ENSC 835: COMMUNICATION NETWORKS

SPRING 2018

Final Project

Simulation and Analysis of Sybil attack in MANET

https://sfunet.wixsite.com/ensc835

Team - 4

Name: Srinivasan, Aaditya Vasan

SFU ID: asriniva

Email ID: asriniva@sfu.ca

Abstract

The evolution of Wireless networks has brought together a number of benefits in areas such as health, defense, education, etc. A type of Ad hoc network, MANET is a wireless connection of mobile devices, where each device in the network functions independently, resulting in a dynamic topology. With the absence of an infrastructure, MANETs are prone to several cyber-attack methods, compromising the security of the nodes within the network.

This paper focuses on one such attack. Sybil attack is one of the serious threats when it comes to Wireless networks, where the attacker claims multiple identities gaining a large influence in the peer-to-peer network. The victim's data comes at risk and the network's communication can be disrupted. In this project simulation we will implement the Sybil attack on Mobile Ad hoc Networks and study the effects, using the Riverbed Modeler Academic Edition 17.5.

Keywords: Security, Wireless Networks, Sybil, Peer-to-Peer.

Acknowledgements

I would like to thank the people without whom this project would not have been possible. I extend my gratitude to Dr. Ljiljana Trajkovic, our course instructor, for her guidance throught the term and support during the project, and to the TA, Zhida Li for his help with initial stages of the project.

Aaditya Vasan Srinivasan

Table of Contents

List of Figures

List of Acronyms

IEEE	Institute of Electrical and Electronics Engineers
MANET	Mobile Ad Hoc Network
P2P	Peer-to-Peer
QoS	Quality of Service
AODV	Ad hoc On Demand Vector
DSR	Dynamic Source Routing
TORA	Temporally Ordered Routing Algorithm
IMEP	Internet MANET Encapsulation Protocol
RREQ	Route Request
RREP	Route Reply
RRER	Route Error
DSDV	Destination-Sequenced Distance-Vector Routing
OLSR	Optimized Link State Routing Protocol
CGSR	Cluster Switch Gateway Routing
WRP	Wireless Routing Protocol
ACOR	Admission Control Enabled On-Demand Routing
ABR	Associativity Based Routing
ZRP	Zone Routing Protocol
IP	Internet Protocol
FTP	File Transfer Protocol

Chapter 1.

Introduction

The earliest development of wireless networks was made under ALOHAnet at University of Hawaii in late 1960s, although commercial wireless networks weren't used until 1986. Over three decades into the future now, Wireless networks have advanced to a great extent, and into several types. The advancement in the wireless communication technology has brought forth different types of wireless links such as Communication satellites, terrestrial microwave, free space optical communication, etc. Based on the infrastructure of the network, wireless networks are classified into multiple types. Wireless ad hoc network also known as Mobile Ad hoc Network(MANET) is one such network where the communication between the links is handled by the independent nodes that forms the network. Ad hoc networks are "*on demand*" networks, which means communications in the ad hoc networks are made spontaneously where there is no predefined infrastructure between the nodes. The ad hoc networks make this possible with the use of several network layer routing protocols namely, Associativity based routing, ad-hoc on-demand distance vector routing, and dynamic vector routing, etc. In the Mobile Ad hoc Network, the nodes are not stationary, and this mobility of the nodes provides significant improvements and advantages over a network with an infrastructure. In the case of a cellular network, base station failure results in the drop in the coverage, but in the case of MANETs, such single point of failure is significantly reduced since the data in an Ad hoc network can be transferred through multiple paths, on demand. This characteristic of MANET makes it prone to several security vulnerabilities.

This paper focuses on explaining the vulnerability due to one such attack called *sybil* and its effects on the ad hoc nodes through simulation in Riverbed Modeler. Routing protocols such as Ad-hoc On demand Vector, Dynamic Source Routing, and Temporally Ordered Routing algorithm are used for simulation in two different network models, more of which are discussed in the later chapters of the paper.

Chapter 2.

Literature Review

The Ad hoc networks due to the lack of permanent infrastructure between the nodes, depend on a peer-to-peer model for communication. Since any node can initiate the communication in a P2P network, security is a huge concern when it comes to the protection of the nodes from the attacker. The attacker can take advantage of the lack of establishment and initiate an attack that compromises the data sent in the network and in many cases to the network itself. But before getting into the types of attacks MANETs are vulnerable to, we must look at the underlying principle that MANETs operate in.

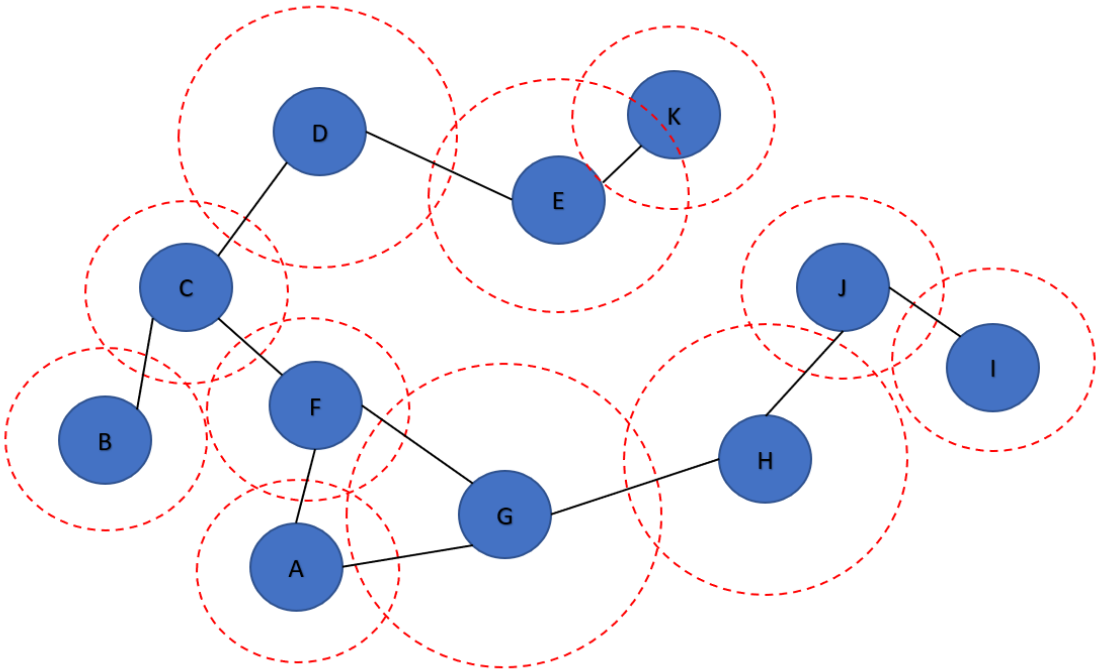

Figure 2(a): Ad hoc Network Scenario-1

In the Mobile Ad hoc networks, each node operates independently with mobility. Considering the figure 2(a), based on the signal strength, each node can communicate with other nodes in the network to form all possible links. The routing protocol decides which link to choose at the time of data transfer, based on parameters such as cost of the link or

the shortest path to destination. If node A has data that it wants to transfer to node K, it can either take path, based on routing protocol from A→F→C→D→E→K or A→G→F→C→D→E→K.

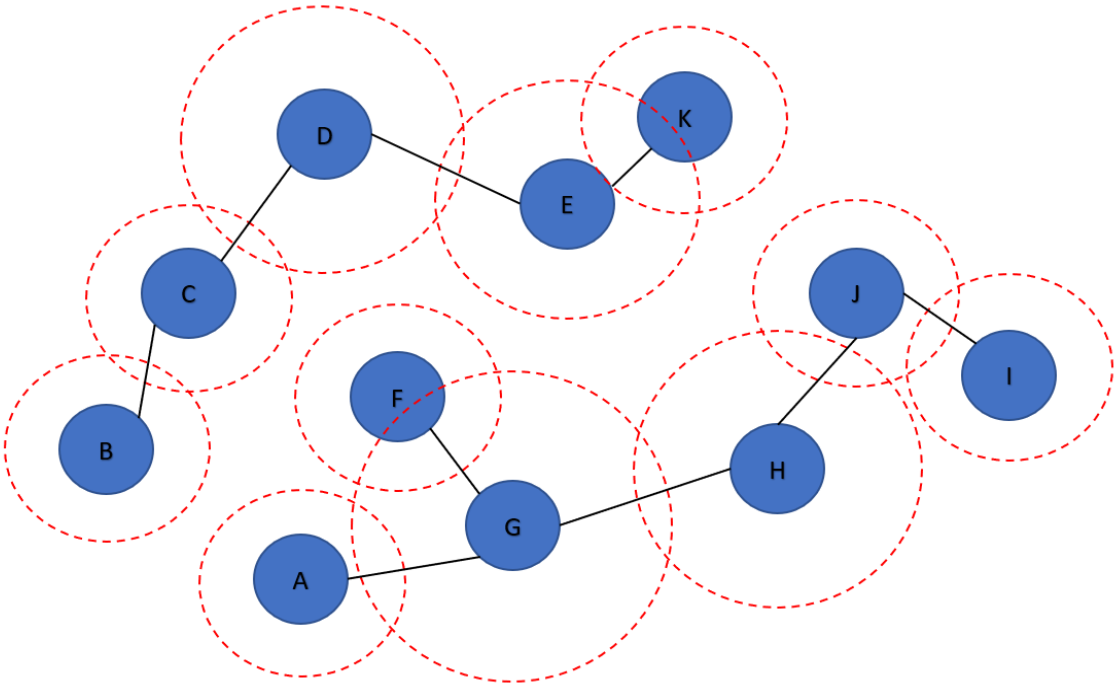

Figure 2(b): Ad hoc Network Scenario-2

Since the nodes are mobile, consider the case where a node leaves the network like in figure 2(b), which is possible in real life, like in the case where you lose reception when you leave the coverage area of the nearest transmission point. In this case of Mobile Ad hoc network, the link is broken and communication is not possible from node A to node K. This is one disadvantage of a network with no infrastructure as a secure stationary communication link is absent between the nodes.

2.1 Classification of Major Attacks

As mentioned earlier, P2P networks like MANETs are prone to security vulnerabilities based on their hop-by-hop communication method. Since there are no constrains for a node to join a network, the attacker has no restriction. We try to provide a brief background on

the major types of attacks in the Ad hoc Networks. Based on the target, lets classify the attack into two types, Data attack and Control attack [1], targeting the data plane and control plane respectively.

2.1.1 Data Attack

The data attacks focus on intercepting the data that is on route to the destination. The attacker can get hold of sensitive information or simply drop all or some of the packets disrupting communication.

Black-hole attack

This is one of the most damaging attack that focuses the data plane. The attacker through a malicious node intercepts the communication and drops all the packets like a black hole. Another version of the attack exists where more than one malicious node takes part in the attack, which is classified as cooperative black-hole attack.

Jellyfish attack

Unlike the black-hole attack, in this attack, the attacker drops some packets rather than all of them. In addition to dropping the packets, the attacker can choose to re order them when routing it to the destination, disrupting the data flow and QoS.

2.1.2 Control Attack

Unlike the attacks that occur in the data plane, the control plane attacks are far more dangerous because not only the communication is disrupted, but the attacker has no intention of blindly dropping packets. Instead the attacker can choose to sniff the packets for sensitive information thus making the data confidentiality obsolete. Only some of the most damaging attacks are mentioned in the paper.

Wormhole attack

Like its cosmological definition, two distance points are connected by a short route, one or more malicious nodes can participate in the network and intercept data sent to the destination, without disrupting the order of the packets.

Man in middle attack

In this attack, the attacker becomes part of the network to sniffs packet flowing through the network. This attack can be damaging if multiple malicious nodes takes part in the attack.

Blackmailing attack

In the blackmailing attack, the malicious node(s) takes identity as innocent nodes, accusing a honest node as harmful, or by advertising high cost for certain nodes. Blackmailing attack can be devastating if multiple nodes take part in the attack which counters even more secure protocols involved.

Sybil attack

When the local network has no physical background on the remote network, it looks at the informational abstractions. In this attack, the attacker assumes multiple identities to gain influence in the network thereby eliminating redundancy. By this way, the nodes in the established network can vouch for the other nodes. With the absence of an authority for identity, the sybil nodes can generate a chain of trust with the malicious nodes thereby compromising all identities. The dangerousness of the attack comes from the efficient low cost of implementing this attack through certification software in the market. The remainder of the paper focuses on Sybil attack and its effects in an Ad hoc network.

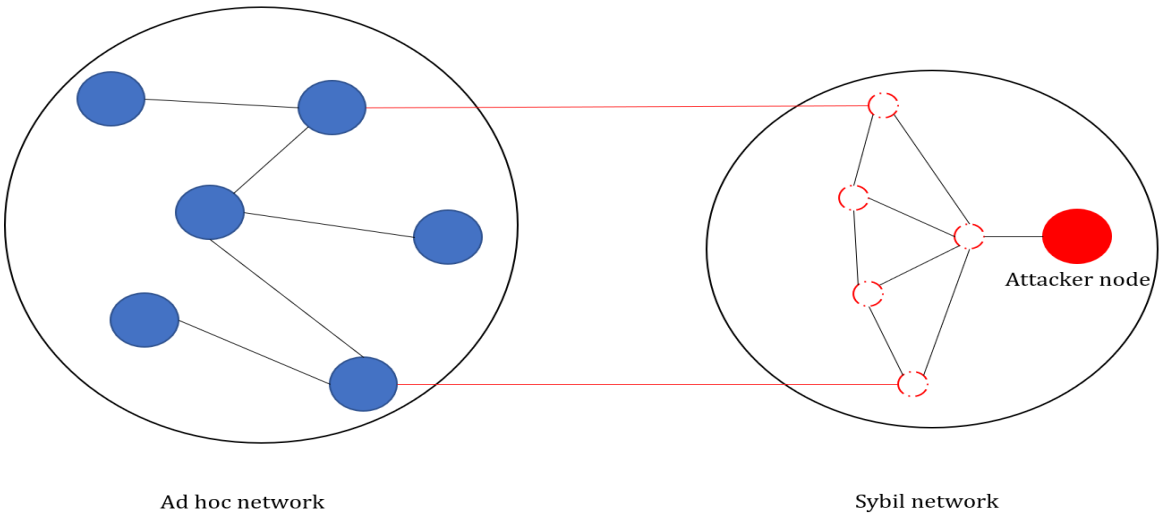

Figure 2.1.2: Sybil attack representation

The figure 2.1.2 represents the attacker posing with the identity of 5 nodes, establishing connection with the Ad hoc network containing the actual nodes.

2.2 Routing Protocols in Mobile Ad hoc Networks

The Wireless Ad hoc Networks being an infrastructure less network, relies primarily on routing algorithms for efficient transfer of packets from peer to peer on an Ad hoc basis. Although there are several efficient routing protocols in use, only 3 widely used protocols are used in the simulation scenarios that follows.

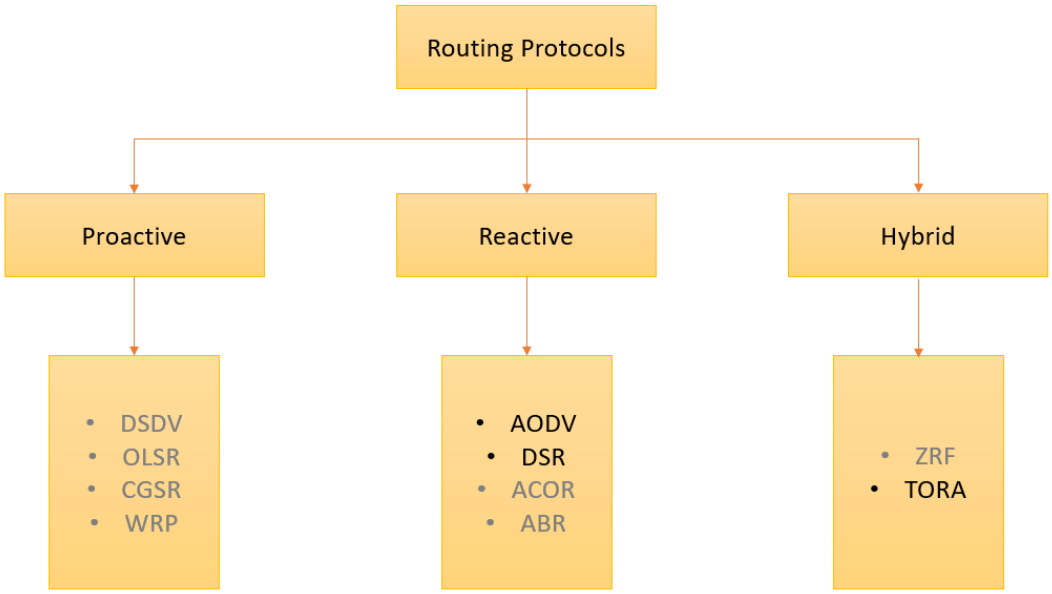

Figure 2.2: Routing Protocol Classification

2.2.1 Ad hoc On demand Vector

The routing protocols in MANET can be classified into 3 types, *reactive*, *proactive* and *hybrid*. AODV routing algorithm falls under the reactive category. This means the route construction happens on demand reducing the routing load. It uses sequence numbers for routing packets to destination nodes and holds the information in routing tables [2]. AODV has three message types. Route Requests(RREQs), Route Replies(RREPs) and Route Errors(RRERs).

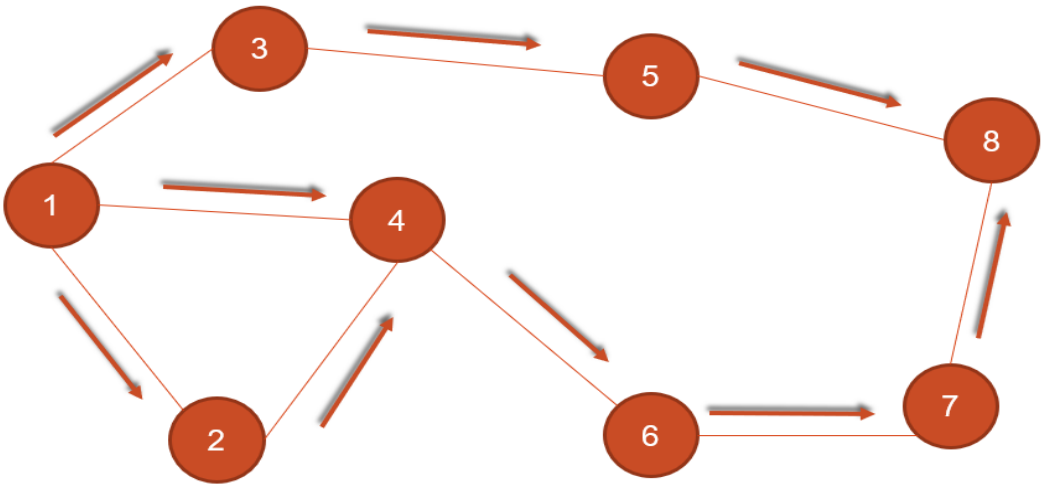

Figure 2.2.1(a): RREQ broadcast

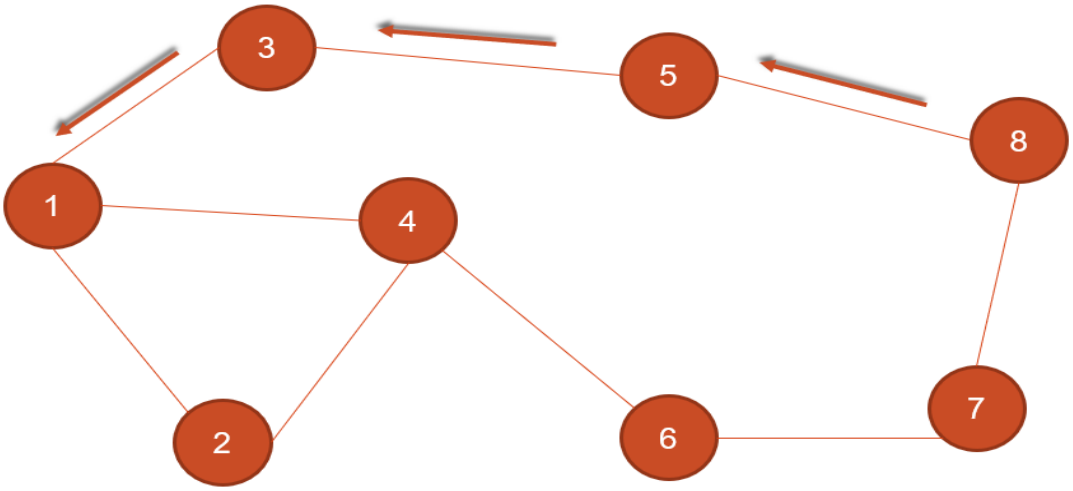

Figure 2.2.1(b): RREP reply path

The source initially floods the network with RREQs, with the route made possible by unicast RREP sent back to the source. RRER comes into action when the destination nodes are no longer reachable or by a broken link. Figures 2.2.1(a) & 2.2.1(b) shows the RREQ and RREP message propagation in the network.

2.2.2 Dynamic Source Routing

Dynamic Source Routing is another reactive routing protocol which uses the concept of *source routing* where each packet carries the complete source to destination route in its header. DSR is designed especially for multi hop wireless ad hoc networks containing mobile nodes. DSR allows multiple routes to destination. Unlike AODV, DSR does not use any periodic routing messages. DSR functions through two mechanisms namely, *Route Discovery* and *Route Maintenance* [3]. Route Discovery is used when source attempts to send a packet to the destination, with the route to the destination, unknown. Route maintenance kicks in when the source is able to detect the route to the destination is no longer valid, while using that route.

2.2.3 Temporally Ordered Routing Algorithm

TORA algorithm falls under the third category, *hybrid* protocol. TORA is efficient in highly dynamic, multi-hop mobile networks. One of the biggest advantages of TORA is its adaptivity in repairing routes during link failures and prepare multiple routes to destination. TORA algorithm provides three mechanisms, route creation, route maintenance and route erasure, all through Internet MANET Encapsulation Protocol(IMEP). The three mechanisms are as the name suggests and fairly self-explanatory. Since TORA always has multiple routes to the destination, it does not always favor the shortest path to the destination.

Chapter 3.

Related Work

The simulation of the security attacks in various wireless networks and wired ones have been done using different tools. Since Sybil attack has not been done as a published journal or research, for this project, simulation and other types of attacks have been referred for basic understanding of the work. Three such online materials including IEEE research paper and tutorial websites were very helpful for the project.

- A survey on the different types of security attacks possible in Mobile Ad hoc networks [1].
  This paper gives a general idea on all the security vulnerabilities in Mobile Ad hoc Networks. In addition to the discussion on the various attacks, the authors of the paper provide with techniques on how to mitigate the effects of each attack. By reading this paper, it was helpful in identifying and understanding which attacks to simulate for the project work.

- Analyzing performance affected by Sybil and wormhole attack in Mobile Ad hoc Networks with AODV routing algorithm [4].
  This IEEE paper deals with the simulation of sybil and Wormhole attack in AODV routing. Although this paper is very short in length and doesn't go through any details of the experiment, the discussion on simulation results were helpful in choosing the network architecture such as number of nodes, and statistics to record for the project work.

- Simulation of network intrusion using OPNET modeler [5].
  Since not many network intrusion simulations have been done using riverbed modeler aka OPNET modeler, this tutorial which deals with a network intrusion simulation in the OPNET modeler helped in the understanding of how to simulate a security attack in a network. Though this tutorial was not in any way related to the Sybil attack or Wireless Ad hoc Networks, the mindset to generate a security attack in a simulation and network configurations, were understood to certain extent by reading this tutorial.

Chapter 4.

Simulation Scenarios & Results

In this chapter, we show the simulation of Sybil attack in the Wireless Ad hoc Network environment and study the effects of the attack in communication. For this simulation, the Academic edition of Riverbed Modeler 17.5 is used, due to its ease of use with rich features.

The simulation is planned to be carried in three parts. Ideal scenario and Sybil attack scenario in AODV network, DSR network, and TORA network. A final comparison between the DSR and TORA algorithm is also studied. All simulations were run for 1 hour.

4.1 AODV Network Scenario

4.1.1 Simulation Methodology

For the first scenario, a 20-node wireless peer to peer network is designed. The nodes are arranged in random order and no specific topology is used. Figure 4.1.1(a) shows the design of the P2P network used in the first scenario.

Figure 4.1.1(a): 20 node P2P network using AODV routing protocol

The most important network configurations are made in the Traffic generation parameters of the source. The destination IP is specified in the configuration of the source node, where traffic is generated. This is shown in Figure 4.1.1(b).

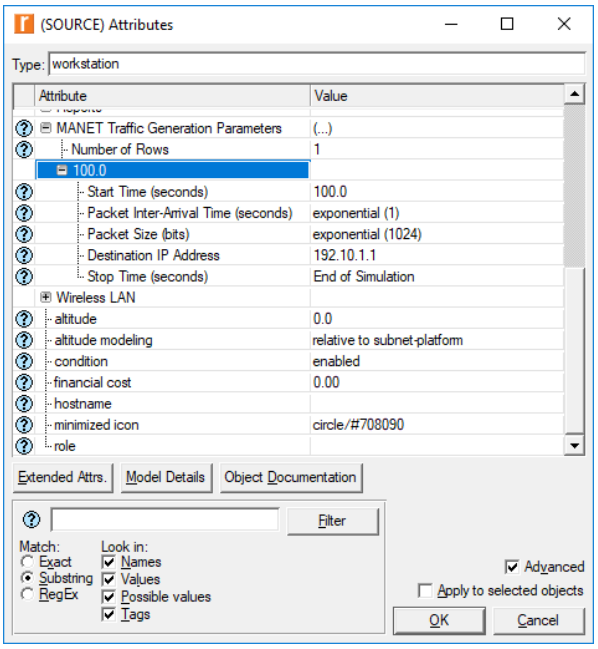

Figure 4.1.1(b): MANET Traffic Generation Parameters at source

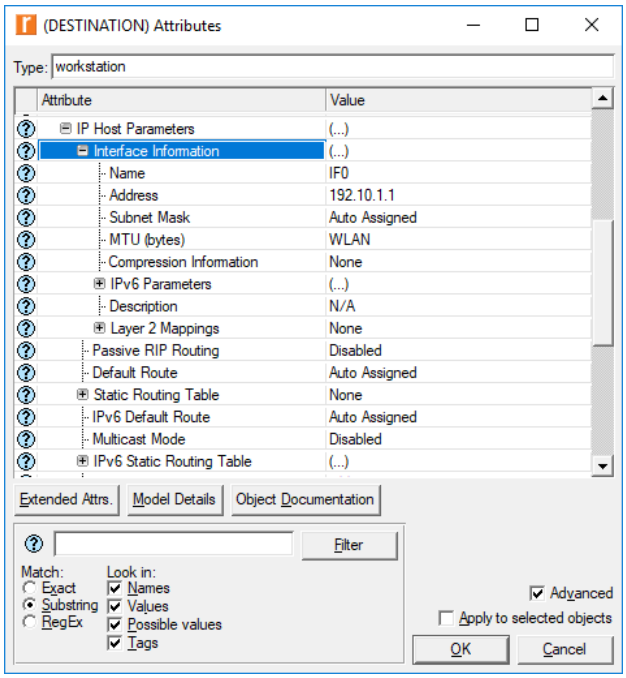

Figure 4.1.1(c): AODV routing parameters at source node

In addition to MANET parameters, certain configurations related to the routing protocol and the destination IP host configurations needs to be setup. Figure 4.1.1(c) and (d) shows the AODV routing protocol parameters at the source node and the IP host parameters at the destination node.

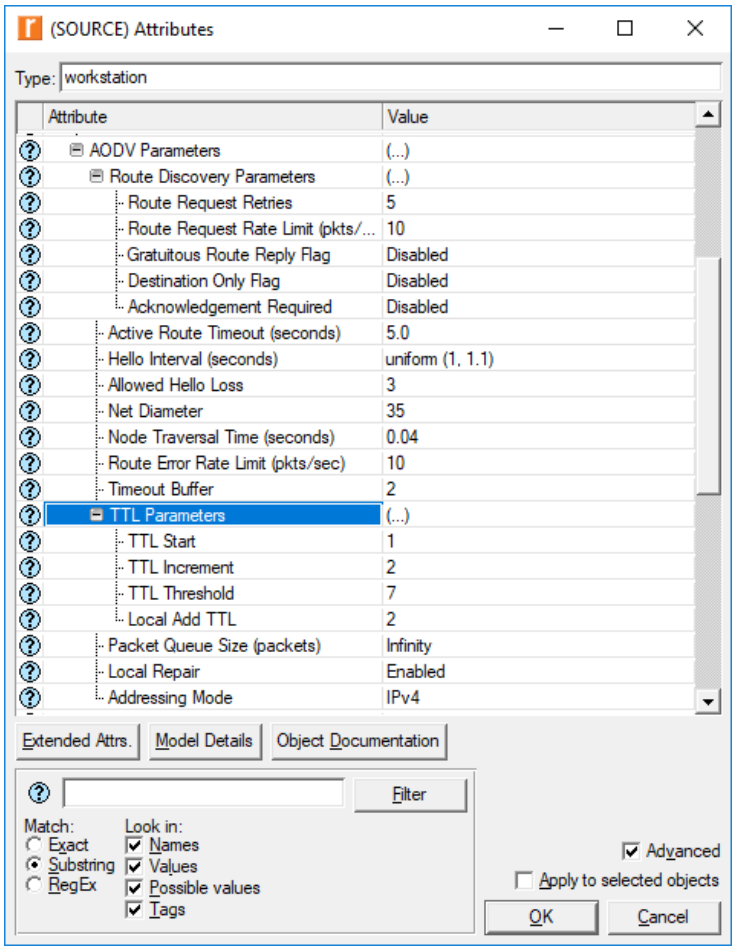

Figure 4.1.1(d): IP Host parameters at destination node

The second part of the scenario deals with the Sybil attack setup and simulation. Compared to the Ideal scenario, the network architecture does not vary a lot, only with the addition of few other nodes as part of the Sybil network at the right as shown in Figure 4.1.1(e). The Sybil network reroutes the traffic that is on route to the destination, to the attacker. The simulation result of this will be discussed in the later half of this section.

Figure 4.1.1(e): Sybil Attack scenario

4.1.2 Simulation Results

Now that both the scenarios are set, the simulation was run to check the traffic flow. In this scenario, the only statistic that was recorded is the traffic from source to destination, since we are interested in how this traffic will be intercepted in the Sybil scenario. Figure 4.1.2(a) shows the simulation results of the ideal scenario.

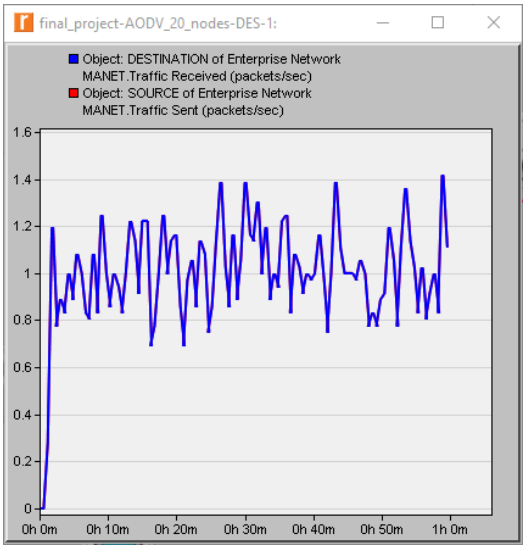

Figure 4.1.2(a): Source to Destination Traffic(Packets/Sec)

With no change in the network configurations of source and destination or any intermediate nodes in the initial case, comparing to the graph of the Ideal scenario with the Sybil scenario, we can see from figure 4.1.2(b), that in the sybil scenario, all of the traffic is completely rerouted to the attacker through the Sybil nodes even though the destination was much closer to the source than the attacker.

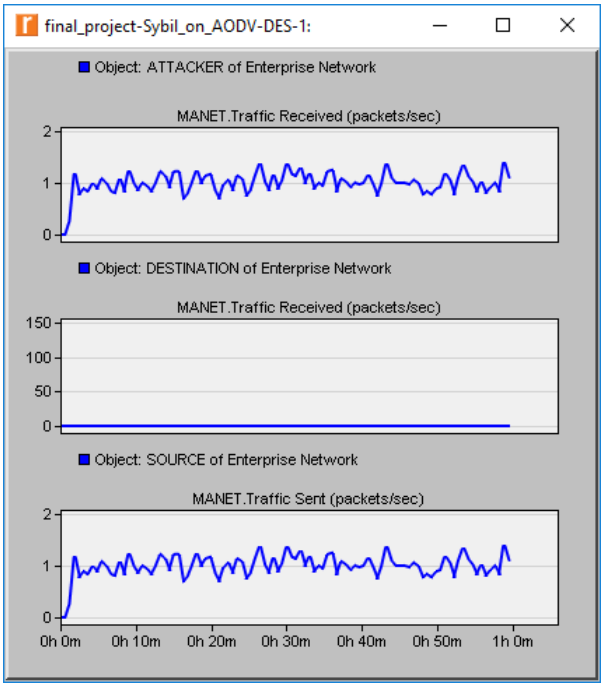

Figure 4.1.2(b): Source to Destination and Attacker Traffic(Packets/Sec)

4.2 DSR Network Scenario

4.2.1 Simulation Methodology

For the next scenario, a 50-node Wireless network, with random arrangement of nodes is considered. Unlike the AODV scenario, statistics such as the network load, Media Access Delay and the Total packets dropped are measured. In addition to the Sybil attack, we will be coupling it with the Ping of death attack on the server performing the DSR routing to see its adverse effects. Figure 4.2.1(a) and 4.2.1(b) shows the Ideal and the Sybil scenario of the second simulation case.

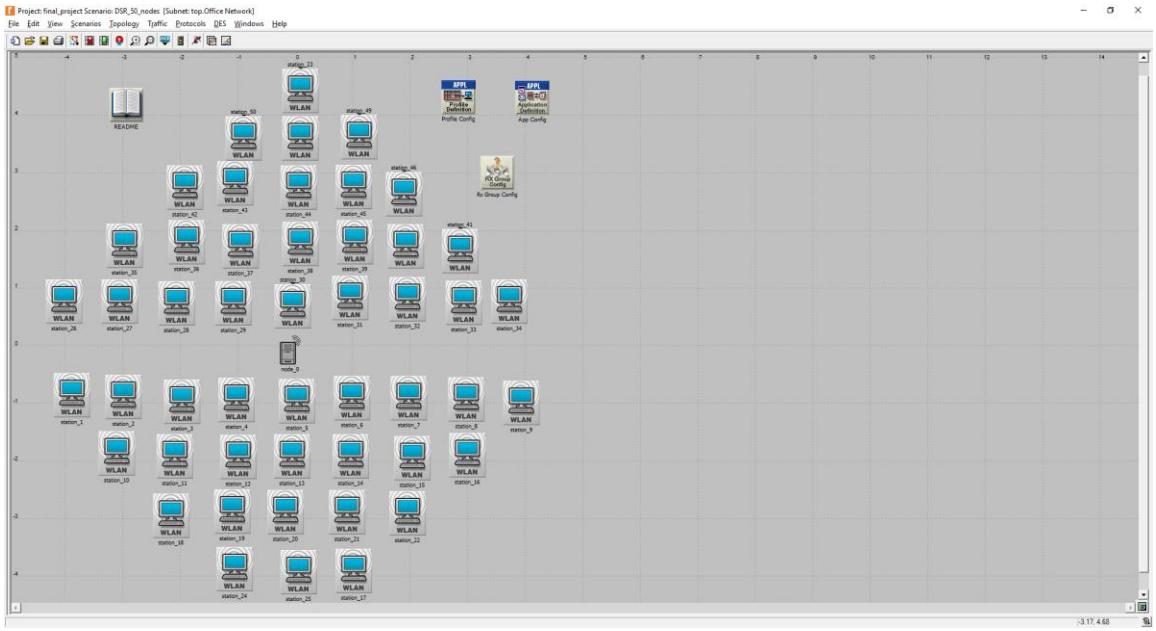

Figure 4.2.1(a): 50 node DSR network

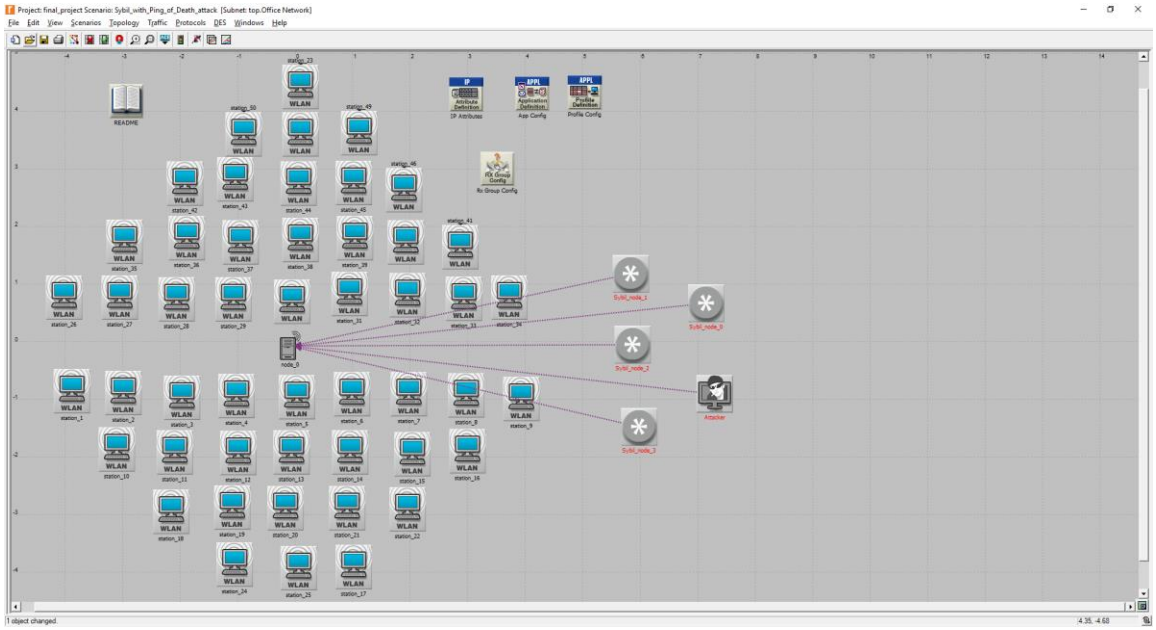

Figure 4.2.1(b): 50 node DSR network with sybil network

In the figure above, the links from the attacking nodes to the server represents the Ip Ping traffic that will be part of the Ping of Death attack. For the general traffic generation, we will be generating a high load of FTP traffic in the network.

The DSR network configurations are provided below. Unlike the AODV scenario, we need to use Application and Profile configuration nodes in addition to the IP attributes, due to FTP traffic generation.

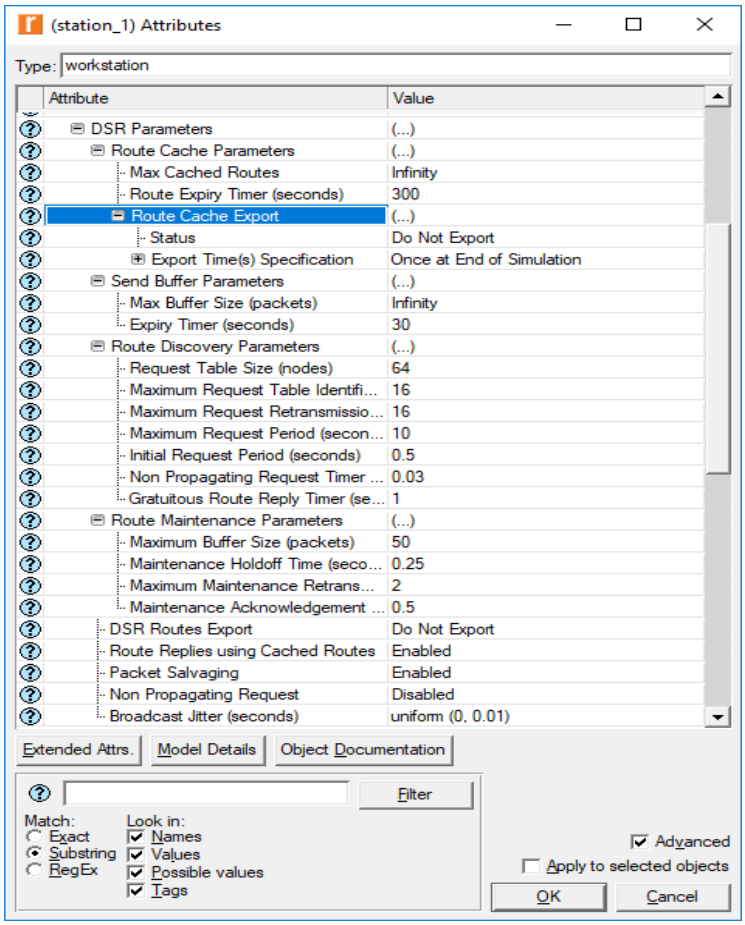

Figure 4.2.1(c): DSR routing protocol parameters

In the application config, we define the FTP application to be generated for traffic, and we use that application configuration in the profile config to specify more technical details specific to the FTP traffic generation. Figure 4.2.1(d) and 4.2.1(e) shows the profile and application config details.

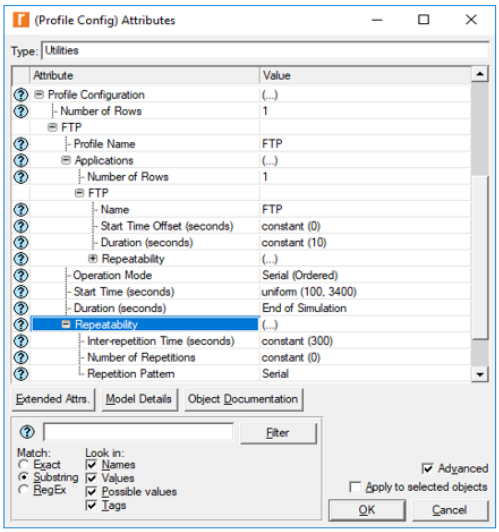

Figure 4.2.1(d)

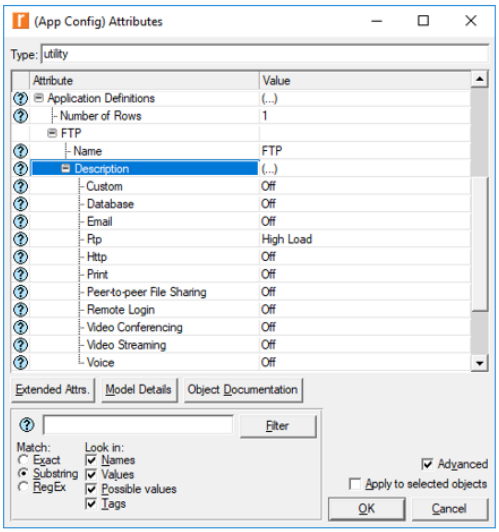

Figure 4.2.1(e)

Figure 4.2.1(d): Profile Configuration; 4.2.1(e) : Application Configuration

For the final configuration setup, we need to activate the IP traffic ping links to the server and the attacker nodes for the Sybil scenario. The attacker node configurations are the same as the regular nodes in the network. The IP ping traffic generation parameters are listed below.

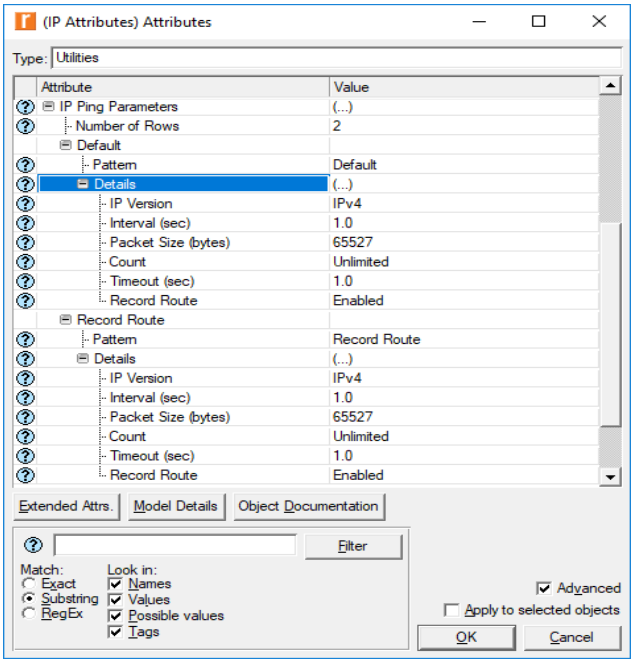

Figure 4.2.1(f): IP Ping traffic generation

4.2.2 Simulation Results

The simulation results for the ideal and the Sybil scenario are compared into a single graph for each of the statistics measured. In this section, we measure the load on the network, Media Access delay, and the total number of packets dropped.

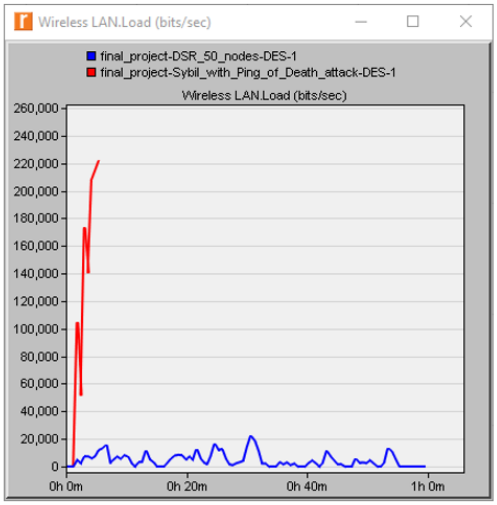

Figure 4.2.2(a)

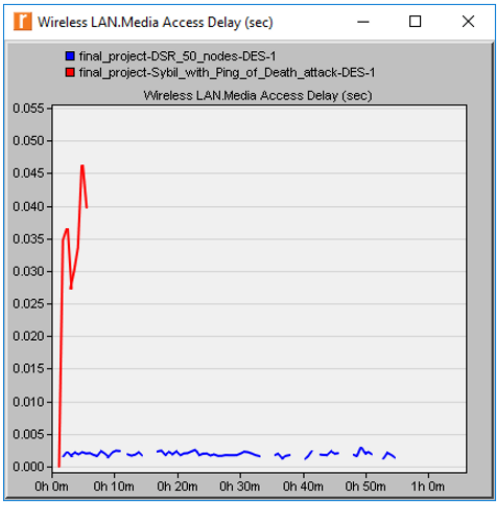

Figure 4.2.2(b)

Figure 4.2.2(a): Network load(bits/sec); 4.2.2(b): Media Access Delay(Sec)

From the graphs above we see that in the case of Sybil scenario, the number of bits transferred each second is more than 10 times the ideal value. The Server with the DSR routing fails after approximately 6 minutes due to high load from the attacking nodes. The same goes with the Media access delay where the delay rises to almost 10 times the ideal value in the Sybil attack scenario.

And where there is high network load, we expect more packets dropped. Figure 4.2.2(c) shows the packets dropped in the network every second due to the high load by the attacker. The packets dropped reaches 250 packets an instant, at one point of the simulation.

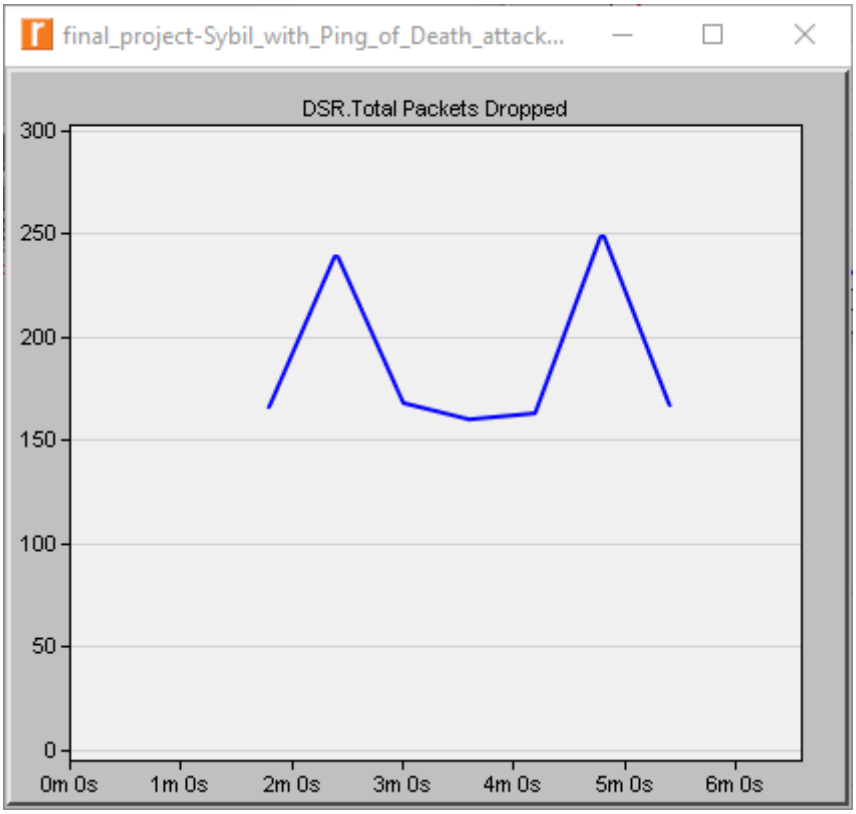

Figure 4.2.2(c): Total Packets Dropped

4.3 TORA Network Scenario

4.3.1 Simulation Methodology

For the third network scenario, we used the same network used for DSR routing scenario, with minor changes related to TORA routing algorithm. Configuration changes related to traffic generation and other infrastructural changes were not made.

Figure 4.3.1 shows the TORA routing algorithm parameter configurations. For this simulation scenario we will be recording the network load, media access delay and network end to end delay.

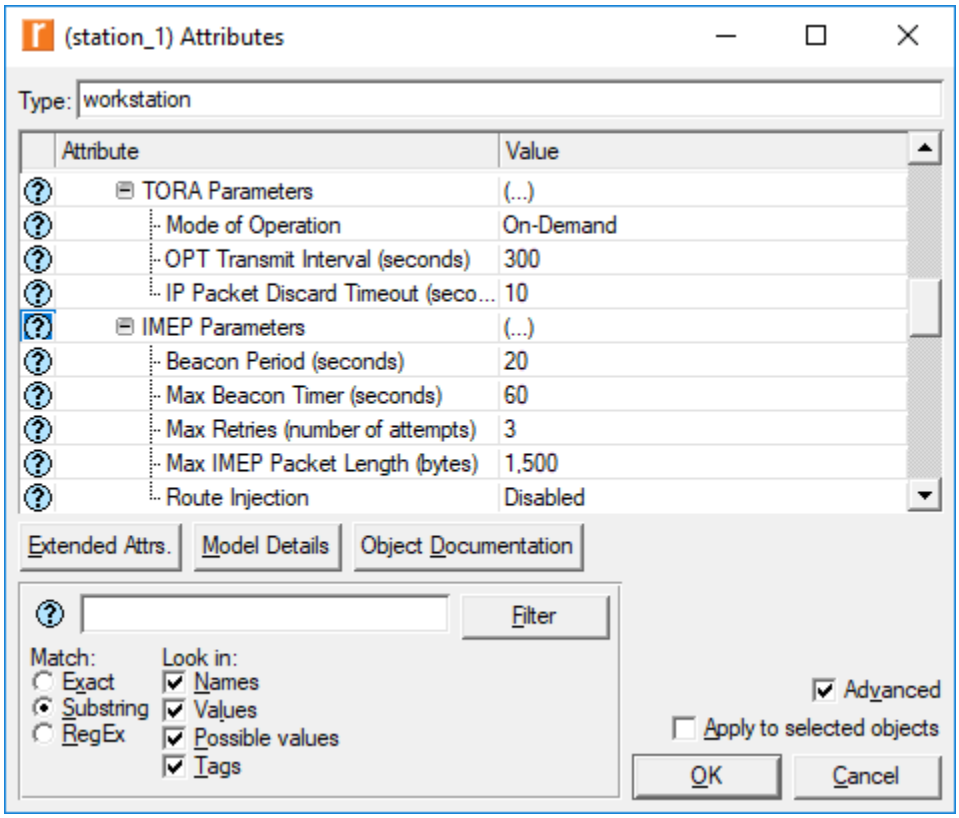

Figure 4.3.1: TORA algorithm parameter configurations

4.3.2 Simulation Results

Like the DSR scenario, the simulation result was recorded as a comparison between the ideal Sybil-less simulation and the Sybil coupled with the Ping of Death attack simulation.

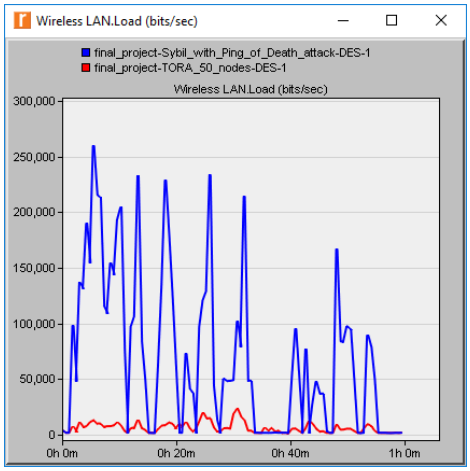

Figure 4.3.2(a): Network Load(bits/sec)

From Figure 4.3.2(a) we notice that the server does not crash even though the TORA algorithm network received the same load as the DSR network. Due to its hybrid nature, the TORA network having multiple routes, was able to efficiently reroute the traffic through unbroken links.

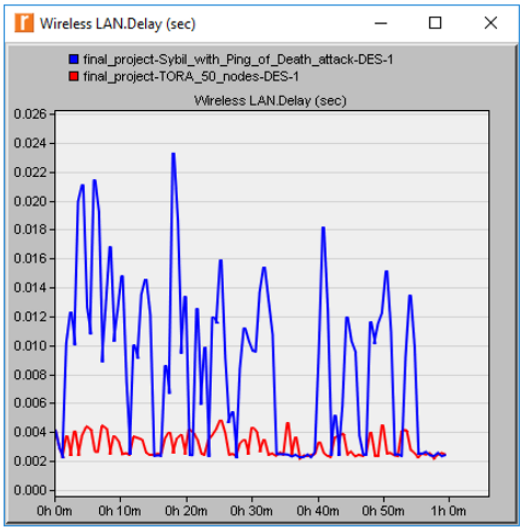

Figure 4.3.2(b)

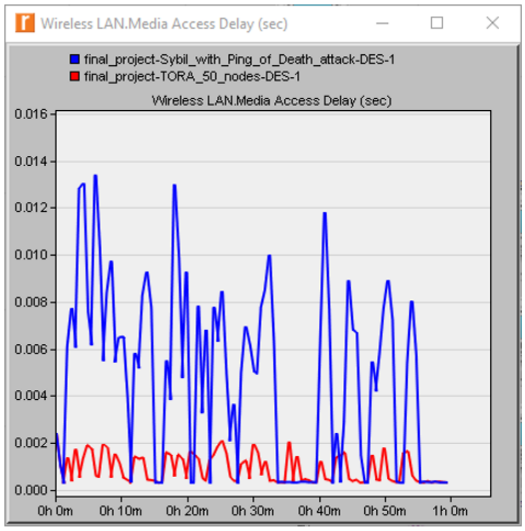

Figure 4.3.2(c)

Figure 4.3.2(b): Delay(Sec); 4.3.2(c): Media Access Delay(Sec)

There seems to be no change in end to end delay and the media access delay through the end of the simulation, except for the constant average difference of 0.008 seconds.

4.4 DSR vs TORA Comparison

4.4.1 Simulation Methodology

Analyzing the performance of DSR and TORA networks on scenario 2 and 3, out of interest, the performance of DSR and TORA algorithms was compared in this final scenario without any Sybil case involved.

For the comparison, the same 50 node network used in the previous two scenarios were taken again for comparison. Network configurations were left untouched.

4.4.2 Simulation Results

Through this comparison simulation, statistics such as throughput and network end to end delay were recorded.

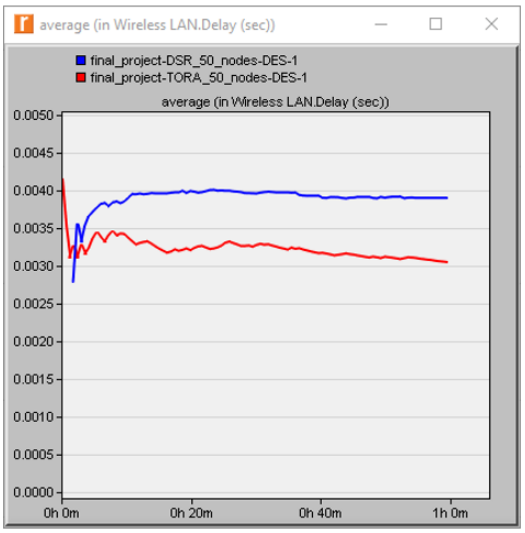

Figure 4.4.2(a)

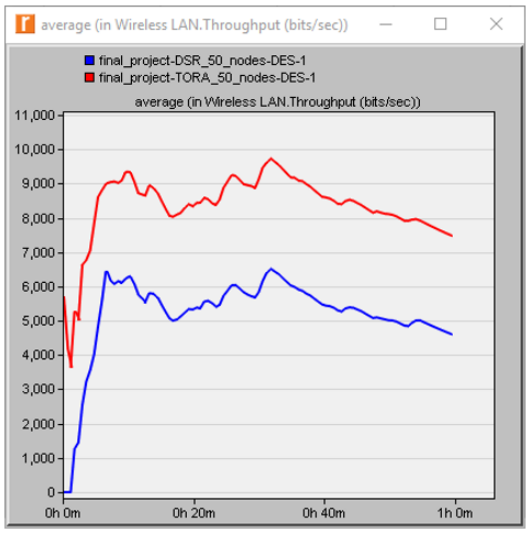

Figure 4.4.2(b)

Figure 4.4.2(a): Throughput(bits/Sec); 4.4.2(b): Network Delay(Sec)

Figure 4.4.2(a) and (b) shows that TORA routing algorithm outperforms the DSR routing for a 50-node wireless P2P network, even though both the algorithms were designed for multi hop wireless networks.

Chapter 5.

Discussion

As per the initial goal of understanding the effects of Sybil attack, we were able to simulate the attack with different routing protocols and study its effects. Due to the limitations of the simulation tool, we were not able to involve more routing protocols or prevention methodologies.

5.1 Future Work

Though we achieved the initial goal of simulating and analyzing sybil attack in MANET, we still have more room for understanding and clearing more queries that arise. Below are some of the proposed future works related to the current project.

Changes in Infrastructure

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

Changes in Implementation

- Implement additional routing algorithms with existing or new network

Taking it further

- Simulate Sybil/other possible attacks in MANET with the detection and prevention methodologies.

All of these suggested future work seems not possible to be realised in the academic edition of riverbed modeler due to its limited features. Open source tools such as NS3 or OMNET++, or licensed version of Riverbed Modeler can be used for future work.

5.2 Challenges

There were few challenges that I faced at the beginning of the project. Due to minimal features in the academic edition, realising the project whether it can be simulated was the first challenge. Understanding how the packets are generated and routed to destination was the next challenge faced, which took considerate amount of time to find the answer for. Troubleshooting the issue of no result for AODV scenario with nodes more than 8 was the final challenge.

Chapter 6.

Conclusion

With the 4 simulation scenarios in the project, we were able to understand how Sybil attack works and how vulnerable MANET is to such attacks due to lack of a central authority. We also realized TORA routing algorithm performs better than the other routing algorithms due to its hybrid nature. Due to the limitations of riverbed modeler, further progress on detection methodology and preventive measures couldn’t be made.

References

[1] (2018, Apr.) A. Dorri, S.R. Kamel, E. Kheyrkhah, “Security Challenges in Mobile Ad Hoc networks: A Survey” [Online]. Retrieved from http://www.airccse.org/journal/ijcses/papers/6115ijcses02.pdf.

[2] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, DOI 10.17487/RFC3561, July 2003, <https://www.rfc-editor.org/info/rfc3561>.

[3] Johnson, D., Hu, Y., and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, DOI 10.17487/RFC4728, February 2007, <https://www.rfc-editor.org/info/rfc4728>.

[4] Z. Kasiran and J. Mohamad, "Throughput performance analysis of the wormhole and sybil attack in AODV," *2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, Bangkok, 2014, pp. 81-84.

[5] (2018, Apr.) S. Razak, M. Zhou and S. Lang, “Network Intrusion Simulation Using OPNET” [Online]. Retrieved from https://splash.riverbed.com/servlet/JiveServlet/previewBody/2465-102-1-2746/376.430.pdf

[6] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004, 2004, pp. 259-268.

[7] S. K. Chowdhury and M. Sen, "Attacks and mitigation techniques on mobile ad hoc network — A survey," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, Tirunelveli, 2017, pp. 11-18.

[8] (2018, Apr.) J.R. Douceur, « The Sybil Attack” [Online]. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf