Simulation of Sybil Attack in VANET
ENSC833: PERFORMANCE OF COMMUNICATION NETWORKS

Team05 - Final Project

Salman Imtiaz, Amandeep Singh Bhogal

Spring 2019

Project Webpage

simtiaz@sfu.ca

abhogal@sfu.ca

Outline

- Motivation and Goal
- Introduction & Overview
  - A peek into VANET
  - Security in wireless network: SYBIL attack, what and why!
- Related Work
- Implementation
  - Tools
  - Technical Aspects and Validation
- Results and Analysis:
  - Simulation in NS3 and Riverbed Modeler
  - Simulation Comparison
- Analysis and Learning
- Future Work and Difficulties
- References

Motivation and Goal

- To study communication and attacks in VANET
- In today's age of interconnected network systems, security and privacy is a big concern
- Looking into these vulnerabilities is essential for secure and reliable communication
- Develop insight for most common attack – SYBIL
- Implement model for VANET for above mentioned attack
- To analyze performance of VANET under normal conditions and Sybil attack for two different simulation platforms, NS-3 and Riverbed Modeler

Introduction & Overview
A peek into Vehicular Adhoc Network (VANET)

- A special class of Mobile adhoc networks (MANET)
- VANET was first introduced in 2001 under “car to car ad-hoc mobile communication and networking” and is an amendment to IEEE 802.11 standard to add wireless access in vehicular environments (WAVE)
- **Purpose**: To develop a network where information can be relayed through vehicles and road side unit acting as nodes making it both infrastructure and infrastructure less
- **Topology:** includes vehicle-to-vehicle, vehicle-to-roadside unit communication network including wireless sensors, GPS, Event recording and computing unit –More sensor networks can be added
- **To provide services**: Road safety (traffic management and coordination) and Efficiency (navigation)

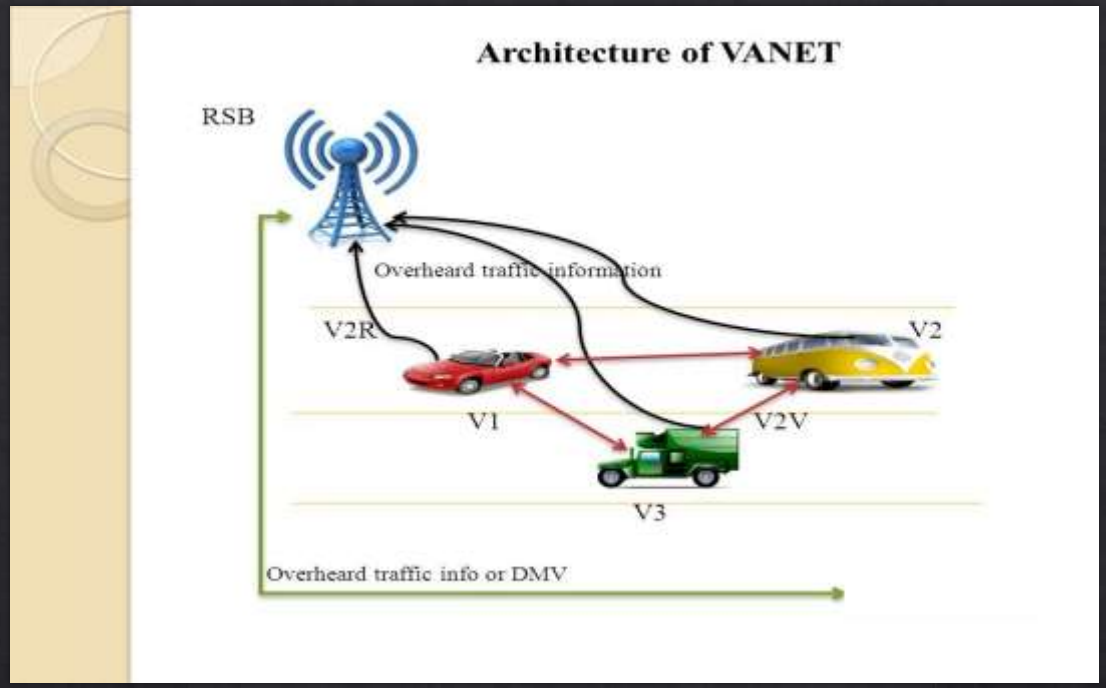

Fig 1 Architecture of VANET Source: https://slideplayer.com/slide/9291015/ [ONLINE]

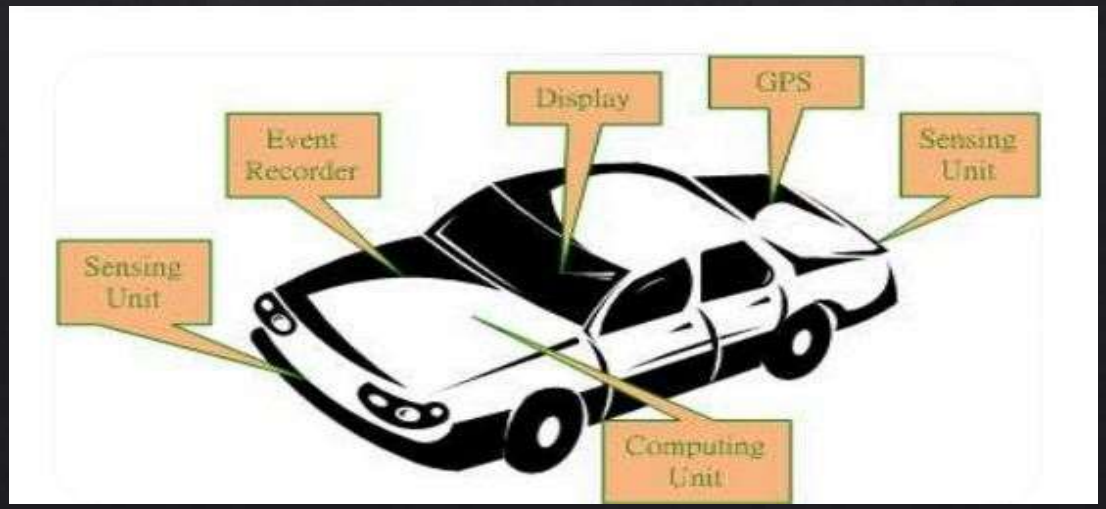

Fig -2 Information providing units Source: https://www.slideshare.net/sudama98611/vanet-52976807[ONLINE]

Introduction & Overview
A peek into Vehicular Adhoc Network (VANET)

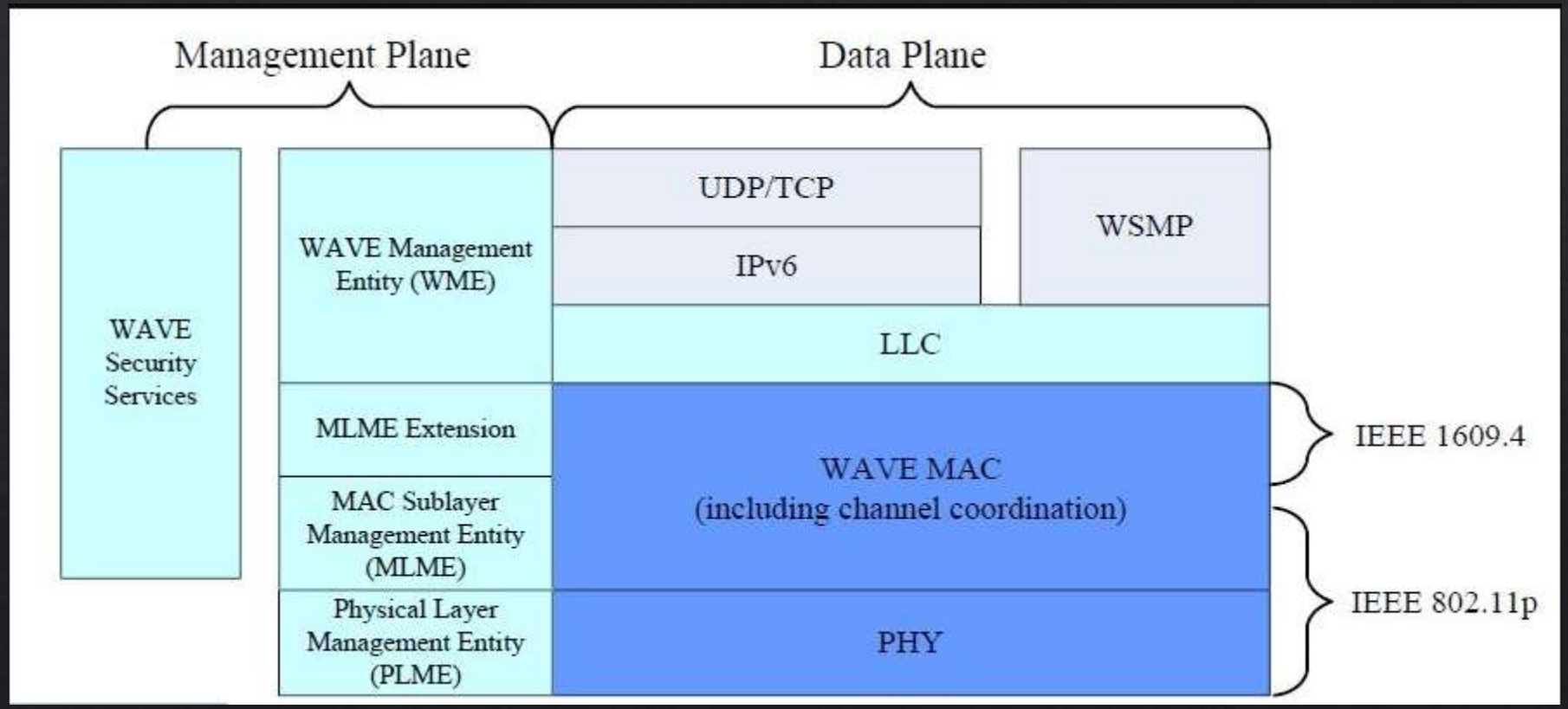

Fig-3 Wireless Access in Vehicular Environment Architecture

LLC – Logical Link Control

WSMP - Wave Short Message Protocol

Source: https://www.semanticscholar.org/paper/A-Survey-of-IEEE-802-.-11-p-MAC-Protocol-Miao-Djouani/b5edf2b0b3422924334a154689a8fd463a33f5a9/figure/1 [ONLINE]

Introduction & Overview

Security in VANET: SYBIL attack, what and why!

- Advantages of such technology bring concerns of security and privacy
- Large data generation in VANET, safety and efficiency oriented focus makes it sensitive to security
- Sybil attack is one of the attacks regarded as most serious for wireless ad-hoc networks
- Sybil attack causes security breach through identity hijacking resulting in information theft, communication disruption or data corruption

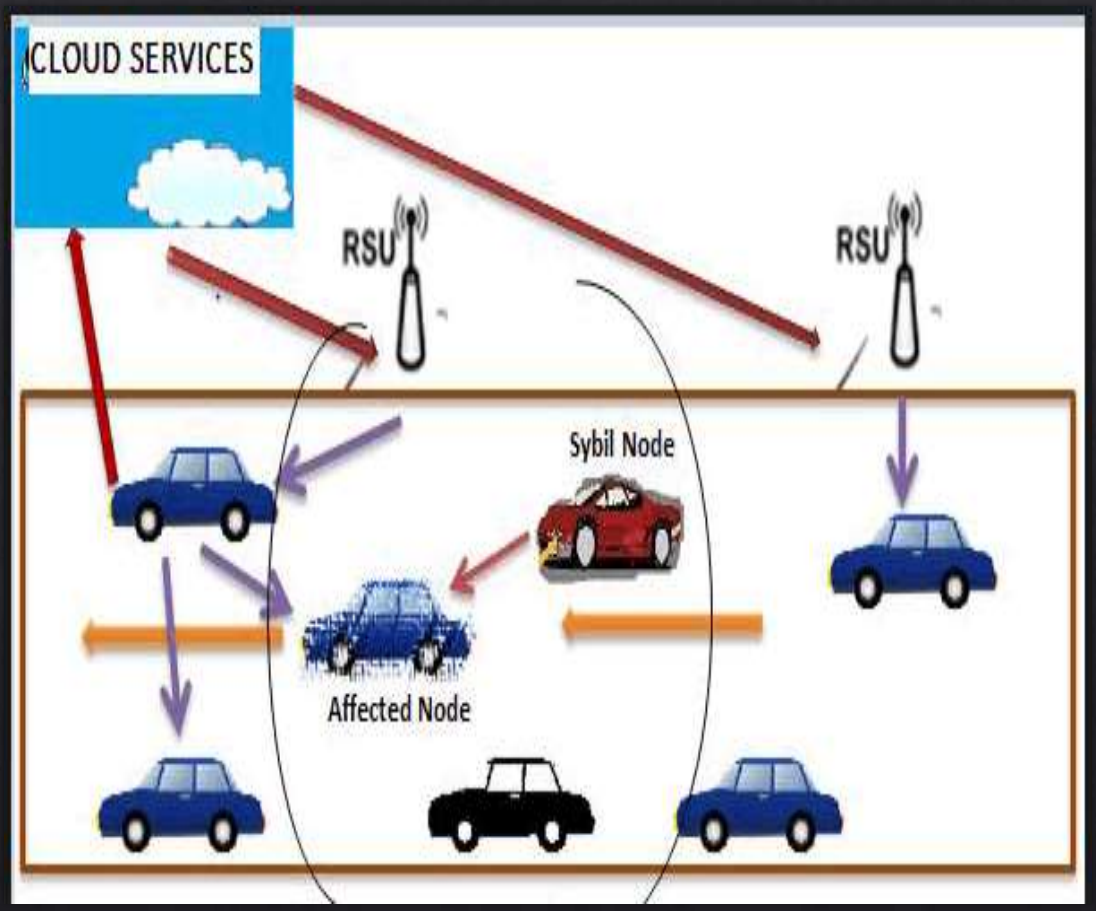

Fig-4 Sybil attack scenario

Source: http://www.ijircce.com/upload/2015/march/15_Sybil.pdf [ONLINE]

Related Work

Most of the related work has been done in this field as below:

[1] Vehicular Ad-Hoc Networks (VANETs) – An overview and Challenges

[3] Defense Against Sybil Attack in Vehicular Ad Hoc Network Based on Roadside Unit Support

[5] Performance Study of IEEE 802.11p for Vehicle to Vehicle Communications Using Opnet

Implementation: Tools

- Developing topology for VANET in NS-3 and Riverbed Modeler
- Choosing simulation platforms – what is important:
  - Support in getting better understanding for the concern topic
  - Must provide support in terms of available resources and support
  - Learn the tool!

- Network Simulator 3 (NS-3):
  - A discrete, free, open source network simulator targeted primarily for research and education purposes
  - Extensive available examples, flexibility of parameters, library functions, online support community makes implementation and troubleshooting easy
  - Require good understanding of NS-3 modules, working and C++ or python language
- Riverbed Modeler
  - Network simulator provide infrastructure for modeling, analyzing and developing network systems
  - Available rich GUI features makes it easy to implement network topologies
  - Limited features available in Academic edition

Implementation: Technical Aspects and Validation

Network Simulator-3 – Parameter Definition

Parameter	Value
Transmission Rate	2048 bits per second (BPS)
Packet Size	64 bytes
Wifi Standard	802.11p
PHY Layer	Orthogonal Frequency Division Multiplexing (OFDM)
Routing Protocol	Ad-hoc on demand distance vector (AODV)
Traffic	Unicast, Constant Bit Rate
Application	NS-3: On-Off Application
Mobility Model	Random mobility model Range: 100x100 Speed: 10m/s
Frequency	5.9GHz
Transmit Power	7.5dBm
Transport Layer	User Datagram Protocol (UDP)

Implementation: Technical Aspects and Validation

Riverbed Modeler – Parameter Definition

Parameter	Value
Transmission Rate	2048 bits per second (BPS)
Packet	Hello (uniform interval)
Wifi Standard	802.11a
PHY Layer	Orthogonal Frequency Division Multiplexing (OFDM)
Routing Protocol	Ad-hoc on demand distance vector (AODV)
Traffic	Unicast, Constant Bit Rate
Mobility Model	Random mobility model Speed: 10m/s
Frequency	5GHz
Transmit Power	7dBm
Transport Layer	User Datagram Protocol (UDP)

Implementation Ideas: Technical Aspects and Validation

Network Simulator-3 – Parameter Details

- Routing Protocol –Ad-hoc on Demand Vector
  - Routing protocol designed for wireless and mobile ad-hoc networks, establishes routes to destination on demand
- Wi-fi Standard – 802.11p
  - Operates within 5.850 – 5.925 GHz frequency
  - Designed for 10MHz wide channel instead of 20MHz used in 802.11 family, intended for higher reliability and lower throughput
  - Data rate up to 27Mbps, while other Wi-fi standards support up to 54Mbps
  - Uses physical layer same as other wi-fi standards (OFDM)
  - Most of the changes are in Data Link layer in order to cater for high pace communication environment

Implementation: Technical Aspects and Validation

Network Simulator-3 – Sybil Attack

- Focus on data corruption from malicious node, to introduce error from sender and eventual packet drop
- Focus on channel disruption, simulate the attack scenario through decrease in nodes registering output (sink nodes) and eventual decrease in throughput

Network Simulator-3 – Required Output

For simulation time of 100s, following outputs were checked

- Throughput - Measured at receiving end in terms of “bits received per second” for normal condition and under attack
- Bytes Dropped – Number of bytes dropped from sender to receiver under normal condition and under attack condition

Implementation: Technical Aspects and Validation cont.

Network Simulator-3 – Validation

Initial validation done with two nodes at distance 10 in x- & y- direction

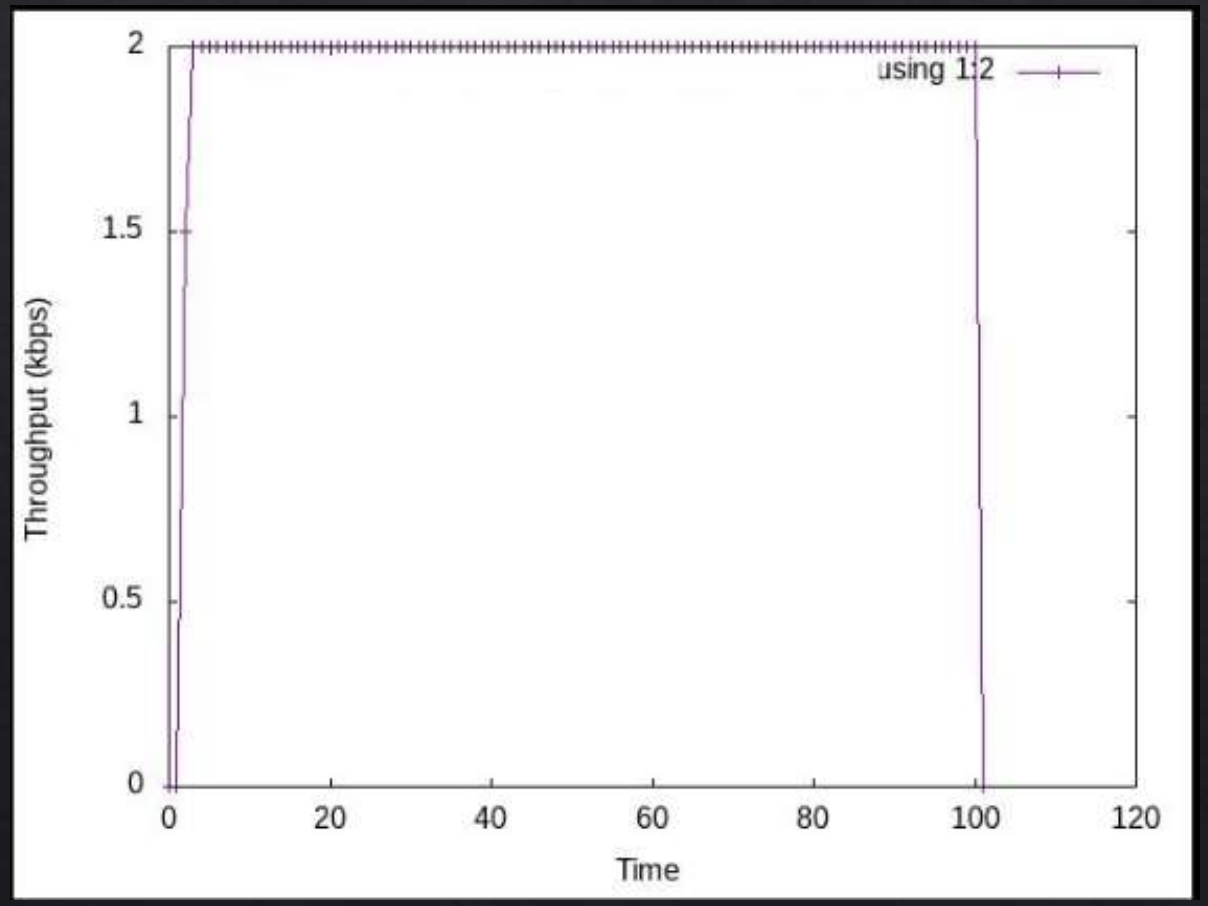

Fig- 5 Throughput vs Time

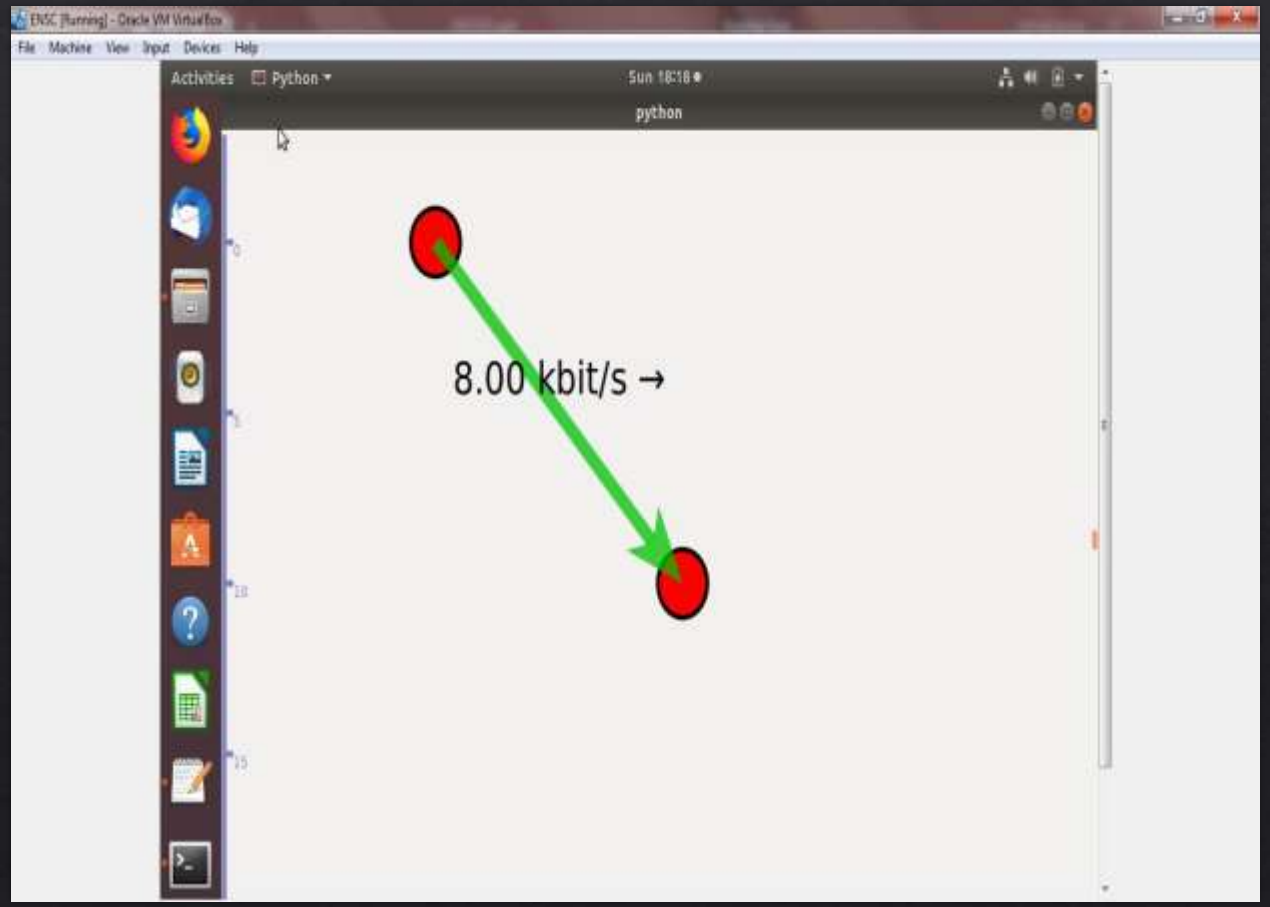

Fig-6 Initial Validation

Results: Scenarios – NS3

Simulation on network simulator conducted with one scenario for normal condition and under attack condition:

- Scenario#1_1 (normal condition):
  - Network of 10 nodes with 3 nodes registering output (as trace sink) under normal condition
  - One road side unit node (non-mobile)
  - Nine vehicle nodes (mobile)
  - Simulation time 100s

- Scenario#1_2 (under attack condition):
  - Network of 10 nodes with 2 node registering output out of 3 (as trace sink), one malicious node
  - One road side unit node (non-mobile)
  - Nine vehicle nodes (mobile)
  - Simulation time 100s

Results: Simulation and Results - NS3

Topology

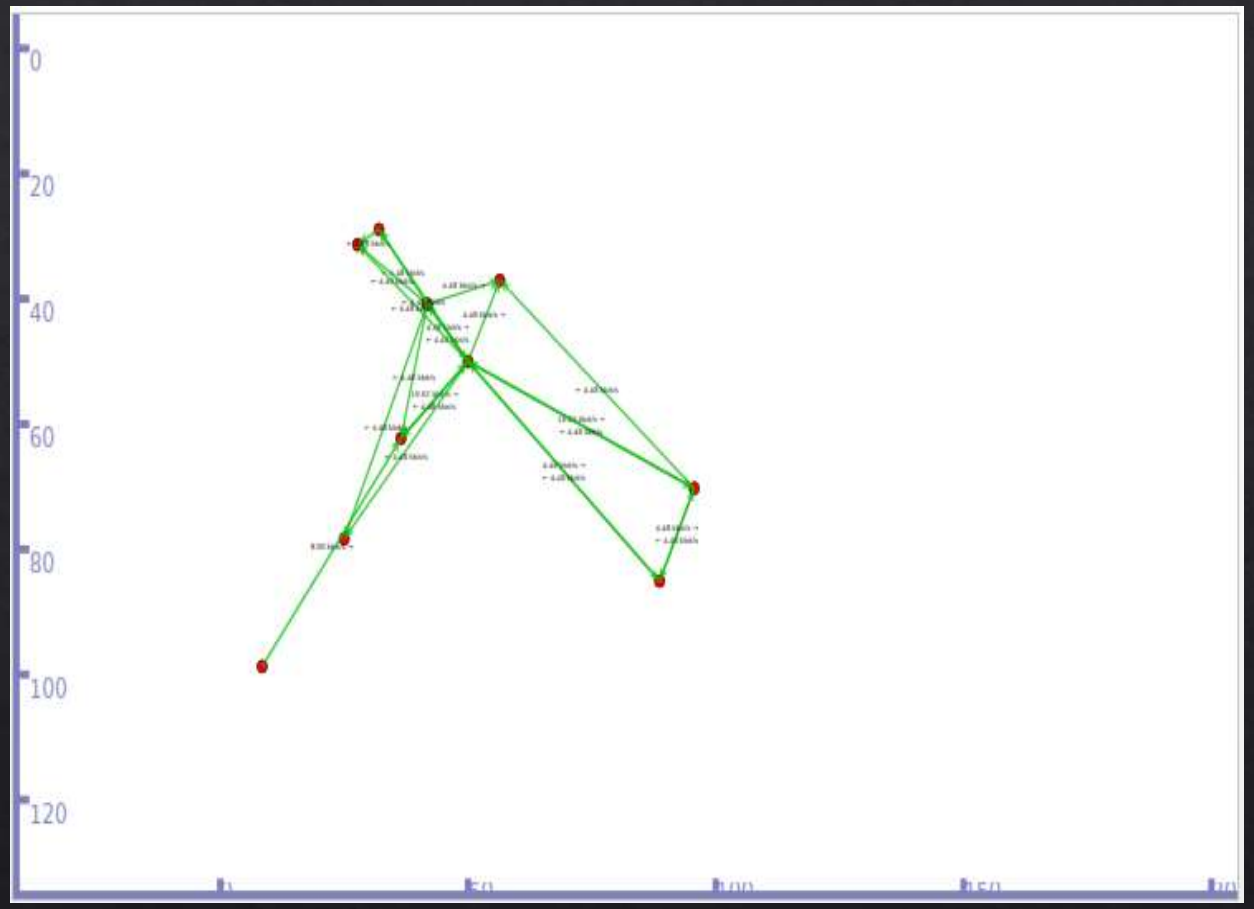

Fig -7 Scenario with 10 nodes

Results: Scenario – Riverbed Modeler

Topology

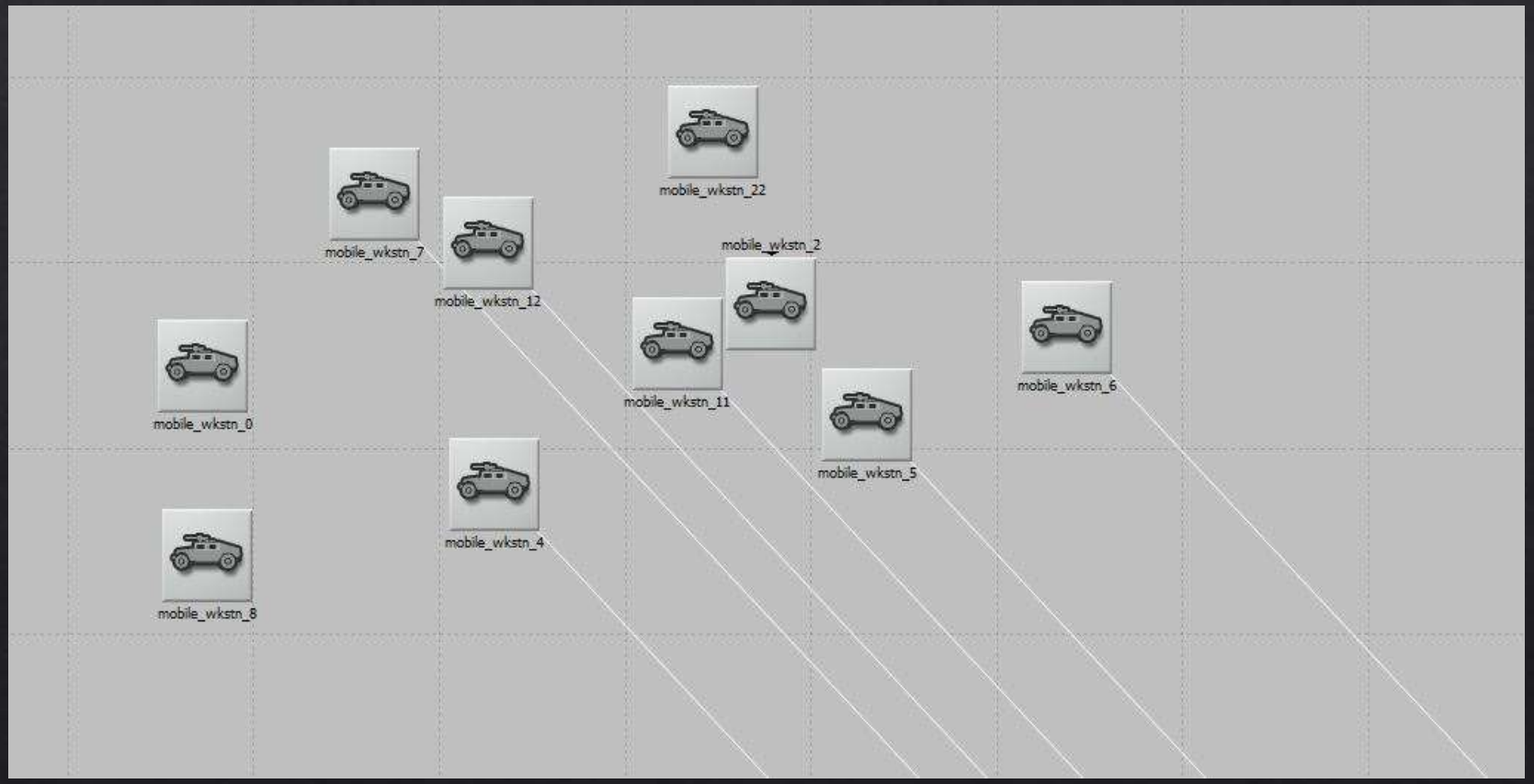

Fig-8 – Scenario with 10 nodes

Results: Simulation in NS3

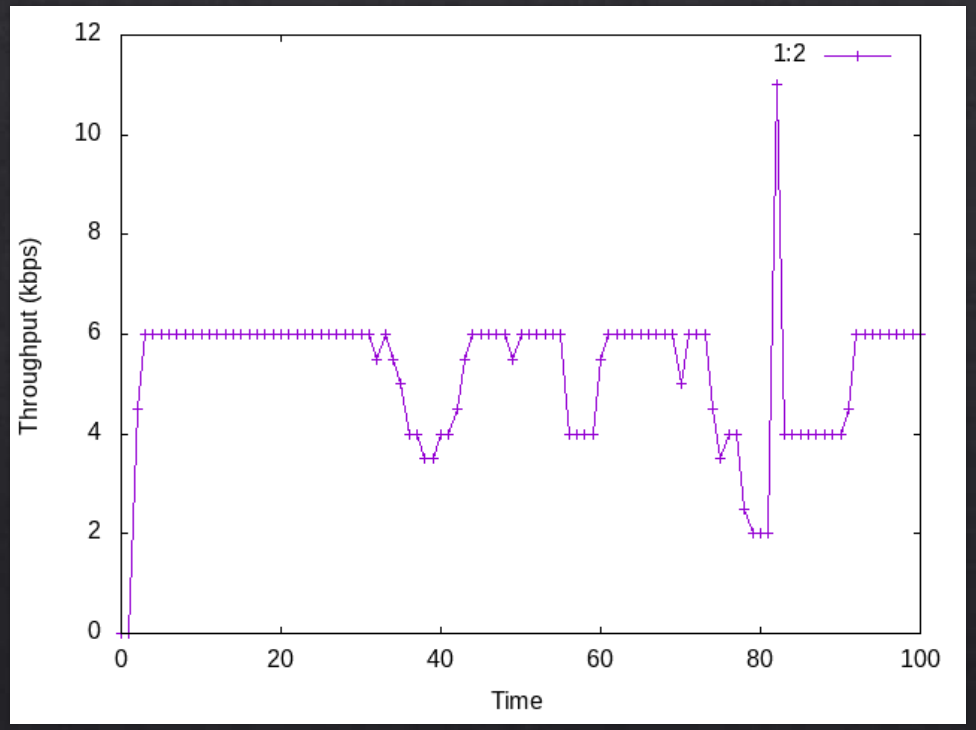

Fig -9 Scenario1_1 – Throughput

Normal condition

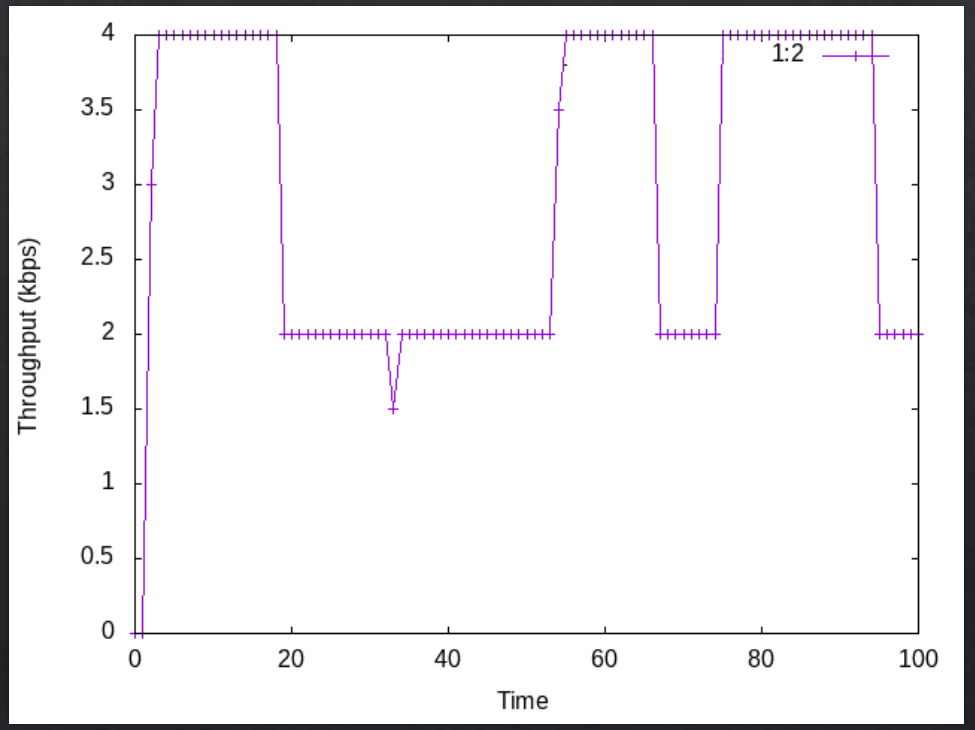

Fig- 10 Scenario1_2 – Throughput under sybil attack

Results: Simulation in NS3 (contd.)

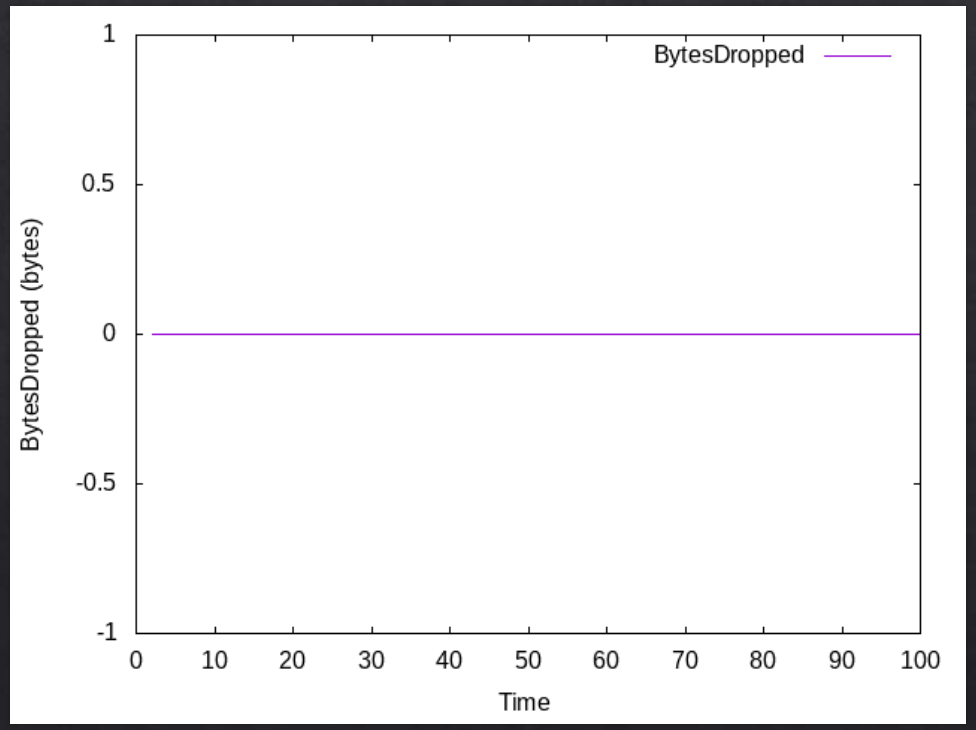

Fig-11 Scenario1_1 – Bytes Dropped in normal condition

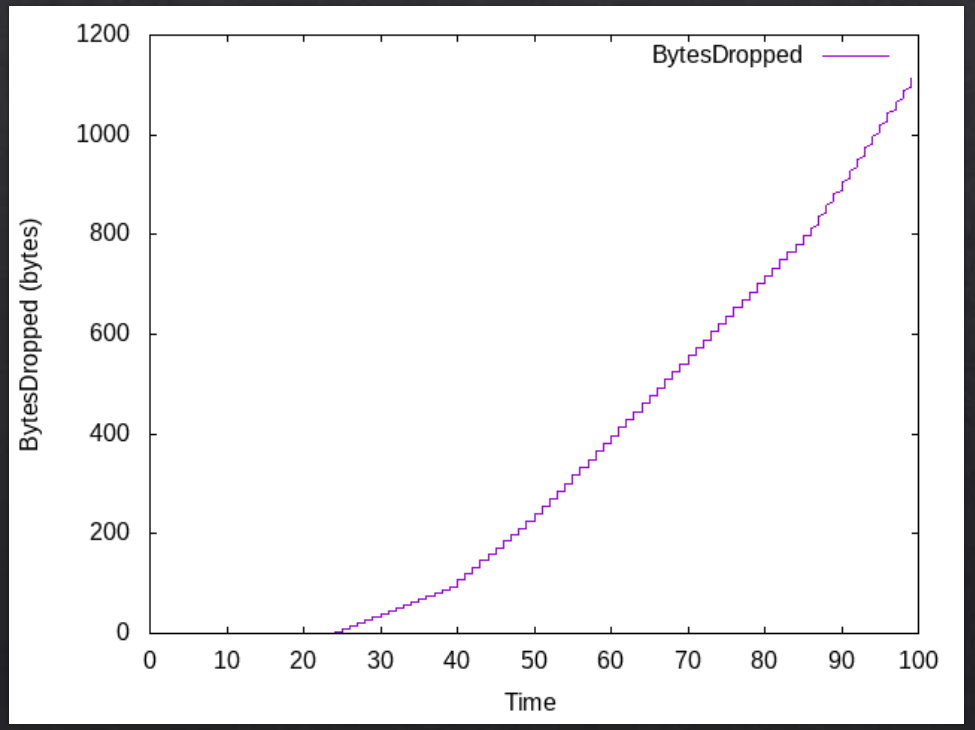

Fig -12 Scenario1_2 – Bytes Dropped under sybil attack

Results: Simulation comparison

Below we did initial comparison of Throughput with NS3 and Riverbed Modeler

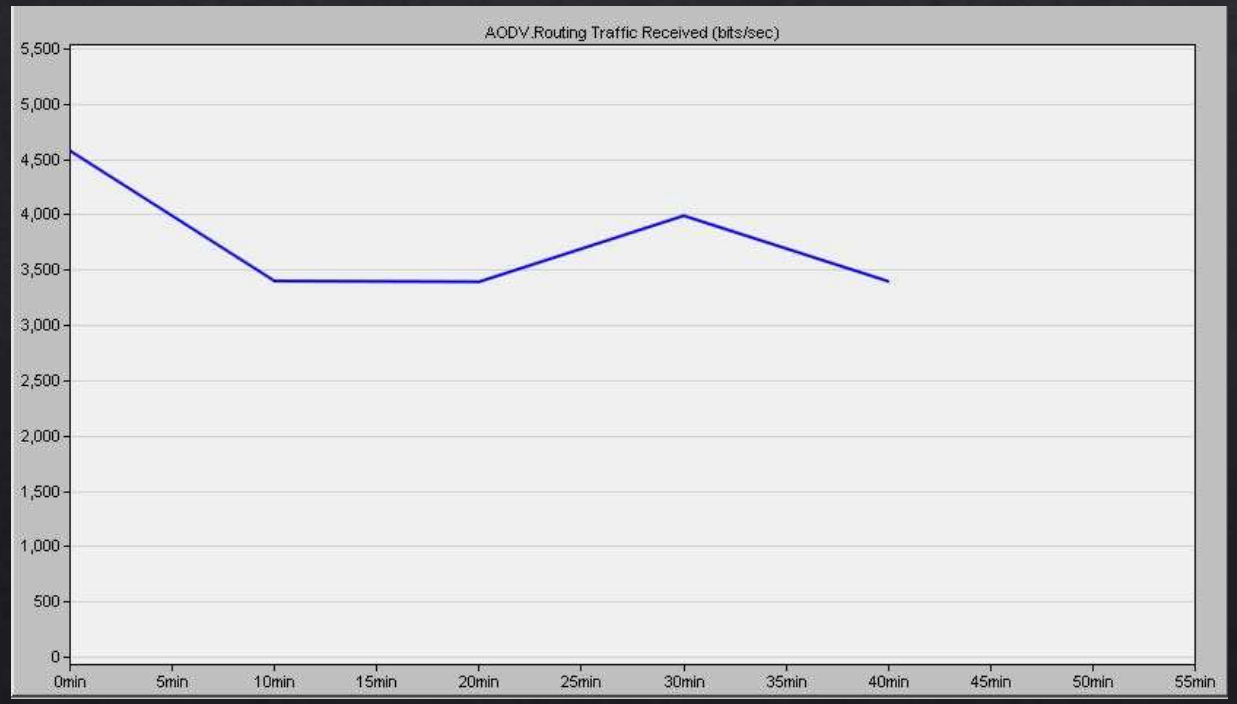

Fig-13 Throughput in Riverbed

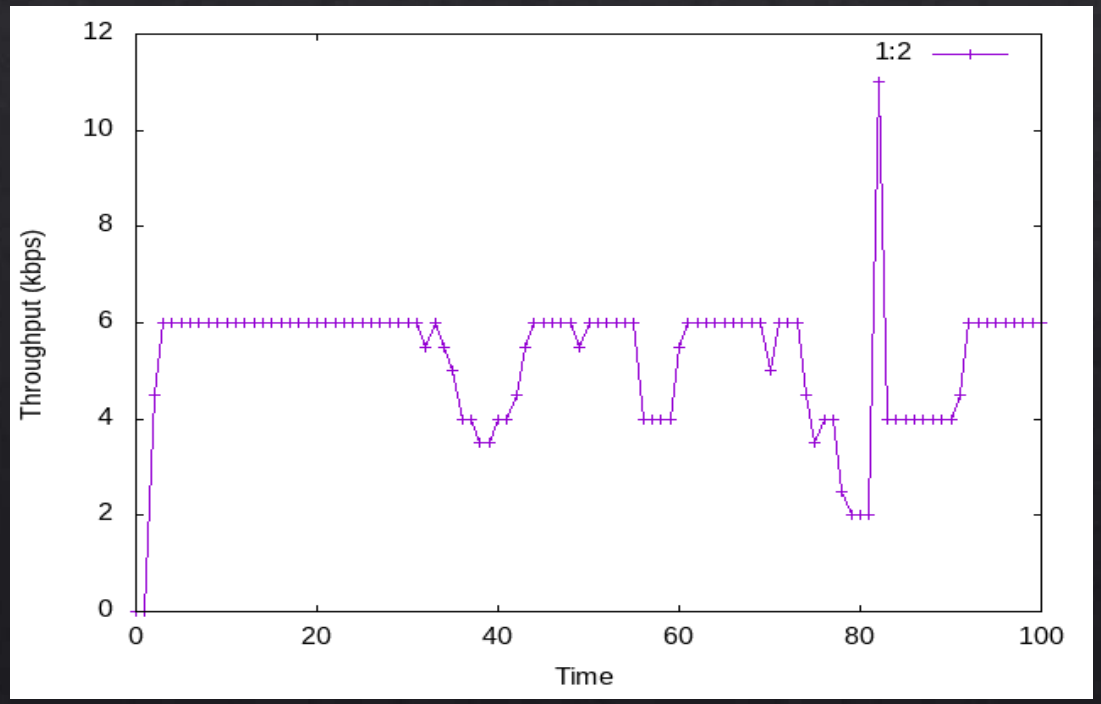

Fig-14Throughput in NS3

Analysis and Learning

- Created topology for VANET in network simulator-3 and simulated scenarios for network output under Sybil attack
- We can observe the decrease in overall throughput when network is under attack. This is because of multiple nodes communicating with infected node are affected
- We can also observe the packet drops are more likely in network under attack
- The severity of the attack depends on number of infected nodes, high number of infected nodes will decrease output more and increase packet drop
- Initial comparison result of NS-3 802.11p topology and Riverbed 802.11a topology shows close result. Some further tuning of parameters in riverbed required for better comparison
- Clearly network under attack can experience channel disruption, packet loss and can result in consequences such as traffic mismanagement, loss of efficiency and in severe case accidents

Analysis and Learning (contd.)

- Develop key insight in working of VANET and how this technology can shape the way for future traffic management and intelligent transportation
- Develop insights of the Sybil attack, how it affects the network and what can be observed consequences and behavior of network under this attack and some ideas proposed for its detection and prevention
- Required lots of reading for ns-3 modules, its classes, objects and techniques to develop topologies and most importantly gather useful data from simulations

Difficulties and Future Works

- Little support on network simulator is available for vehicular ad-hoc networks as it is still developing technology
- Simulation was not carried out with large scale scenario i.e. > 50 nodes due to hardware capability limitation
- Develop more realistic scenarios by implementing topology using trace files from Simulation of Urban Mobility (SUMO), Open street maps which than can be incorporated in NS-3
- More comprehensive simulations can be carried out with more parameters such as different modulation schemes, routing algorithms and large scale topology
- Other behavior of network can be simulated under Sybil attack such as replication of valid node (each replicate posing as valid node), more specific cases such as node communicating directly with malicious node and see its output (we did for a general case where malicious node is random)

References

[1] S. U. Rehman, M. A. Khan, T. A. Zia, L. Zheng, “Vehicular Ad-Hoc Networks (VANETS) – An overview and Challenges”, *Journal of Wireless Networking and Communications,* January 2013, 3(3):29-38 [1]

[2] P. Gu, R. Khatoun, Y. Begriche, A. Serhrouchni, “k-Nearest Neighbours Classification Based Sybil Attack Detection in Vehicular Networks”, *TELECOM ParisTech*, Universit´e Paris-Saclay, 75013, Paris, France

[3] S. Park, B. Aslam, D. Turgut, C. C. Zou, “Defense Against Sybil Attack in Vehicular Ad Hoc Network Based on Roadside Unit Support”, School of Electrical Engineering and Computer Science University of Central Florida, Paper ID# 900042

[4] G. Guette and B. Ducourthial, “On the Sybil attack detection in VANET,” Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems, 2007

[5] T. Zhou, R.R. Choudhury, P. Ning and K. Chakrabarty, “Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks,” Proc. of International Conference on MobiQuitous 2007, pp. 1-8, 2007

[6]N. Sun, “Performance Study of IEEE 802.11p for Vehicle to Vehicle Communications Using Opnet”, M. S. thesis, Massey University, Auckland, NZ, Nov.2011

[7] J. Grover, M.S. Gaur and V. Laxmi, “Sybil Attacks in VANETs: Detection and Prevention”, in Security of Self organizing networks: MANET, WSN,WMN, VANET, A. S. K. Pathhan, CRC Press, Taylor & Francis Group, USA, Jan.2010, pp.269-294