment in the Riverbed modeler and relevant studies associated with the project.

REFERENCES

[1] R. Redy, “A brief overview of ad hoc networks: Challenges and directions,” IEEE Communications Magazine, 25-May-2014.

[2] What is ad-hoc network? (n.d.). Retrieved April 15, 2022, from https://www.tutorialspoint.com/what-is-ad-hoc-network

[3] Srinivasan, Aaditya Vasan, “Simulation and Analysis of Sybil attack in MANET”,pp. 1, 2018, https://sfunet.wixsite.com/ensc835

[4] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks in mobile ad hoc networks," *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2012, pp. 1-6, doi: 10.1109/CCECE.2012.6335025.

[5] E. Fazeldehkordi, I. S. Amiri, O. A. Akanbi, and M. Neely, *A study of Black Hole Attack Solutions: On AODV routing protocol in Manet*. Waltham, MA: Elsevier, 2016. https://doi.org/10.1016/C2015-0-04114-4

[6] Yingying Chen, Jie Yang, Chapter 8 - Defending Against Identity-Based Attacks in Wireless Networks,Editor(s): Sajal K. Das, Krishna Kant, Nan Zhang,Handbook on Securing Cyber-Physical Critical Infrastructure, Morgan Kaufmann, pp 191-222, 2012.

[7] Rashmi V. Deshmukh, Kailas K. Devadkar, Understanding DDoS Attack & its Effect in Cloud Environment, Procedia Computer Science, Volume 49, pp. 202-210, 2015.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] P. M. Rao, Y. C. Rao and M. A. Kumar, "Performance analysis of ZigBee wireless sensor networks using Riverbed simulation modeler," *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018, pp. 1272-1277, doi: 10.1109/ICISC.2018.8399010.

[14] F. Yihunie, E. Abdelfattah and A. Odeh, "Analysis of ping of death DoS and DDoS attacks," *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2018, pp. 1-4, doi: 10.1109/LISAT.2018.8378010.

[15] A. V. Srinivasan, “Simulation and Analysis of Sybil attack in MANET,” *ensc835*, 15-Apr-2018. [Online]. Available: https://sfunet.wixsite.com/ensc835. [Accessed: 16-Apr-2022].

[16] B. Banerjee and S. Neogy, "A brief overview of security attacks and protocols in MANET," *2021 IEEE 18th India Council International Conference (INDICON)*, 2021, pp. 1-6, doi: 10.1109/INDICON52576.2021.9691554.