Simulation and Analysis of Sybil Attack in MANET

ENSC 835: Communication Networks

Prof. Ljiljana Trajkovic

Aaditya Vasan Srinivasan

asriniva@sfu.ca

Team-4

SFU ENGAGING THE WORLD

Outline

- Motivation & Goal
- Introduction
- Related work
- Simulation Scenarios & Results
- Future Work
- Conclusion

Motivation

Clip from the movie "*Snowden*(2016)"

Motivation & Goal

- In the digital age, everything and everyone are connected through the Internet. Devices have gone wireless that can establish connection to almost any other wireless device.
- In an environment where the connection is established in an adhoc basic like in wireless adhoc networks, security is one of the weakest aspects.
- Understanding how the attack works and the damage it causes by the end of the simulation.
- Also learning about cyber security is interesting!

Outline

- Motivation & Goal
- Introduction
- Related work
- Simulation Scenarios & Results
- Future Work
- Conclusion

Introduction

MANET

- Wireless Adhoc Network also know as Mobile Adhoc Network is an infrastructure less OnDemand network of nodes.
- These spontaneous networks are self configuring based on the routing algorithm used and the availability of nodes and network connectivity.
- Due to lack of predefined infrastructure, these networks have huge benefits.

Introduction

Routing Algorithms

- Ad hoc On-Demand Distance Vector(AODV) Routing is one of the most commonly used algorithms in MANET. It is a reactive protocol that establishes connection only when it is required
- Dynamic Source Routing(DSR) is another reactive protocol similar to AODV but uses source routing instead of routing tables.
- Temporally Ordered Routing Algorithm(TORA) is a hybrid protocol, that is highly adaptive in case of link failures, providing several routes to destination.

Outline

- Motivation & Goal
- Introduction
- Related work
- Simulation Scenarios & Results
- Future Work
- Conclusion

Related Work

- A survey on the different types of security attacks possible in Mobile Ad hoc networks[1].
- Analyzing performance affected by Sybil and wormhole attack in Mobile Ad hoc Networks with AODV routing algorithm[2].
- Simulation of network intrusion using OPNET modeler[3].

Outline

- Motivation & Goal
- Introduction
- Related work
- Simulation Scenarios & Results
- Future Work
- Conclusion

Simulation Scenarios

Scenario-1

- For the first scenario, AODV routing algorithm is implemented in a 20 node wireless peer to peer network.
- Two sub scenarios are tested in the first scenario.
  - Ideal scenario
  - Sybil attack scenario
- Packets sent and received are tracked in this scenario

Simulation Scenarios

Scenario-1(Ideal case)

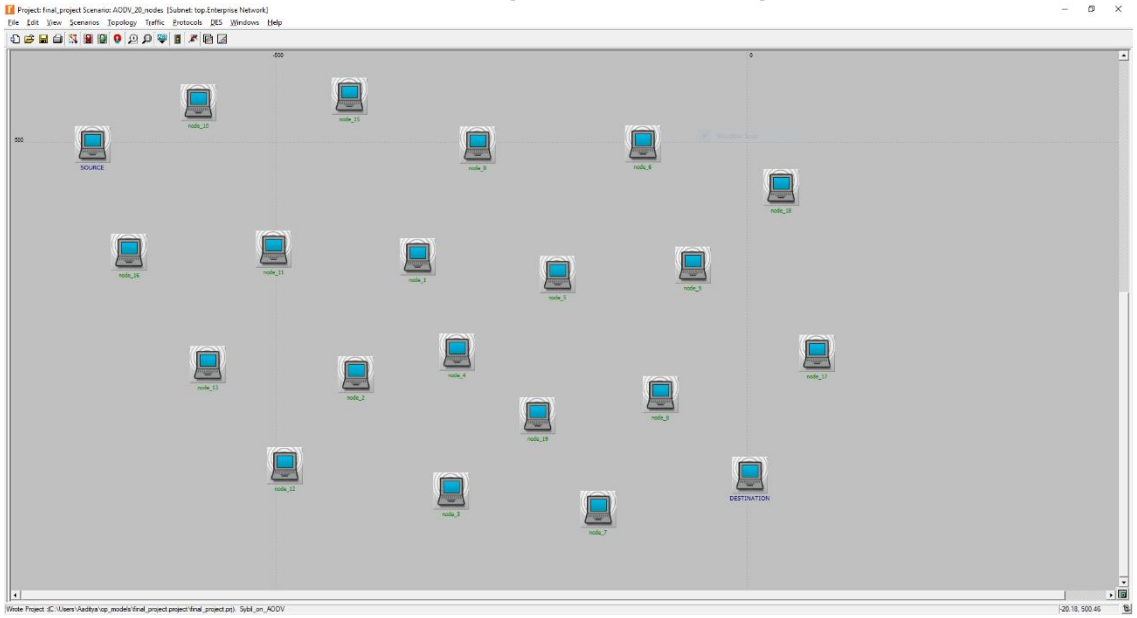
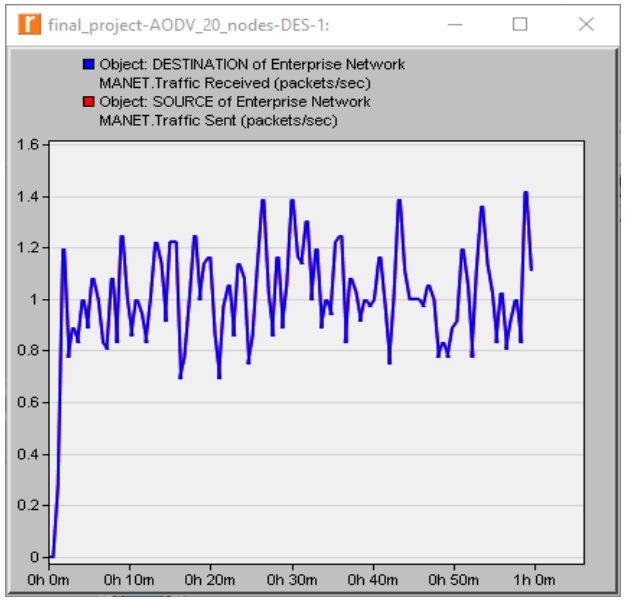


Figure 1(a): P2P network with AODV routing



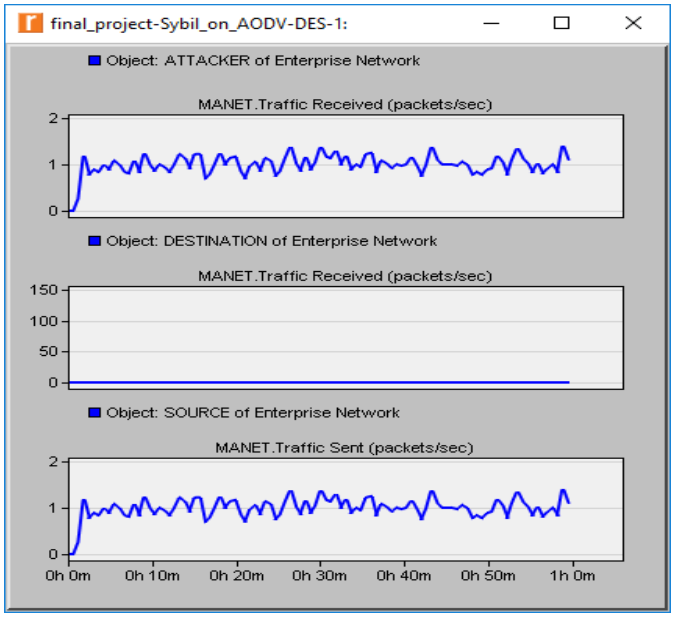
X-axis: 1 unit = 10 mins
Y-axis: 1 unit = 0.2 packets

Figure 1(b): Source to Destination traffic

Simulation Scenarios

Scenario-1(Sybil attack case)

Figure 1(a): P2P network with Sybil Network



X-axis: 1 unit = 10 mins
Y-axis: 1 unit = 1 packet

Figure 1(b): Source to Destination and Attacker traffic

Simulation Scenarios

Scenario-2

- In the second scenario, DSR routing algorithm is implemented in a 50 node wireless peer to peer network.
- Two sub scenarios are tested in the first scenario.
  - Ideal scenario
  - Sybil attack coupled with ping of death scenario
- Statistics such as server load, Media Access Delay, and packets dropped are tracked in this scenario.

Simulation Scenarios

Scenario-3

- In the third scenario, TORA routing algorithm is implemented in the same 50 node wireless peer to peer network reused for DSR routing.
- Two sub scenarios are tested in the first scenario.
  - Ideal scenario
  - Sybil attack coupled with ping of death scenario
- Statistics such as server load, Media Access Delay, and network delay are tracked in this scenario.

Simulation Scenarios

Scenario-2/3(Ideal Scenario)

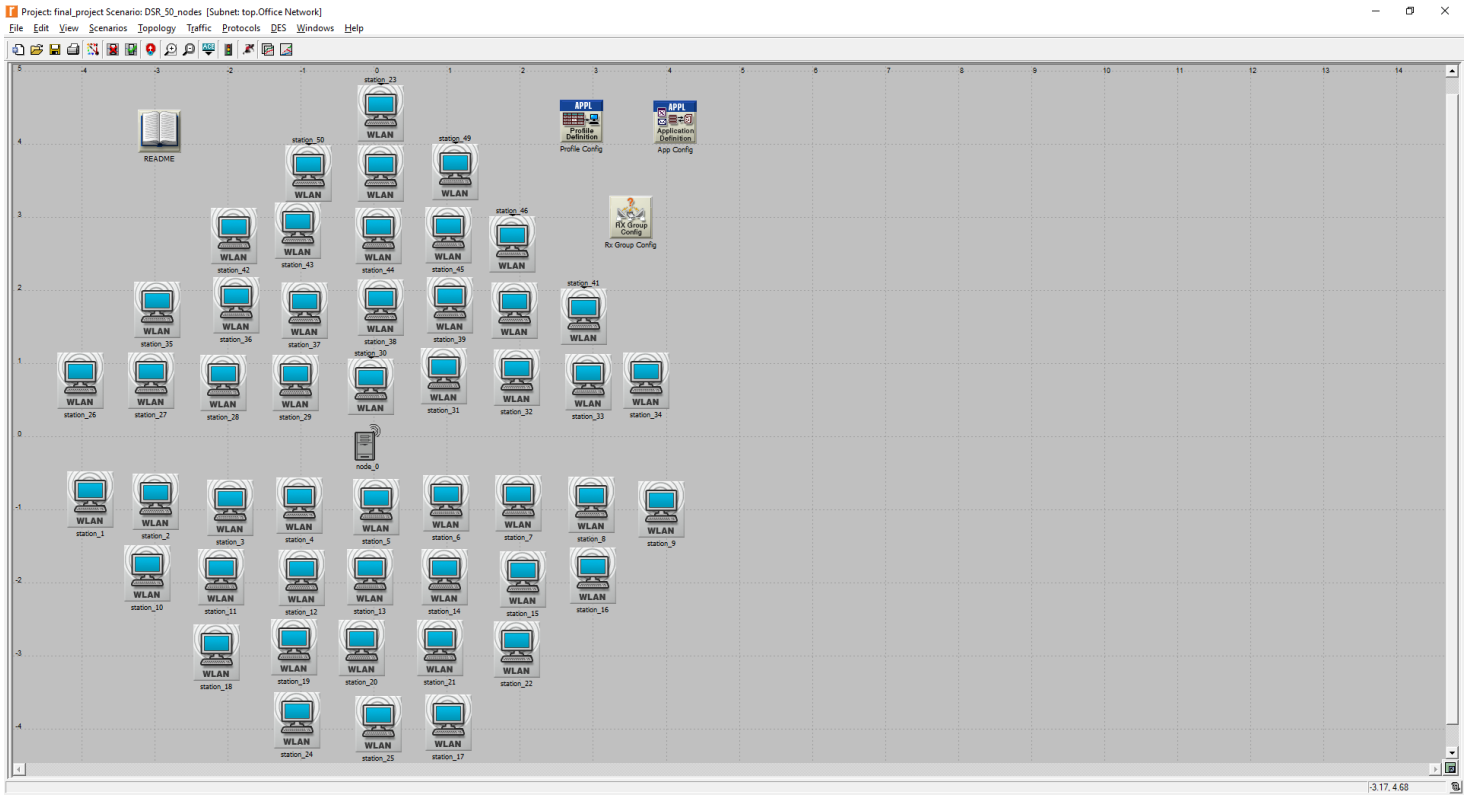


Figure 2(a): WLAN nodes with DSR/TORA routing

Simulation Scenarios

Scenario-2/3(Sybil + Ping of Death Scenario)

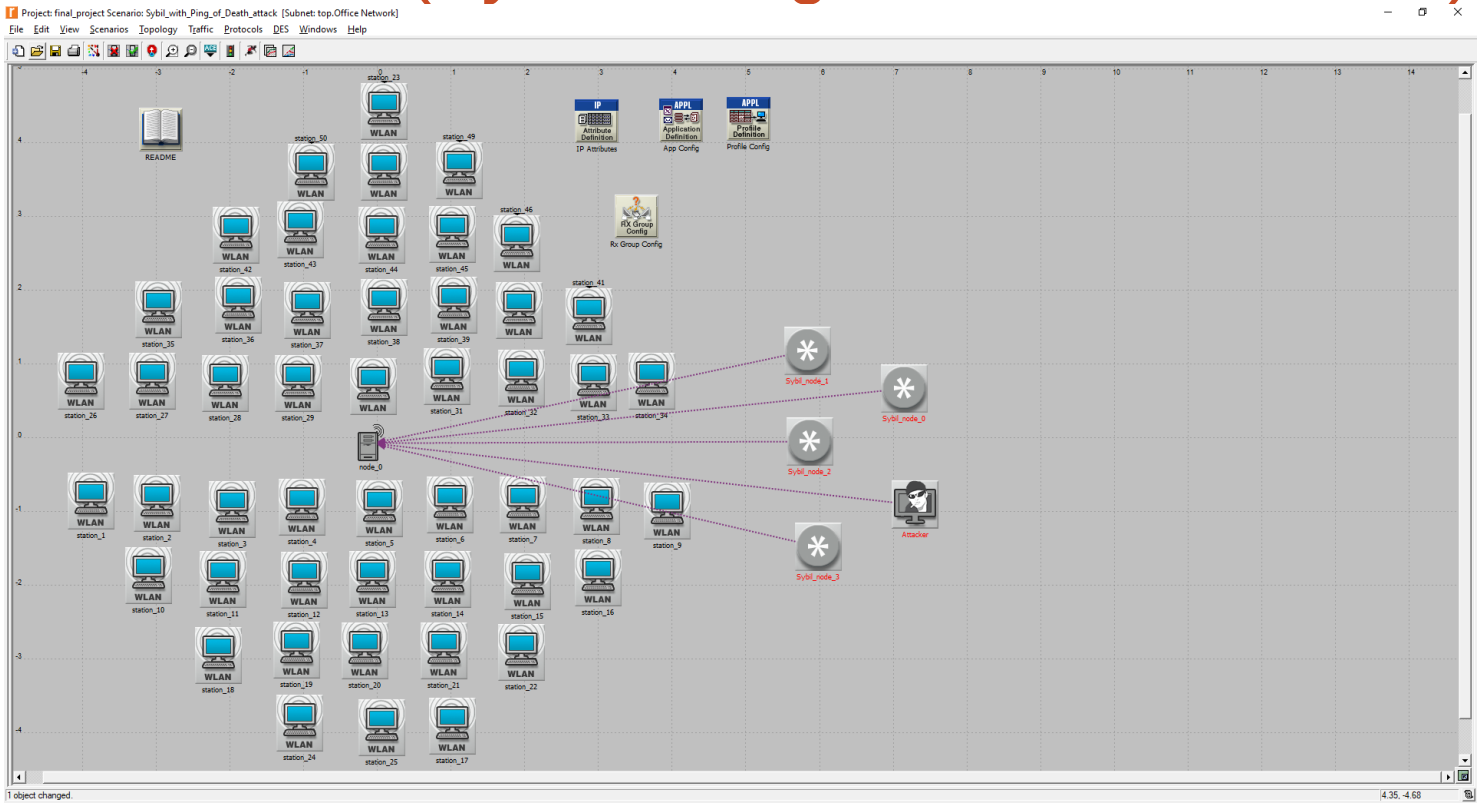
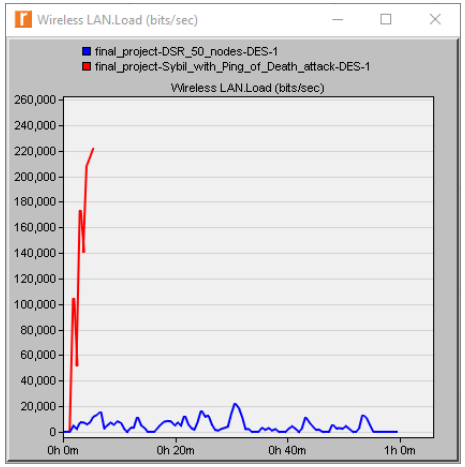


Figure 2(b): Sybil + Ping of Death with Sybil network

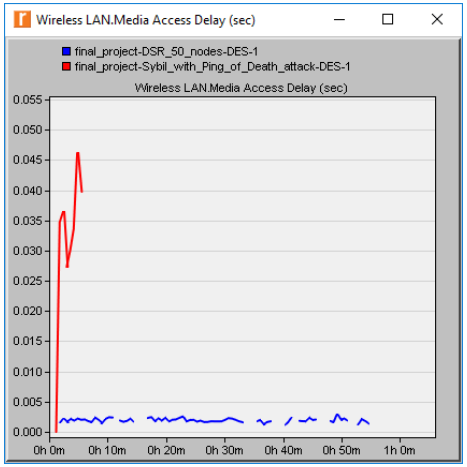
Simulation Scenarios

Scenario-2 (Comparison of Sub scenario 1 & 2)



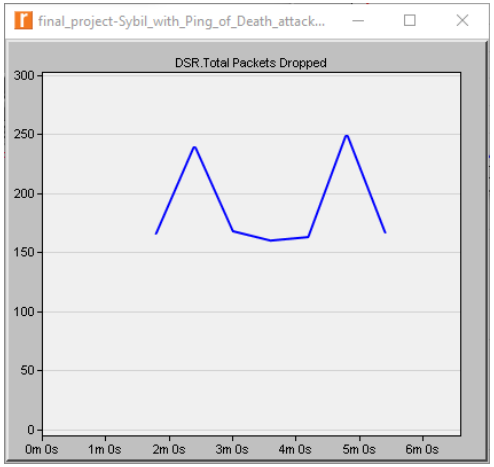
X-axis: 1 unit = 20 mins
Y-axis: 1 unit = 20,000 bits

Figure 2(c): Network Load



X-axis: 1 unit = 10 mins
Y-axis: 1 unit = 0.005 seconds

Figure 2(d): Network MAD

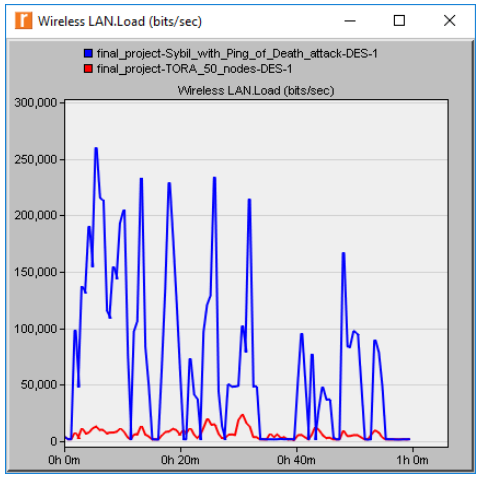


X-axis: 1 unit = 1 min
Y-axis: 1 unit = 50 packets

Figure 2(e): Total packets dropped

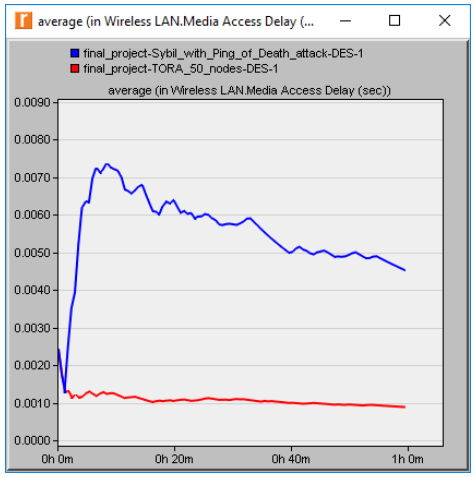
Simulation Scenarios

Scenario-3 (Comparison of Sub scenario 1 & 2)



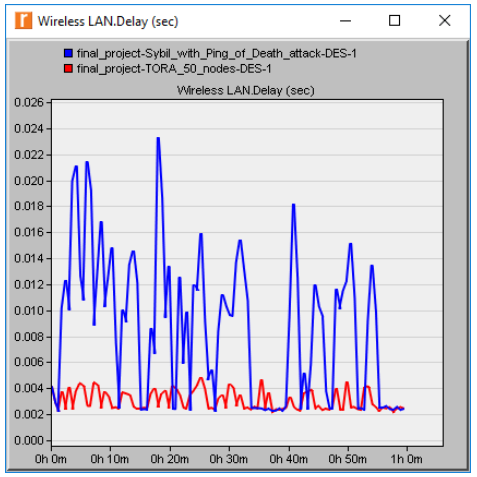
X-axis: 1 unit = 20 mins
Y-axis: 1 unit = 50,000 bits

Figure 3(a): Network Load



X-axis: 1 unit = 10 mins
Y-axis: 1 unit = 0.002 seconds

Figure 3(b): Network MAD



X-axis: 1 unit = 1 min
Y-axis: 1 unit = 0.002 seconds

Figure 3(c): Network Delay

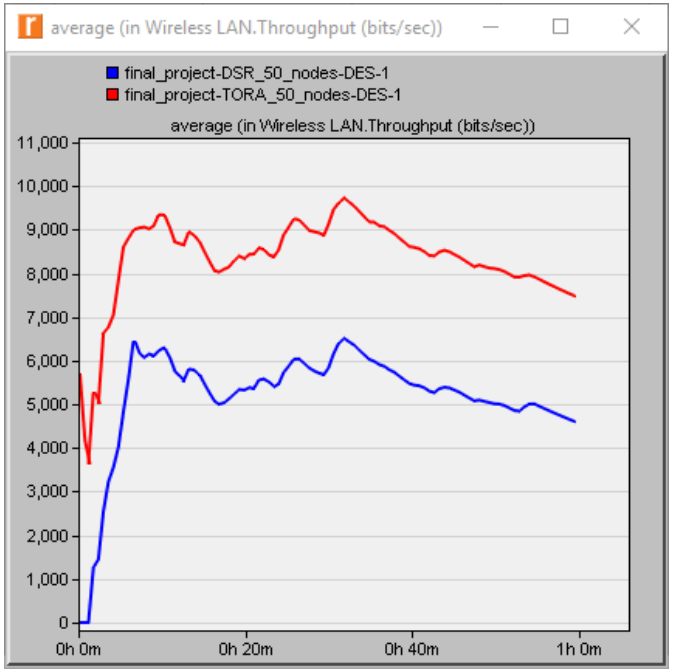
Simulation Scenarios

Scenario-4

- Clearly TORA routing algorithm performs better than the DSR routing algorithm from the results of scenario 2 and 3.
- In the scenario 4, performance of the 50 node network with DSR and TORA algorithm running FTP at high load is tested.

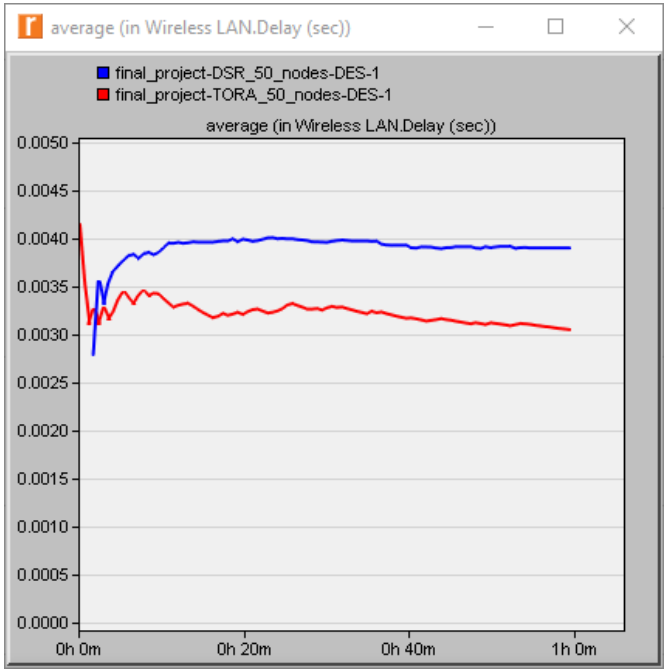
Simulation Scenarios

Scenario-4



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

Figure 4(a): Network Throughput



X-axis: 1 unit = 20 mins
Y-axis: 1 unit = 0.0005 seconds

Figure 4(b): Network Delay

Outline

- Motivation & Goal
- Introduction
- Related work
- Simulation Scenarios & Results
- Future Work
- Conclusion

Future Work

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.

Outline

- Motivation & Goal
- Introduction
- Related work
- Simulation Scenarios & Results
- Future Work
- Conclusion

Conclusion

- As per the goal, we simulated Sybil attack in MANET and studied its effects and performance decrease in wireless P2P networks.
- TORA routing protocol being hybrid, brings in the best of both worlds.
- Sybil attack's efficiency increases with effectiveness of implementation. The damage although not big in our case, can be devastating if implemented with several Sybil nodes.

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] 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.

[3] (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

[4] 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.

[5] 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.