



University Transportation Research Center - Region 2

Final Report



Securing Inter-Vehicular Networks with Time and Driver Identity Considerations

Performing Organization: New York Institute of Technology



December 2018



Sponsor:
University Transportation Research Center - Region 2

University Transportation Research Center - Region 2

The Region 2 University Transportation Research Center (UTRC) is one of ten original University Transportation Centers established in 1987 by the U.S. Congress. These Centers were established with the recognition that transportation plays a key role in the nation's economy and the quality of life of its citizens. University faculty members provide a critical link in resolving our national and regional transportation problems while training the professionals who address our transportation systems and their customers on a daily basis.

The UTRC was established in order to support research, education and the transfer of technology in the field of transportation. The theme of the Center is "Planning and Managing Regional Transportation Systems in a Changing World." Presently, under the direction of Dr. Camille Kamga, the UTRC represents USDOT Region II, including New York, New Jersey, Puerto Rico and the U.S. Virgin Islands. Functioning as a consortium of twelve major Universities throughout the region, UTRC is located at the CUNY Institute for Transportation Systems at The City College of New York, the lead institution of the consortium. The Center, through its consortium, an Agency-Industry Council and its Director and Staff, supports research, education, and technology transfer under its theme. UTRC's three main goals are:

Research

The research program objectives are (1) to develop a theme based transportation research program that is responsive to the needs of regional transportation organizations and stakeholders, and (2) to conduct that program in cooperation with the partners. The program includes both studies that are identified with research partners of projects targeted to the theme, and targeted, short-term projects. The program develops competitive proposals, which are evaluated to insure the most responsive UTRC team conducts the work. The research program is responsive to the UTRC theme: "Planning and Managing Regional Transportation Systems in a Changing World." The complex transportation system of transit and infrastructure, and the rapidly changing environment impacts the nation's largest city and metropolitan area. The New York/New Jersey Metropolitan has over 19 million people, 600,000 businesses and 9 million workers. The Region's intermodal and multimodal systems must serve all customers and stakeholders within the region and globally. Under the current grant, the new research projects and the ongoing research projects concentrate the program efforts on the categories of Transportation Systems Performance and Information Infrastructure to provide needed services to the New Jersey Department of Transportation, New York City Department of Transportation, New York Metropolitan Transportation Council, New York State Department of Transportation, and the New York State Energy and Research Development Authority and others, all while enhancing the center's theme.

Education and Workforce Development

The modern professional must combine the technical skills of engineering and planning with knowledge of economics, environmental science, management, finance, and law as well as negotiation skills, psychology and sociology. And, she/he must be computer literate, wired to the web, and knowledgeable about advances in information technology. UTRC's education and training efforts provide a multidisciplinary program of course work and experiential learning to train students and provide advanced training or retraining of practitioners to plan and manage regional transportation systems. UTRC must meet the need to educate the undergraduate and graduate student with a foundation of transportation fundamentals that allows for solving complex problems in a world much more dynamic than even a decade ago. Simultaneously, the demand for continuing education is growing – either because of professional license requirements or because the workplace demands it – and provides the opportunity to combine State of Practice education with tailored ways of delivering content.

Technology Transfer

UTRC's Technology Transfer Program goes beyond what might be considered "traditional" technology transfer activities. Its main objectives are (1) to increase the awareness and level of information concerning transportation issues facing Region 2; (2) to improve the knowledge base and approach to problem solving of the region's transportation workforce, from those operating the systems to those at the most senior level of managing the system; and by doing so, to improve the overall professional capability of the transportation workforce; (3) to stimulate discussion and debate concerning the integration of new technologies into our culture, our work and our transportation systems; (4) to provide the more traditional but extremely important job of disseminating research and project reports, studies, analysis and use of tools to the education, research and practicing community both nationally and internationally; and (5) to provide unbiased information and testimony to decision-makers concerning regional transportation issues consistent with the UTRC theme.

Project No(s):

UTRC/RF Grant No: 49198-33-28

Project Date:

December 2018

Project Title:

Securing Inter-Vehicular Networks with Time and Driver Identity Considerations

Project's Website:

<http://www.utrc2.org/research/projects/securing-inter-vehicular-networks>

Principal Investigator(s):

Wenjia Li, Ph.D.

Assistant Professor

Department of Computer Science

New York Institute of Technology (NYIT)

1855 Broadway

EGGC 807

New York, NY 10023

Tel: (212) 261-1500

Email: wli20@nyit.edu

Co-Principal Investigator(s):

Nabi Sertac Artan, Ph.D.

Assistant Professor

Department of Electrical and Computer Engineering

New York Institute of Technology (NYIT)

1855 Broadway

EGGC 803A

New York, NY 10023

Tel: (212) 261-1732

Email: nartan@nyit.edu

Performing Organization(s):

New York Institute of Technology (NYIT)

Sponsor(s):

University Transportation Research Center (UTRC)

To request a hard copy of our final reports, please send us an email at utrc@utrc2.org

Mailing Address:

University Transportation Research Center

The City College of New York

Marshak Hall, Suite 910

160 Convent Avenue

New York, NY 10031

Tel: 212-650-8051

Fax: 212-650-8374

Web: www.utrc2.org

Board of Directors

The UTRC Board of Directors consists of one or two members from each Consortium school (each school receives two votes regardless of the number of representatives on the board). The Center Director is an ex-officio member of the Board and The Center management team serves as staff to the Board.

City University of New York

Dr. Robert E. Paaswell - Director Emeritus of NY
Dr. Hongmian Gong - Geography/Hunter College

Clarkson University

Dr. Kerop D. Janoyan - Civil Engineering

Columbia University

Dr. Raimondo Betti - Civil Engineering
Dr. Elliott Sclar - Urban and Regional Planning

Cornell University

Dr. Huaizhu (Oliver) Gao - Civil Engineering
Dr. Richard Geddes - Cornell Program in Infrastructure Policy

Hofstra University

Dr. Jean-Paul Rodrigue - Global Studies and Geography

Manhattan College

Dr. Anirban De - Civil & Environmental Engineering
Dr. Matthew Volovski - Civil & Environmental Engineering

New Jersey Institute of Technology

Dr. Steven I-Jy Chien - Civil Engineering
Dr. Joyoung Lee - Civil & Environmental Engineering

New York Institute of Technology

Dr. Nada Marie Anid - Engineering & Computing Sciences
Dr. Marta Panero - Engineering & Computing Sciences

New York University

Dr. Mitchell L. Moss - Urban Policy and Planning
Dr. Rae Zimmerman - Planning and Public Administration

(NYU Tandon School of Engineering)

Dr. John C. Falcocchio - Civil Engineering
Dr. Kaan Ozbay - Civil Engineering
Dr. Elena Prassas - Civil Engineering

Rensselaer Polytechnic Institute

Dr. José Holguín-Veras - Civil Engineering
Dr. William "Al" Wallace - Systems Engineering

Rochester Institute of Technology

Dr. James Winebrake - Science, Technology and Society/Public Policy
Dr. J. Scott Hawker - Software Engineering

Rowan University

Dr. Yusuf Mehta - Civil Engineering
Dr. Beena Sukumaran - Civil Engineering

State University of New York

Michael M. Fancher - Nanoscience
Dr. Catherine T. Lawson - City & Regional Planning
Dr. Adel W. Sadek - Transportation Systems Engineering
Dr. Shmuel Yahalom - Economics

Stevens Institute of Technology

Dr. Sophia Hassiotis - Civil Engineering
Dr. Thomas H. Wakeman III - Civil Engineering

Syracuse University

Dr. Baris Salman - Civil Engineering
Dr. O. Sam Salem - Construction Engineering and Management

The College of New Jersey

Dr. Thomas M. Brennan Jr - Civil Engineering

University of Puerto Rico - Mayagüez

Dr. Ismael Pagán-Trinidad - Civil Engineering
Dr. Didier M. Valdés-Díaz - Civil Engineering

UTRC Consortium Universities

The following universities/colleges are members of the UTRC consortium under MAP-21 ACT.

City University of New York (CUNY)
Clarkson University (Clarkson)
Columbia University (Columbia)
Cornell University (Cornell)
Hofstra University (Hofstra)
Manhattan College (MC)
New Jersey Institute of Technology (NJIT)
New York Institute of Technology (NYIT)
New York University (NYU)
Rensselaer Polytechnic Institute (RPI)
Rochester Institute of Technology (RIT)
Rowan University (Rowan)
State University of New York (SUNY)
Stevens Institute of Technology (Stevens)
Syracuse University (SU)
The College of New Jersey (TCNJ)
University of Puerto Rico - Mayagüez (UPRM)

UTRC Key Staff

Dr. Camille Kamga: *Director, Associate Professor of Civil Engineering*

Dr. Robert E. Paaswell: *Director Emeritus of UTRC and Distinguished Professor of Civil Engineering, The City College of New York*

Dr. Ellen Thorson: *Senior Research Fellow*

Penny Eickemeyer: *Associate Director for Research, UTRC*

Dr. Alison Conway: *Associate Director for Education/Associate Professor of Civil Engineering*

Nadia Aslam: *Assistant Director for Technology Transfer*

Nathalie Martinez: *Research Associate/Budget Analyst*

Andriy Blagay: *Graphic Intern*

Tierra Fisher: *Office Manager*

Dr. Sandeep Mudigonda, *Research Associate*

Dr. Rodrigue Tchamna, *Research Associate*

Dr. Dan Wan, *Research Assistant*

Bahman Moghimi: *Research Assistant;*
Ph.D. Student, Transportation Program

Sabiheh Fagigh: *Research Assistant;*
Ph.D. Student, Transportation Program

Patricio Vicuna: *Research Assistant*
Ph.D. Candidate, Transportation Program

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle Securing Inter-Vehicular Networks with Time and Driver Identity Considerations		5. Report Date 12/19/2018	
		6. Performing Organization Code	
7. Author(s) Wenjia Li, Ph.D. Nabi Sertac Artan, Ph. D.		8. Performing Organization Report No.	
9. Performing Organization Name and Address New York Institute of Technology 1855 Broadway New York, NY, 10023		10. Work Unit No.	
		11. Contract or Grant No. 49198 33 28	
12. Sponsoring Agency Name and Address UTRC The City College of New York, Marshak Hall 910 West 137th Street and Convent Avenue New York, NY 10031		13. Type of Report and Period Covered Final,	
		14. Sponsoring Agency Code	
15. Supplementary Notes			
16. Abstract <p>The exchange of information in a timely fashion is critical to accident prevention in transportation systems. Research has demonstrated that anticipating future collisions by as little as half a second before impact could lead to a 60% decrease in traffic accidents. Moreover, in July of 2015, researchers demonstrated a remote exploit of a commercially available vehicle from 10 miles away while it was on the highway, leading to the recall 1.4 million vehicles; this represents the first known automotive recall due to a cyber-security vulnerability. However, the exchange of information also makes vehicular networks prone to security-related issues. In this research project, we conduct research to address the security issues in vehicular networks. First, we perform a literature review on the attack surface and the corresponding countermeasures for vehicular networks. Then, we study one specific attack, the packet dropping attack, which is a common security threat for vehicular networks, and propose an approach to detect the packet dropping attack. To validate the proposed approach, experiments have been conducted based on network simulation.</p>			
17. Key Words Accident Prevention, Collision, Traffic, Vehicles, Cyber-security. Vehicular networks, simulation.		18. Distribution Statement	
19. Security Classif (of this report) Unclassified	20. Security Classif. (of this page)	21. No of Pages 24	22. Price

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. The contents do not necessarily reflect the official views or policies of the UTRC, New York Institute of Technology, or the Federal Highway Administration. This report does not constitute a standard, specification or regulation. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, in the interest of information exchange. The U.S. Government New York Institute of Technology assume no liability for the contents or use thereof.

Acknowledgment

The author gratefully acknowledges individuals who contributed towards this research project. Dr. Wenjia Li was the lead principal investigator (PI) of this project along with two Co-Principal Investigators (Co-PIs); Dr. Nabi Sertac Artan, an Assistant Professor of Electrical and Computer Engineering at NYIT, and Dr. Dr. Jonathan Voris, formerly an Assistant Professor at NYIT. Dr. Voris moved to a different institution in the middle of this project, therefore Dr. Li graciously ratify Dr. Voris's research efforts in the beginning of this project and would also consent contributions from Dr. Artan.

Executive Summary

The exchange of information in a timely fashion is critical to accident prevention in transportation systems. Research has demonstrated that anticipating future collisions by as little as half a second before impact could lead to a 60% decrease in traffic accidents. Moreover, in July of 2015, researchers demonstrated a remote exploit of a commercially available vehicle from 10 miles away while it was on the highway, leading to the recall 1.4 million vehicles; this represents the first known automotive recall due to a cyber security vulnerability. However, the exchange of information also makes vehicular networks prone to security-related issues. In this research project, we conduct research to address the security issues in vehicular networks. First, we perform a literature review on the attack surface and the corresponding countermeasures for vehicular networks. Then, we study one specific attack, the packet dropping attack, which is a common security threat for vehicular networks, and propose an approach to detect the packet dropping attack. To validate the proposed approach, experiments have been conducted based on network simulation.

Background

In recent years, there have been some research efforts on gathering and analyzing sensing data to help improve safety and efficiency in Transportation Cyber-Physical Systems (TCPS). However, most of the existing approaches merely consider using the data from a single sensing infrastructure. At the same time, there are a wide variety of sensing infrastructures that generate a significant amount of heterogeneous sensing data, such as road-side infrastructure sensors, in-vehicle on-board sensors, and sensors embedded in mobile devices. Due to security, trust and privacy concerns, these heterogeneous types of data have not been shared across different infrastructures, thus limiting their usage in practice. For instance, in the traffic accident alert application, it may not be sufficient to rely only on the road-side infrastructure sensors to report any traffic congestion or accident because of the limited coverage and availability of those sensors. In this case, the data sensed by the in-vehicle on-board sensors and the embedded sensors in mobile devices become complementary and important.

The aforementioned research efforts do not generally align with the goal of TCPS, which is the seamless interoperability of a rich set of sensors embedded in vehicles, roadside units and in many other infrastructures with a wide range of computing platforms, from smartphones to cloud servers, through a variety of communication mechanisms. A successful and ideal TCPS will allow many smart and scalable solutions to solve some of the major problems that urban societies are facing nowadays including high fatalities in traffic accidents, excessive time and emission costs brought by traffic congestions, and efficient allocation of parking spaces especially in major metropolitan areas such as New York City. However, the practicality of such a TCPS is challenged by (1) stakeholders with different and often conflicting security, trust, and privacy requirements, (2) the demands of real-time data intensive computing and communication, and (3) a high level of variation in the types of technologies that could be deployed [25].

Therefore, it is critical to formalize the study of TCPS security. More specifically, we aim at researching the security aspects of inter-vehicle (Vehicle-to-Vehicle, or V2V) and Vehicle-to-Infrastructure (V2I) communication - i.e., messages which are exchanged between multiple vehicles or vehicles and roadside assets through vehicular networks.

Objectives

The primary objective of this project is to explore how organizations can take full advantage of current heterogeneous sensing platforms by sharing and analyzing sensor data from different infrastructures in a secure and trustworthy manner. More specifically, we first investigate attacks against transportation systems, and then seek for solutions to cope with these attacks. We intend to formalize the study of potential attack vectors against vehicular systems and develop a more comprehensive taxonomy of the attack surface of these networks. Identifying this attack surface will allow us to prioritize issues according to their severity. Beyond studying the vulnerabilities present in these systems, we will also look into potential defenses against the attacks which we have discovered.

Introduction

This project aims at enhancing the security of inter-vehicular networks by detecting and coping with the potential security threats that are common in inter-vehicular networks. More specifically, we look into the Blackhole attack that is a well-known security threat, and seek to work out a solution to detect its presence with high packet delivery ratio and low time overhead. To ensure that the proposed solution meets the expectations, we conduct some experiments based on network simulation to validate the proposed solution.

Summary of the Literature Review

In vehicular networks, high mobility of vehicles raises the security challenge for cars and sensors [1]. Some sensors (e.g., road sensors) are deployed in unattended or even harsh environments and the lack of tamper-resistance hardware increases the possibility to be compromised by adversaries. Once compromised, the adversary can manipulate information, posing serious threats to transportation system. For example, the false traffic alert injected by compromised sensors can lead to incorrect decision made by transportation infrastructure, leading to traffic congestion or collision [2]. The detailed literature review results that we obtained could be found in the Section “Task 1: Literature Review on Security Issues and Countermeasures for Vehicular Networks”.

Summary of the Work Performed

This report summarizes the research efforts performed as part of our UTRC supported project entitled “Securing Inter-Vehicular Networks with Time and Driver Identity Considerations” which has recently been brought to a successful conclusion. The main goal of this project was to identify the security threats in vehicular networks and develop technical solutions to detect and cope with these security threats so that the overall security and safety of the road transportation system could be enhanced.

An outline which briefly summarizes each of the research tasks we completed during the course of this project is given below:

- Performing a comprehensive literature review of the security issues and their countermeasures for vehicular networks,
- Identifying possible network simulation software to utilize in our research study and assessing the feasibility of the network simulation software,
- Development of a preliminary network simulation scenario without malicious attacks,
- Investigating the possibility of injecting malicious attacks into the network simulation scenario,
- Develop a solution which can detect the malicious attack that is injected into the scenario, and
- Conducting experimental study to validate the proposed solution in network simulation.

The remainder of this section of the final report will provide details on each of these accomplishments.

Task 1: Literature Review on Security Issues and Countermeasures for Vehicular Networks

In general, the security issues in vehicular networks can be addressed by two categories of solutions: (1) attack detection and prevention, and (2) trust establishment and management. Some recent research findings on each of these two categories are summarized below.

➤ Attack detection and prevention for vehicular networks

In [3], an intrusion detection scheme is studied for vehicular networks, in which social clustering algorithm is used to detect and isolate malicious vehicles. More specifically, a cluster-based approach was developed to detect malicious vehicles, which took into account the vehicles' features such as their velocity, the dynamic network topology, scalability and also the vehicles' trust level.

Chang et al. proposed a location-hidden authorized message generation scheme to detect and cope with Sybil attacks for vehicular networks [4]. In this scheme, two authorized messages will be generated when a vehicle approaches a Road Side Unit (RSU), and the RSU signatures on these two messages are signer ambiguous so that the RSU location information will not be disclosed from the resulted authorized messages. At the same time, the two authorized messages signed by the same RSU within the same given period of time (which is known to be temporarily linkable) are recognizable so that they can be used for identification. By this means, the trajectories of Sybil attackers can be identified and the location privacy of each vehicle can be preserved.

In [5], Guo et al. studied a misbehavior detection scheme to detect Blackhole and Greyhole attacks for vehicular delay tolerant networks. The Blackhole and Greyhole attacks can be detected by collecting and securely exchanging data of previous encounters among vehicles.

Dias et al. proposed a cooperative watchdog system for vehicular delay tolerant networks to detect and act against misbehaving nodes in order to reduce their impact in the overall network performance [6]. To achieve the goal of misbehaving node detection, a cooperative exchange of nodes' reputation along the network is performed so that each node is aware of how trustworthy its neighbors are.

In [7], Yao et al. proposed a novel Sybil attack detection method based on Received Signal Strength Indicator (RSSI), namely Voiceprint, for VANETs. Unlike most of existing RSSI-based Sybil attack methods, Voiceprint adopts RSSI time series as vehicular speech and compares the similarity among all received series. Moreover, Voiceprint does not rely on any predefined radio propagation model, and conducts independent detection without the support of centralized nodes. Extensive simulations and real-world experiments have demonstrated the effectiveness of Voiceprint.

A jamming attack detection method for vehicular networks was discussed in [8], in which the authors proposed a real-time Medium-Access-Control-based (MAC-based) detection method to meet the requirements of safety applications in vehicular networks, and the proposed method can more accurately distinguish between failed transmissions, such as contention collisions, interferences, and jamming attacks. Consequently, the jamming attacks are detected with a lower probability of false alarms.

In [9], a decentralized trust management system in vehicular networks was proposed based on blockchain. In this system, vehicles can validate the received messages from neighboring vehicles using the Bayesian Inference Model. Based on the validation result, the vehicle will generate a rating for each vehicle. With the ratings uploaded from vehicles, Roadside Units (RSUs) calculate the trust value offsets of involved vehicles and pack these data into a "block". Then, each RSU will try to add their "blocks" to the trust blockchain which is maintained by all the RSUs.

➤ Trust management for securing vehicular networks

It is well known that trust management is an important solution to safeguard vehicular networks. In general, the concept of trust management refers to the idea in which various behaviors of nodes in vehicular networks are observed, recorded and assessed, and then these behaviors are used to build a trust for each node based on the behavior assessment.

In [10], the authors evaluated both probabilistic and deterministic approaches (individually and combined) to estimate trust for enhancing VANET security. More specifically, the probabilistic approach determines the trust level of the peer vehicles based on the received information. The trust level is used to determine legitimacy of the message, which is used to decide whether the message would be considered for further

transmission over the VANET or dropped. The deterministic approach measures the trust level of the received message by using distances calculated using received signal strength (RSS) and the vehicle's geolocation (position coordinate). Combination of probabilistic and deterministic approach gives better results compared to individual approaches.

Chuang and Lee [11] studied a decentralized lightweight authentication scheme named trust-extended authentication mechanism (TEAM) for vehicle-to-vehicle communication networks. TEAM adopts the concept of transitive trust relationships to improve the performance of the authentication procedure and only needs a few storage spaces.

Rostamzadeh et al. [12] proposed a trust-based information dissemination framework for vehicular networks, which is composed of two successive modules. The first module applies three security checks to make sure the message is trusted. More specifically, it assigns a trust value to each road segment and one to each neighborhood, instead of each car. Once a message is evaluated and considered to be trustworthy, the second module looks for a safe path through which the message is forwarded. Experimental results demonstrate that this framework outperforms other well-known routing protocols since it routes the messages via trusted vehicles.

Kerrache et al. proposed a novel trust establishment architecture which is fully compliant with the ETSI ITS standard, which takes advantage of the periodically exchanged beacons (i.e. CAM) and event triggered messages (i.e. DENM). The proposed solution, called T-VNets [13], allows estimating the traffic density, the trust among entities, as well as the dishonest nodes distribution within the network. In addition, by combining different trust metrics such as direct, indirect, event-based and RSU-based trust, T-VNets is able to eliminate dishonest nodes from all network operations while selecting the best paths to deliver legal data messages.

To address the security issues in vehicular ad hoc networks, Li and Song proposed ART [2], an attack-resistant trust management scheme, which is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles; node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively.

In [14], an accurate and lightweight intrusion detection framework named AECFV is proposed to secure vehicular networks. In this framework, the clustering algorithm is used to group the nodes together according to both node's mobility and network vulnerability. Moreover, clusters are constructed with a high stability and good connectivity. Cluster-Heads (CHs) are elected based on both node's mobility and the vehicle's trust-level.

Kumar and Chilamkurti proposed a Trust aware Collaborative Learning Automata based Intrusion Detection System (T-CLAIDS) for Vehicular Ad hoc Networks (VANETs) [15]. In the T-CLAIDS system, Learning Automata (LA) is deployed on vehicles in VANETs to

capture the information about the different states of the vehicles on the road. A Markov Chain Model (MCM) is then constructed for representation of states and their transitions in the network. Transitions from one state to another are dependent upon the density of the vehicles in a particular region. In addition, a new classifier is designed for detection of any malicious activity in the network and is tuned based upon the new parameter called as Collaborative Trust Index (CTI) so that it covers all possible types of attacks in the network. An algorithm for detection of abnormal events using the defined classifier is also proposed.

In [16], an adversary-oriented survey of the existing trust models for VANETs is conducted. The authors also show in this survey when trust is preferable to cryptography, and vice versa. In addition, how trust models are usually evaluated in VANET contexts is discussed as well. Finally, the authors point out some critical scenarios that existing trust models cannot handle, together with some possible solutions.

Haddadou et al. [17] attempted to cope with malicious nodes, which aim to spread false and forged data, and selfish nodes, which cooperate only for their own benefit. To address both of these two types of security threats, a distributed trust model named *DTM²* is proposed, which is adapted from the job market signaling model.

Task 2: Identification and Evaluation of Network Simulators

We have initiated our investigation into potentially viable network simulators for our research study. The primary network simulation platform that we explored was NS-3 (Network Simulator 3) [18].

As the first pilot study, we have explored two types of network topology settings in NS-3. The first network topology is pre-defined in NS-3 with 11 wireless nodes. Figure 1 below shows the network topology #1. At the beginning of the simulation, each node will be placed according to the pre-defined square location.

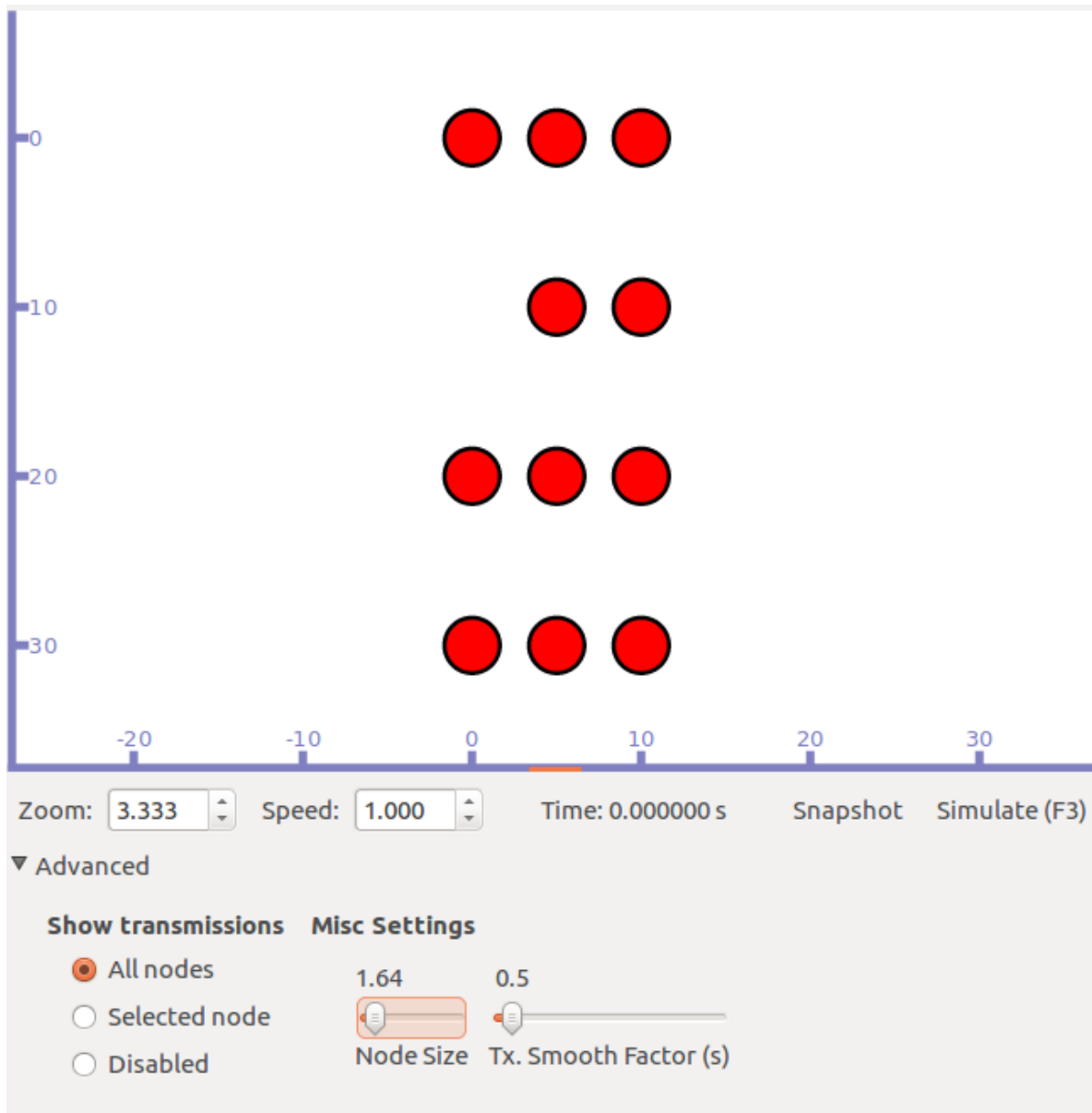


Figure 1. NS-3 Network Topology #1 (Prior to simulation)

During the network simulation, each node is able to move according to the network mobility model, and they also exchange network data packets while moving. Figure 2 shows the exchange of network data packets during the simulation. It is worthwhile to note that the location of these nodes has changes when compared to their initial positions as shown in Figure 1.

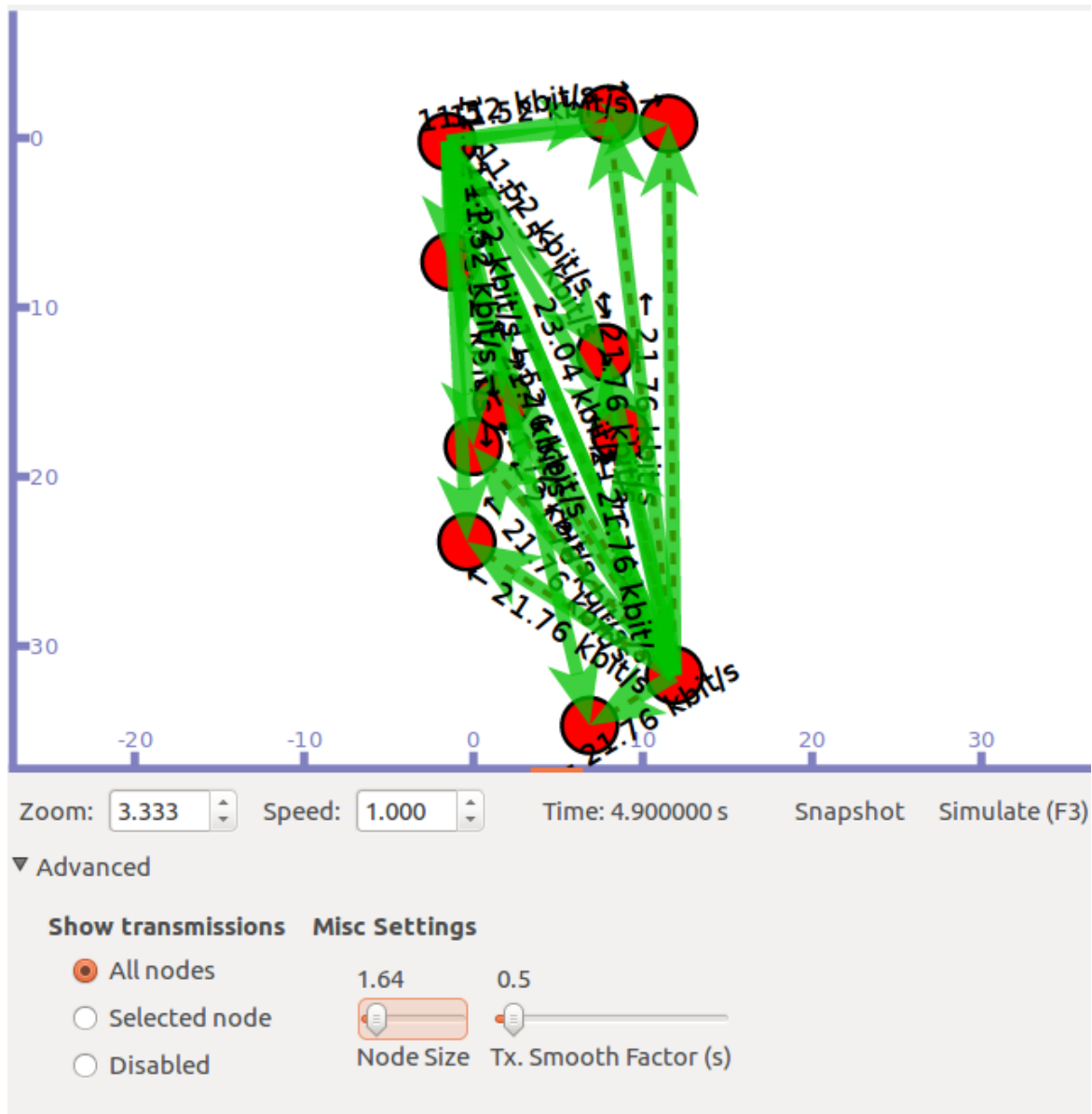


Figure 2. NS-3 Network Topology #1 (During the simulation)

Figure 3 shows the wireless network topology when the simulation ends, which shows that the network topology has changed when compared to Figure 1 and 2.

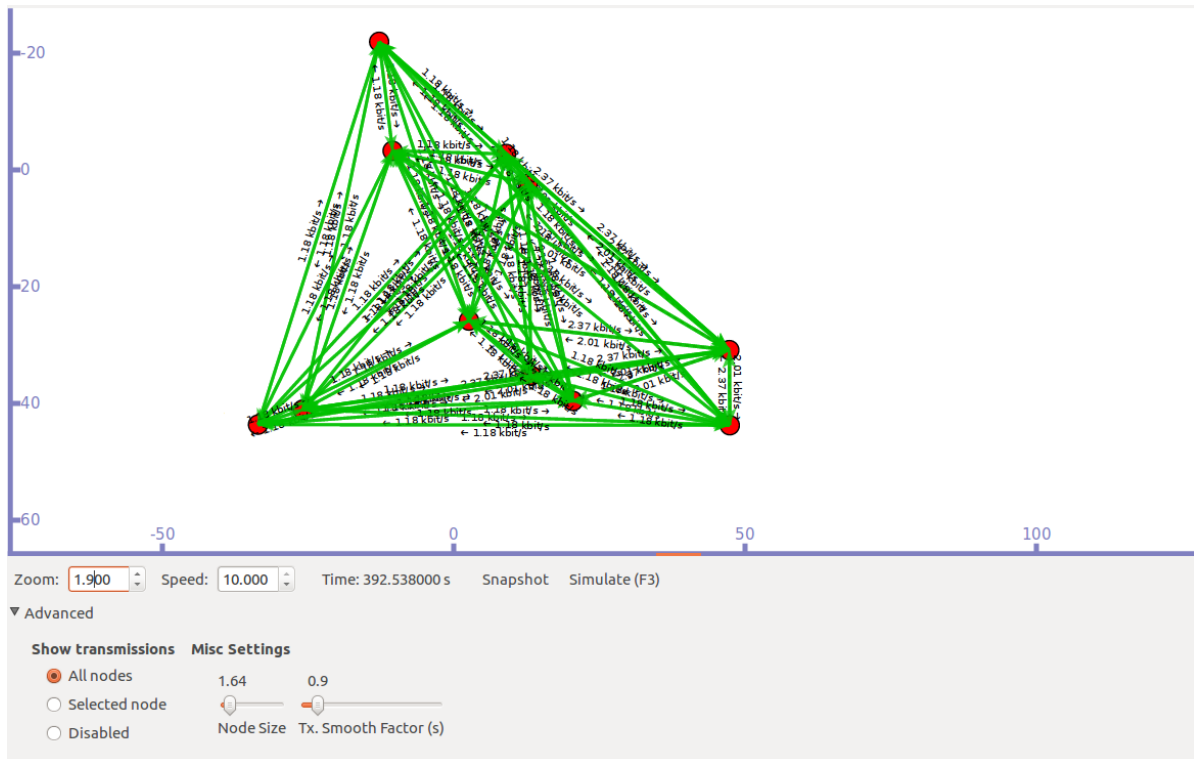


Figure 3. NS-3 Network Topology #1 (At the end of simulation)

The goal of the second NS-3 experiment is to allow users customize the simulation parameters, such as the number of nodes, the number of malicious nodes, network mobility model, simulation duration, etc. As a result, we simulate the following network topology which is composed of 90 nodes as per the user-defined parameters. Figure 4 demonstrates the user-defined parameter file.

```

Open ▾ [+]
No_of_Nodes 90
Malicious 0
Distance_in_X_axis 100
Distance_in_Y_axis 100
Total_time 15
Random_or_constant 0|

```

Figure 4. User-defined Parameter for NS-3 Network Topology #2

As shown in Figure 4, there are 90 nodes which are randomly placed in a defined region, and the duration of the simulation is 15 seconds.

Figure 5 depicts the NS-3 Network Topology #2 prior to the simulation. As we can see, a total number of 90 nodes are spaced out in a defined region 100 meters apart in the X-axis and Y-axis.

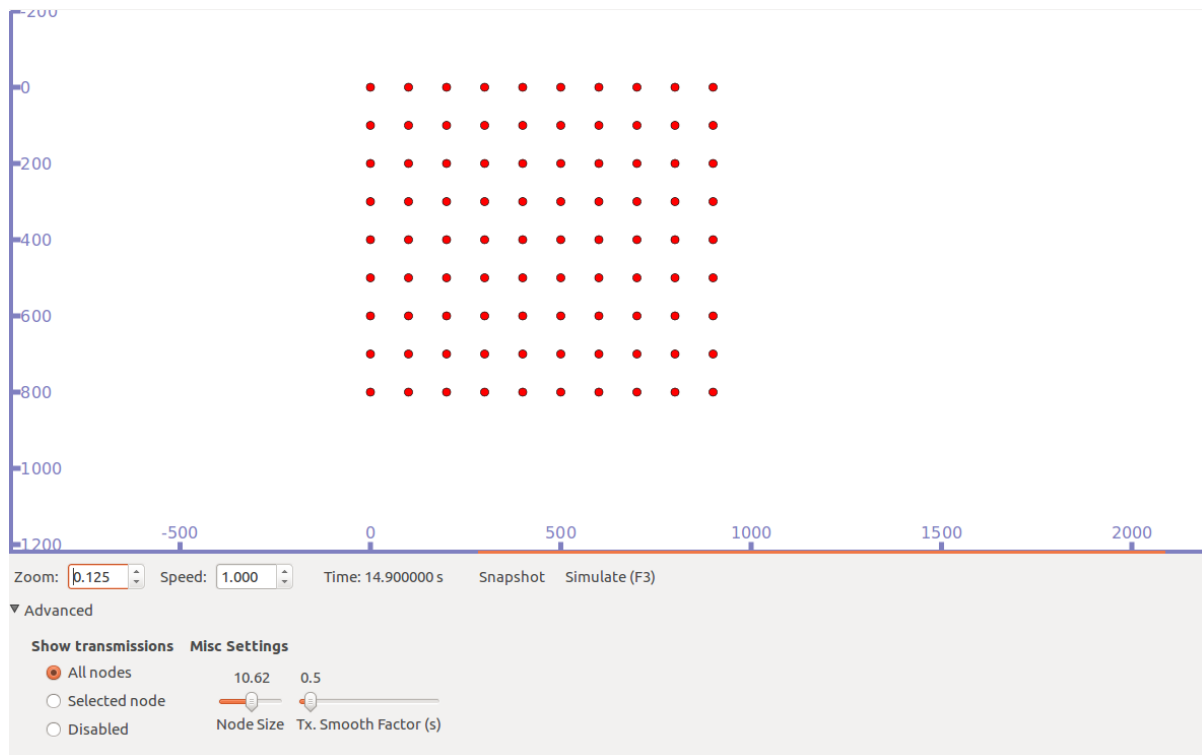


Figure 5. NS-3 Network Topology #2 (Prior to simulation)

Figure 6 demonstrates the network topology during the simulation. From Figure 6, we can clearly notice that each node is sending packets to all the adjacent nodes and this done by using an NS-3 mechanism named the “MobilityHelper”.

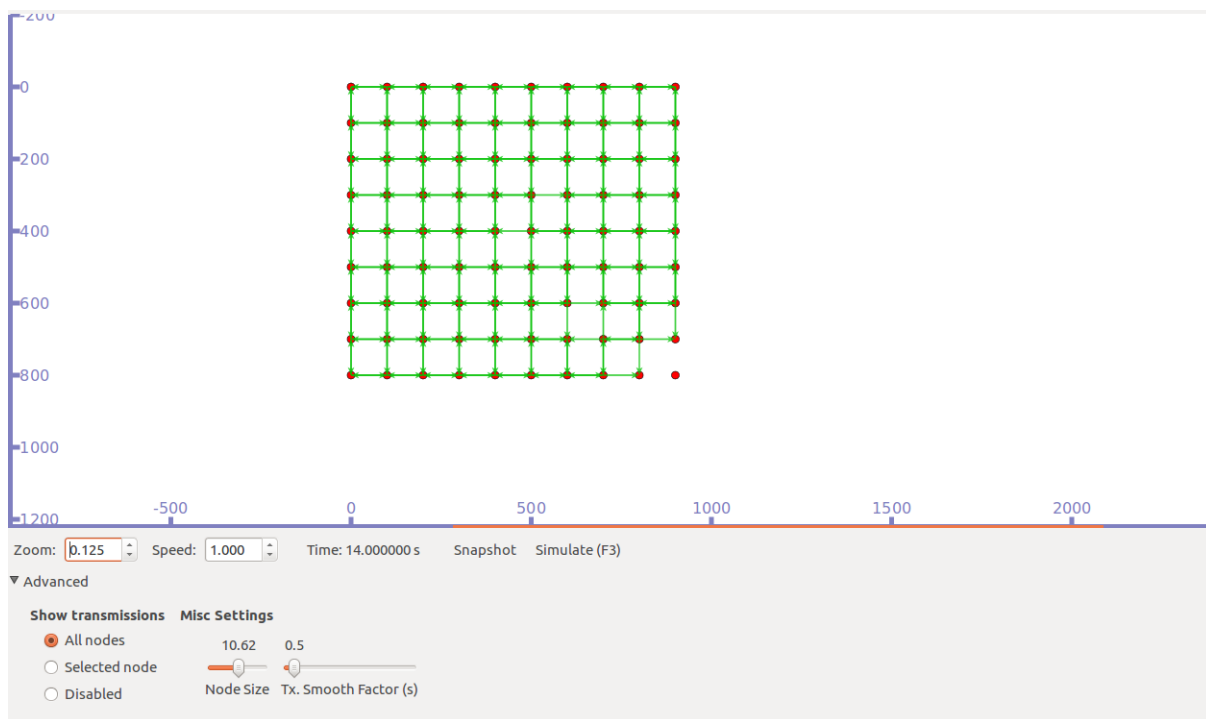


Figure 6. NS-3 Network Topology #2 (During the simulation)

Based on the first pilot study on NS-3 network simulator, we found that it is an appropriate network simulation tool for us to conduct the research study. Given that it is a widely used and accepted network simulation tool in academic research, we decided to use NS-3 for this research project.

In addition to conducting the first pilot study of network simulation to better understand the principles of NS-3 and how to customize the simulation parameters, we also look into how we can possibly define the network mobility model so that it can better reflect the real vehicular networks.

In this regards, we first explore using OpenStreetMap [19], which is an online tool to generate a given map of the user's choice (Figure 7).

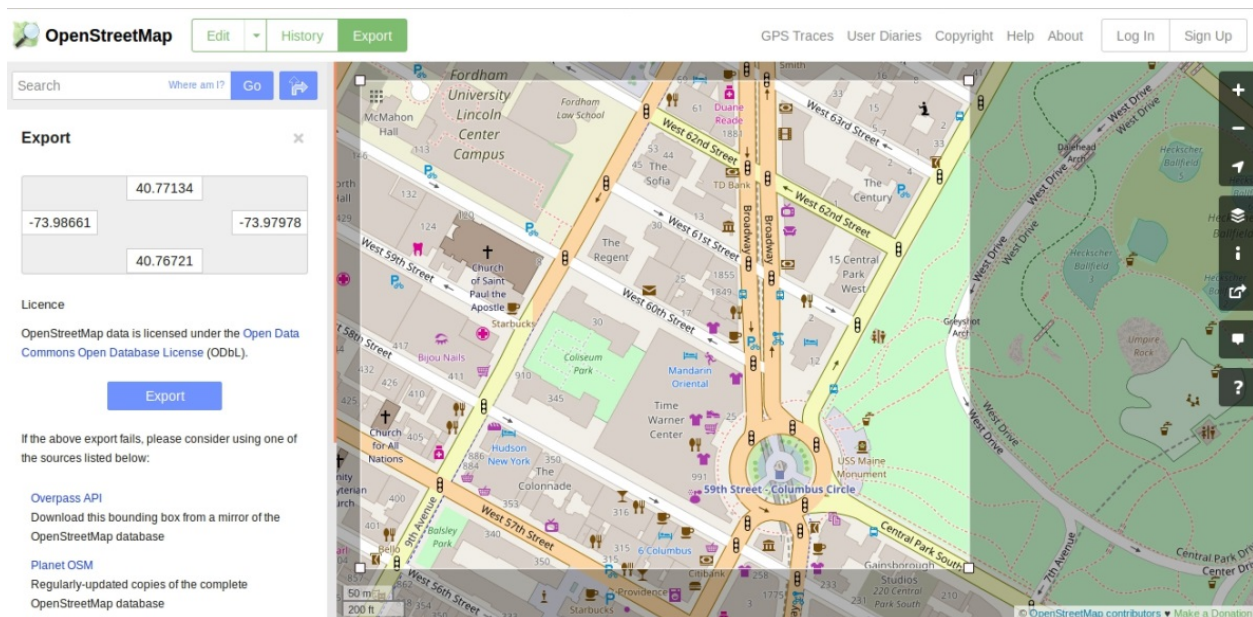


Figure 7. An Example of OpenStreetMap

After we generate the OpenStreetMap file, we load the map file into a tool named SUMO [20] to generate the mobility model, which is shown in Figure 8.

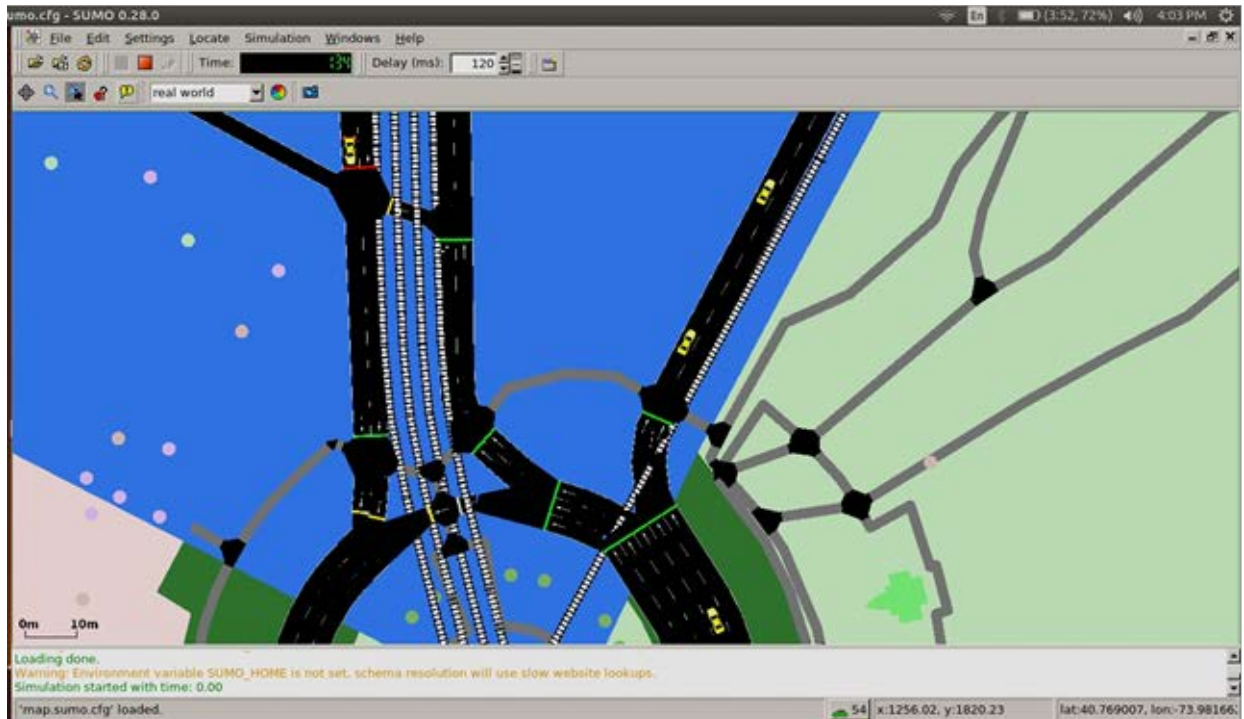


Figure 8. The Network Mobility Model generated by SUMO Tool

Based on our research investigation into OpenStreetMap and SUMO, we decided that the tedious task of generating elaborate map files and mobility models using these tools goes beyond the scope of the primary focus of this research project. Therefore, we decided to use the mobility models that are currently embedded in the NS-3 itself, which are more than adequate for the main research tasks.

Task 3: Development of a Vehicle to Vehicle (V2V) Network Simulation without Malicious Attacks

In this research task, we implemented a network simulation to study the feasibility of simulating a Vehicle to Vehicle (V2V) network with the node's mobility model as "Random Waypoint". As a key feature of the V2V networks, mobility model plays an important role in properly simulating a realistic V2V network. In this task, we built a V2V network with 10 vehicular nodes, and demonstrated that they were mobile according to the random waypoint model. The screen shots of the simulation are shown in Figures 9, 10, and 11.

The Random Waypoint model is a widely used mobility model in mobile networks [21]. In this mobility model, each of the mobile nodes will move according to the following principle: at the beginning of the simulation, the node will remain stationary for a fixed period of time. After that time period ends, the node then selects a random destination within the simulation area and a random speed between 0 (excluded) and a pre-defined maximum speed. The node moves to this destination at the randomly chosen speed and again stay stationary for another fixed time period before another random location and speed are chosen. This behavior is repeated for the whole duration of the network simulation [22].

```
n-w@nw-VirtualBox: ~/Desktop/ns-allinone-3.26/ns-3.26
n-w@nw-VirtualBox:~/Desktop/ns-allinone-3.26/ns-3.26$ ./waf --run scratch/aodv_r
andomwp --vis
Waf: Entering directory `/home/n-w/Desktop/ns-allinone-3.26/ns-3.26/build'
Waf: Leaving directory `/home/n-w/Desktop/ns-allinone-3.26/ns-3.26/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (3.610s)
Creating 10 nodes 100 m apart.
Starting simulation for 10 s ...
Could not load icon applets-screenshooter due to missing gnomedesktop Python module
scanning topology: 10 nodes...
scanning topology: calling graphviz layout
scanning topology: all done.
```

Figure 9. NS-3 Simulation Log at the Beginning of the Simulation

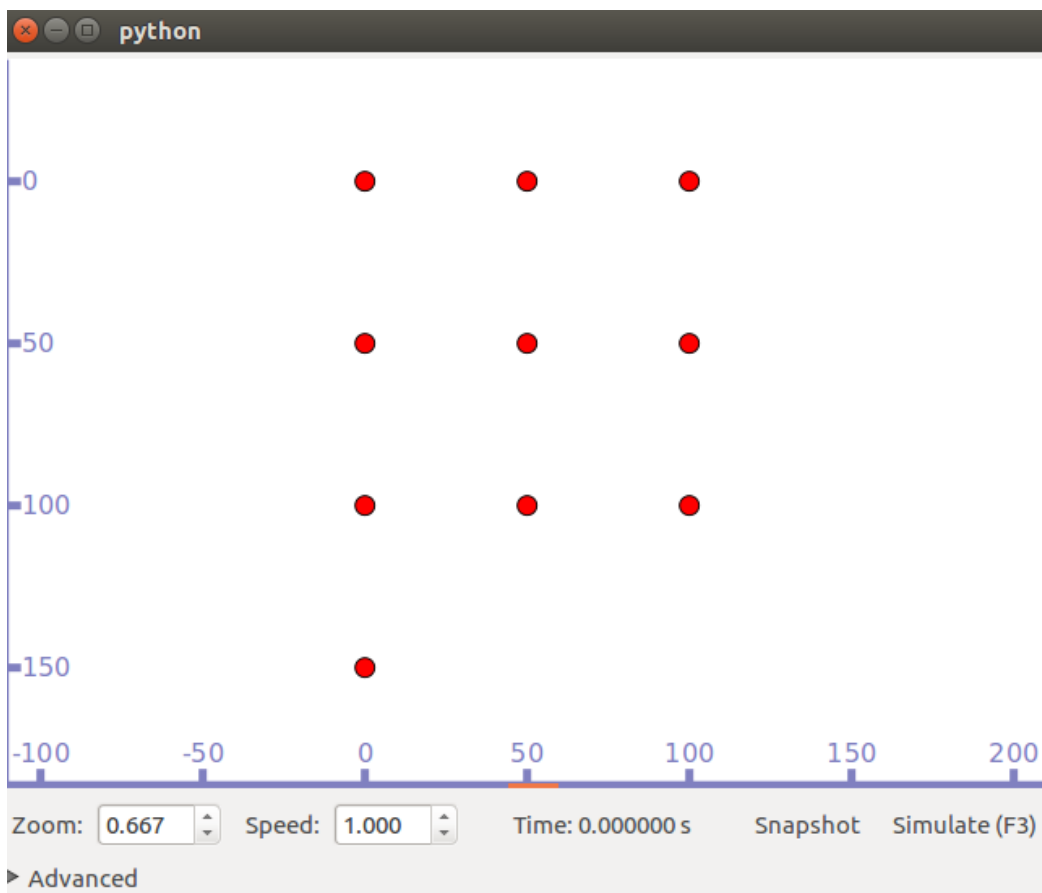


Figure 10. Initial Placement of Nodes in the V2V network

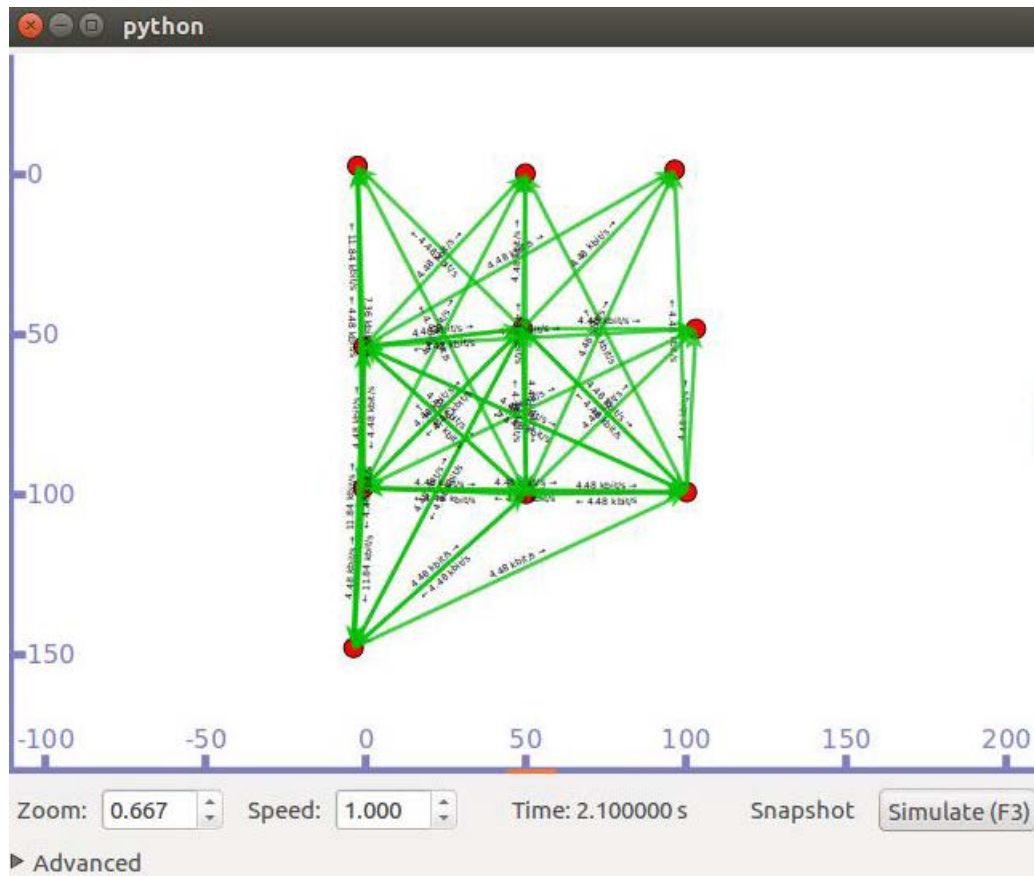


Figure 11. A Snapshot of the V2V Network during the NS-3 Simulation

Figure 9 demonstrates the process by which we start the NS-3 network simulation, and we can find that some of the real-time status information is also shown in the log of the simulation platform, which could help us keep track of what is happening during the simulation. Figure 10 shows the initial placement of nodes in the V2V network, and we can see that there are 10 nodes that are placed in a grid structure. Figure 11 depicts the V2V network at the time 2.1 second after the simulation starts. The green lines represent the occurrence of V2V communication in terms of network packet exchanges.

Task 4: Injection of Malicious Attacks into V2V Network Simulation

In this research task, we aim at introducing malicious attacks (behaviors) into the V2V network simulation. The malicious attack that we at first attempted to inject was a well-known routing misbehavior that misuses the RREQ/RREP mechanism in V2V networks.

One of the most widely-used routing protocols in vehicular networks is the Ad hoc On-Demand Distance Vector (AODV) protocol [23]. In the AODV protocol, the two key types of network packets are the RREQ (Route Request) and RREP (Route Reply) packets. When a node needs to send out some actual data packets to another node without knowing the route to the destination, it will first send out the RREQ packet to perform route discovery. Once it gets back the RREP, it will have a better knowledge on which

immediate neighboring node it should send the packet to. The following diagram shows how the RREQ/RREP mechanism works.

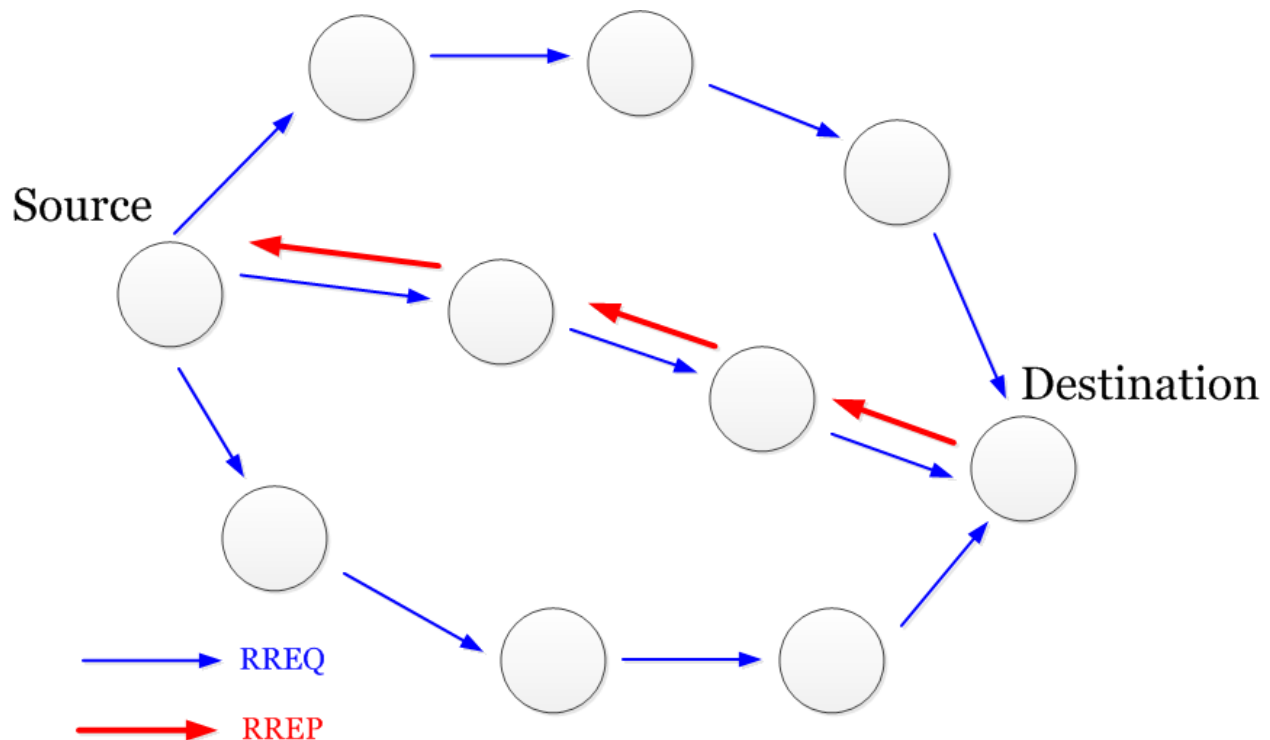


Figure 12. An Example of Route Discovery in AODV Protocol Using RREQ and RREP

From Figure 12 when the source node wants to communicate with the destination node, due to the long distance between them, the source node has to rely on other intermediate nodes to relay the data packets for it. Without the knowledge of which node it should relay the packets to, the source node will first have to initiate a route discovery process by sending out the RREQ packets to all its neighbors. If a node receives the RREQ packet, it has two options: if it knows how to directly reach the destination, it will send the RREP packet back to the source node; otherwise it will forward the RREQ packets to its neighbors.

However, the RREQ/RREP mechanism could also be misused by adversaries who can drop/modify the RREQ/RREP packets so that the route discovery fails. This is also known as one type of Blackhole attack [24]. Thus, we explore the possibility of introducing malicious behaviors in terms of dropping RREQ/RREP packets.

The output of the NS-3 simulation that demonstrates the presence of RREQ/RREP packet dropping misbehaviors is shown below.

```

asus@asus-N53SM: ~/Desktop/ns-allinone-3.26/ns-3.26
asus@asus-N53SM:~/Desktop/ns-allinone-3.26/ns-3.26$ ./waf --run scratch/aodv_drop_packet
Waf: Entering directory `/home/asus/Desktop/ns-allinone-3.26/ns-3.26/build'
[2258/2649] Compiling scratch/aodv_drop_packet.cc
[2638/2649] Linking build/scratch/aodv_drop_packet
Waf: Leaving directory `/home/asus/Desktop/ns-allinone-3.26/ns-3.26/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (6.750s)
0 received one packet from 10.1.1.11 at 0.555658 seconds
2 received one packet from 10.1.1.13 at 0.597819 seconds
1 received one packet from 10.1.1.12 at 0.772165 seconds
0 received one packet from 10.1.1.11 at 0.780566 seconds
2 received one packet from 10.1.1.13 at 0.850055 seconds
6 received one packet from 10.1.1.17 at 0.897576 seconds
---Malicious Node: Packet dropped
---Malicious Node: Packet dropped
1 received one packet from 10.1.1.12 at 1.01763 seconds
5 received one packet from 10.1.1.16 at 1.02641 seconds
0 received one packet from 10.1.1.11 at 1.03503 seconds
2 received one packet from 10.1.1.13 at 1.08351 seconds
---Malicious Node: Packet dropped
6 received one packet from 10.1.1.17 at 1.13514 seconds
7 received one packet from 10.1.1.18 at 1.18387 seconds
3 received one packet from 10.1.1.14 at 1.25895 seconds

```

Figure 13. Demonstration of Packet Dropping Misbehaviors at the Beginning of Simulation

```

asus@asus-N53SM: ~/Desktop/ns-allinone-3.26/ns-3.26
2 received one packet from 10.1.1.13 at 1.82933 seconds
---Malicious Node: Packet dropped
6 received one packet from 10.1.1.17 at 1.88514 seconds
7 received one packet from 10.1.1.18 at 1.92491 seconds
1 received one packet from 10.1.1.12 at 2.01763 seconds
5 received one packet from 10.1.1.16 at 2.02102 seconds
0 received one packet from 10.1.1.11 at 2.03085 seconds
3 received one packet from 10.1.1.14 at 2.05089 seconds
2 received one packet from 10.1.1.13 at 2.08011 seconds
---Malicious Node: Packet dropped
6 received one packet from 10.1.1.17 at 2.16275 seconds
7 received one packet from 10.1.1.18 at 2.19854 seconds
1 received one packet from 10.1.1.12 at 2.28725 seconds
---Malicious Node: Packet dropped
2 received one packet from 10.1.1.13 at 2.33286 seconds
6 received one packet from 10.1.1.17 at 2.39943 seconds
5 received one packet from 10.1.1.16 at 2.52312 seconds
0 received one packet from 10.1.1.11 at 2.53663 seconds
1 received one packet from 10.1.1.12 at 2.53728 seconds
0 received one packet from 10.1.1.11 at 2.57833 seconds
8 received one packet from 10.1.1.19 at 2.57993 seconds
---Malicious Node: Packet dropped
2 received one packet from 10.1.1.13 at 2.58195 seconds
3 received one packet from 10.1.1.14 at 2.63636 seconds

```

Figure 14. Demonstration of Packet Dropping Misbehaviors during the Simulation


```
asus@asus-N53SM: ~/Desktop/ns-allinone-3.26/ns-3.26
3 received one packet from 10.1.1.14 at 3.30081 seconds
2 received one packet from 10.1.1.13 at 3.32933 seconds
--Malicious Node: Packet dropped
6 received one packet from 10.1.1.17 at 3.38514 seconds
--Malicious Node: Packet dropped
1 received one packet from 10.1.1.12 at 3.5182 seconds
5 received one packet from 10.1.1.16 at 3.52102 seconds
0 received one packet from 10.1.1.11 at 3.53087 seconds
3 received one packet from 10.1.1.14 at 3.54995 seconds
2 received one packet from 10.1.1.13 at 3.57933 seconds
--Malicious Node: Packet dropped
6 received one packet from 10.1.1.17 at 3.63514 seconds
--Malicious Node: Packet dropped
1 received one packet from 10.1.1.12 at 3.76763 seconds
5 received one packet from 10.1.1.16 at 3.77102 seconds
0 received one packet from 10.1.1.11 at 3.78067 seconds
3 received one packet from 10.1.1.14 at 3.80061 seconds
2 received one packet from 10.1.1.13 at 3.83249 seconds
--Malicious Node: Packet dropped
6 received one packet from 10.1.1.17 at 3.88514 seconds
--Malicious Node: Packet dropped
Packets dropped: 24
Packets Delivery Ratio: 83%
asus@asus-N53SM:~/Desktop/ns-allinone-3.26/ns-3.26$
```

Figure 15. Demonstration of Packet Dropping Misbehaviors at the end of the Simulation

We can find from Figures 13, 14 and 15 that the malicious node will drop the packets that travel through it, which may cause severe security issues if not properly detected and handled.

Task 5: Detection of Blackhole Attack in V2V Networks

In general, the Blackhole attacks in V2V networks can be classified into two categories: the **active** Blackhole attack and the **passive** Blackhole attack. In the **active** Blackhole attack, when the adversary receives a RREQ packet, it will immediately respond with a fake RREP packet claiming that it has the shortest route to the destination node (which is not true), thus attracting all the packets to it and then dropping them, which will cause major packet loss. In the **passive** Blackhole attack, the adversary will not falsify any RREP packet so that it may not attract a large amount of network packets. Instead, it will drop some or all of the network packets (such as the RREQ, RREP, or the general data packets) that are forwarded to it. When comparing these two attack strategies, we can find that the active Blackhole may cause more damage to the network, but it is relatively easier to detect because the excessive packet loss can be discovered fairly quickly. On the other hand, the passive Blackhole attack generally causes less damage to the network, but the adversary may stay undetected for a longer period of time which will still be a security threat for the V2V network in the long run.

To cope with both types of the Blackhole attacks in V2V networks, we propose a hybrid detection method which is based on (1) a probing RREQ mechanism and (2) a cooperative trust management mechanism based on neighbor watching.

The probing RREQ mechanism is used to detect the active Blackhole attacker. As shown in Figure 16, one field in the RREQ message is the destination IP address. Because the goal of the active Blackhole attacker is to attract all the network traffic to it, it will generally respond immediately to any RREQ message that it receives with a RREP message to claim that it has the shortest path to the destination. Therefore, based on this observation, we send out a **probing** RREQ message prior to the actual RREQ message, in which the destination IP address is set to be an IP address that is currently **NOT** assigned to any node in the network.

For example, in a V2V network which has 50 mobile nodes, the IP Addresses can be assigned between 10.0.0.1 and 10.0.0.50. In this case the Destination IP Address field in the probing RREQ is set as 10.0.0.99, which is not currently assigned to any node in the network. Although this IP address does not associate with any actual node in the network, the active Blackhole attacker may still respond to it with a RREP message attempting to attract network traffic. On the other hand, the normal (benign) nodes will not respond to this probing RREQ message because they could not identify any neighboring node that has the non-existent IP address as specified in the probing RREQ message. By this means, the active Blackhole attacker could be properly detected and recorded.

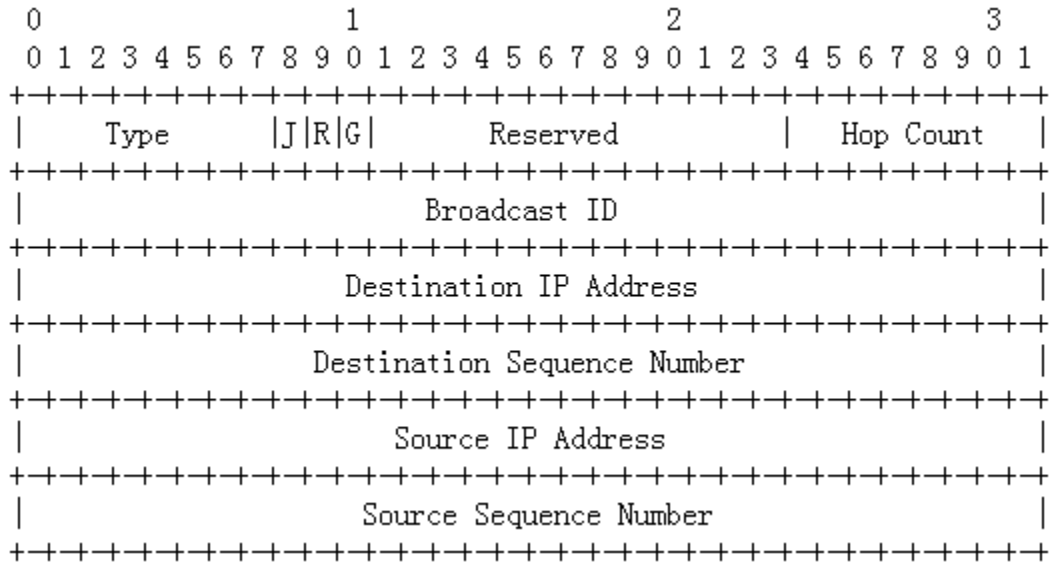


Figure 16. Route Request (RREQ) Message Format [23]

To detect the passive Blackhole attacks in V2V networks, it is essential to closely monitor the packet forwarding process at each hop. Therefore, we propose a trust management mechanism in which each node maintains a list that records the trust score of all its neighboring nodes, and the trust score of each neighboring node is calculated based on how many data packets it has dropped. The less amount of packets it drops, the higher the trust score will be. When the node decides which neighboring node to forward a packet, it will check the trust score of them and make sure that the packet is forwarded to a neighboring node with high trust score. Once the trust score of a neighboring node falls below a given threshold, the neighboring node will be marked as “untrustworthy” and thus be excluded from any successive network operations.

Task 6: Experimental Study for the Detection of Blackhole Attack in V2V Networks

To validate the proposed Blackhole attack detection method, a preliminary experimental study is conducted which is based on NS-3 network simulation. The simulation setup is shown in Table 1 below.

Table 1: Simulation Parameter

Parameter	Value
Routing Protocol	AODV
Simulation Time	600s
Number of Mobile Nodes	40
Number of Active Blackhole Attacker	1, 2, 3
Simulation Area	800 x 500 m
Mobility Model	Random Waypoint

In this simulation, the V2V network is composed of 40 nodes, and the address range is 10.0.0.1 to 10.0.0.40. We set 10.0.0.1 as the source node's IP address and 10.0.0.40 as the destination node's IP address. The initial placement of these nodes is shown in Figure 17.

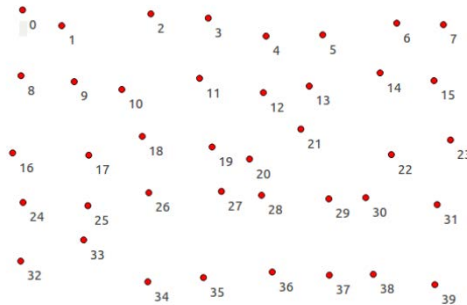


Figure 17. Initial Placement of Forty Mobile Nodes

Due to the limited time that we have, in the preliminary experiment, we only consider the case of active Blackhole attacker, and we use the probing RREQ mechanism to detect it. The network simulation results are shown in Figures 18, 19 and 20.


```

Address: 10.0.0.40the number of received packet is 589
Time:595.305 Node id:6is forwarding packet
Time:595.306 Node id:18is forwarding packet
Time:596.302 Node id:1is forwarding packet
Time:596.303 Node id:23is forwarding packet
Address: 10.0.0.40the number of received packet is 590
Time:596.306 Node id:6is forwarding packet
Time:596.306 Node id:18is forwarding packet
Time:597.302 Node id:1is forwarding packet
Time:597.303 Node id:23is forwarding packet
Address: 10.0.0.40the number of received packet is 591
Time:597.306 Node id:6is forwarding packet
Time:597.306 Node id:18is forwarding packet
Time:598.302 Node id:1is forwarding packet
Time:598.303 Node id:23is forwarding packet
Address: 10.0.0.40the number of received packet is 592
Time:598.305 Node id:6is forwarding packet
Time:598.306 Node id:18is forwarding packet
Time:599.302 Node id:1is forwarding packet
Time:599.303 Node id:23is forwarding packet
Address: 10.0.0.40the number of received packet is 593
Time:599.305 Node id:6is forwarding packet
Time:599.306 Node id:18is forwarding packet

```

Figure 18. Simulation Result with One Active Blackhole Attacker

```

Address: 10.0.0.40the number of received packet is 546
Time:595.306 Node id:21is forwarding packet
Time:595.306 Node id:11is forwarding packet
Time:596.304 Node id:11is forwarding packet
Time:596.305 Node id:21is forwarding packet
Address: 10.0.0.40the number of received packet is 547
Time:596.308 Node id:21is forwarding packet
Time:596.308 Node id:11is forwarding packet
Time:597.302 Node id:11is forwarding packet
Time:597.303 Node id:21is forwarding packet
Address: 10.0.0.40the number of received packet is 548
Time:597.305 Node id:21is forwarding packet
Time:597.306 Node id:11is forwarding packet
Time:598.302 Node id:11is forwarding packet
Time:598.303 Node id:21is forwarding packet
Address: 10.0.0.40the number of received packet is 549
Time:598.306 Node id:21is forwarding packet
Time:598.306 Node id:11is forwarding packet
Time:599.302 Node id:11is forwarding packet
Time:599.303 Node id:21is forwarding packet
Address: 10.0.0.40the number of received packet is 550
Time:599.306 Node id:21is forwarding packet
Time:599.306 Node id:11is forwarding packet
aaa@ubuntu:~/tarballs/ns-allinone-3.26/ns-3.26$

```

Figure 19. Simulation Result with Two Active Blackhole Attacker

```

aaa@ubuntu: ~/tarballs/ns-allinone-3.26/ns-3.26
Address: 10.0.0.40the number of received packet is 544
Time:595.306 Node id:5is forwarding packet
Time:595.306 Node id:11is forwarding packet
Time:596.302 Node id:11is forwarding packet
Time:596.303 Node id:31is forwarding packet
Address: 10.0.0.40the number of received packet is 545
Time:596.305 Node id:5is forwarding packet
Time:596.306 Node id:11is forwarding packet
Time:597.302 Node id:11is forwarding packet
Time:597.303 Node id:31is forwarding packet
Address: 10.0.0.40the number of received packet is 546
Time:597.305 Node id:5is forwarding packet
Time:597.306 Node id:11is forwarding packet
Time:598.302 Node id:11is forwarding packet
Time:598.303 Node id:31is forwarding packet
Address: 10.0.0.40the number of received packet is 547
Time:598.306 Node id:5is forwarding packet
Time:598.306 Node id:11is forwarding packet
Time:599.302 Node id:11is forwarding packet
Time:599.303 Node id:31is forwarding packet
Address: 10.0.0.40the number of received packet is 548
Time:599.306 Node id:5is forwarding packet
Time:599.306 Node id:11is forwarding packet
aaa@ubuntu:~/tarballs/ns-allinone-3.26/ns-3.26$

```

Figure 20. Simulation Result with Three Active Blackhole Attacker

In the experiment, we use the following metrics to evaluate the proposed method: the packet delivery ratio and the time taken to detect the active Blackhole attackers. The packet delivery ratio is defined as following:

$$\text{Packet Delivery Ratio} = \frac{\text{Number of packets successfully received by the destination}}{\text{Total number of packets sent by the source}}$$

The experimental results are shown in Tables 2 and 3.

Table 2: Packet Delivery Ratio with Different Number of Active Blackhole Attackers

Number of active Blackhole Attacker	Packet Delivery Ratio
1	98.3%
2	91.7%
3	91.3%

Table 3. Time taken to Detect Active Blackhole Attackers (in second)

Number of active Blackhole Attacker	Time taken to Detect Attackers (s)
1	0.43
2	1.62
3	4.83

From the experimental results we can find that with the probing RREQ mechanism, we can achieve a high packet delivery ratio, which is above 90% with as many as 3 active Blackhole attackers. At the same time, the time taken to detect these attackers is relatively short, which will ensure that the damage due to the attack is limited.

Conclusions and Recommendations

In this project, we tackle the problem of security issues in vehicular networks, and more specifically the Blackhole attacks in V2V networks. We first investigate the nature of Blackhole attack, and identify two categories of Blackhole attacks, namely the active Blackhole attack and the passive Blackhole attack. To address these two types of attacks, we propose a hybrid approach which integrates both the probing RREQ mechanism and the trust management mechanism based on neighbor watching. To validate the proposed approach, a preliminary experimental study has been conducted based on NS-3 network simulation. Experimental results have shown that the proposed approach can successfully detect the active Blackhole attacks, which can guarantee a high packet delivery ratio with a reasonable time cost to detect the attacks.

There are still some research directions that are left to be explored, such as how the driver authentication would affect the overall security of the road transportation system., how we could ensure a timely exchange and processing of information among different entities (including vehicles, RSUs, pedestrians, etc.) given that many of them are in motion, and so on. We would like to re-visit these unexplored research problems in the future if possible.

Implementation and Training

The proposed research idea was validated using NS-3 network simulation. The research finding also partially resulted the preparation and submission of a research grant proposal to the National Science Foundation (NSF) Cyber Physical Systems (CPS) Program.

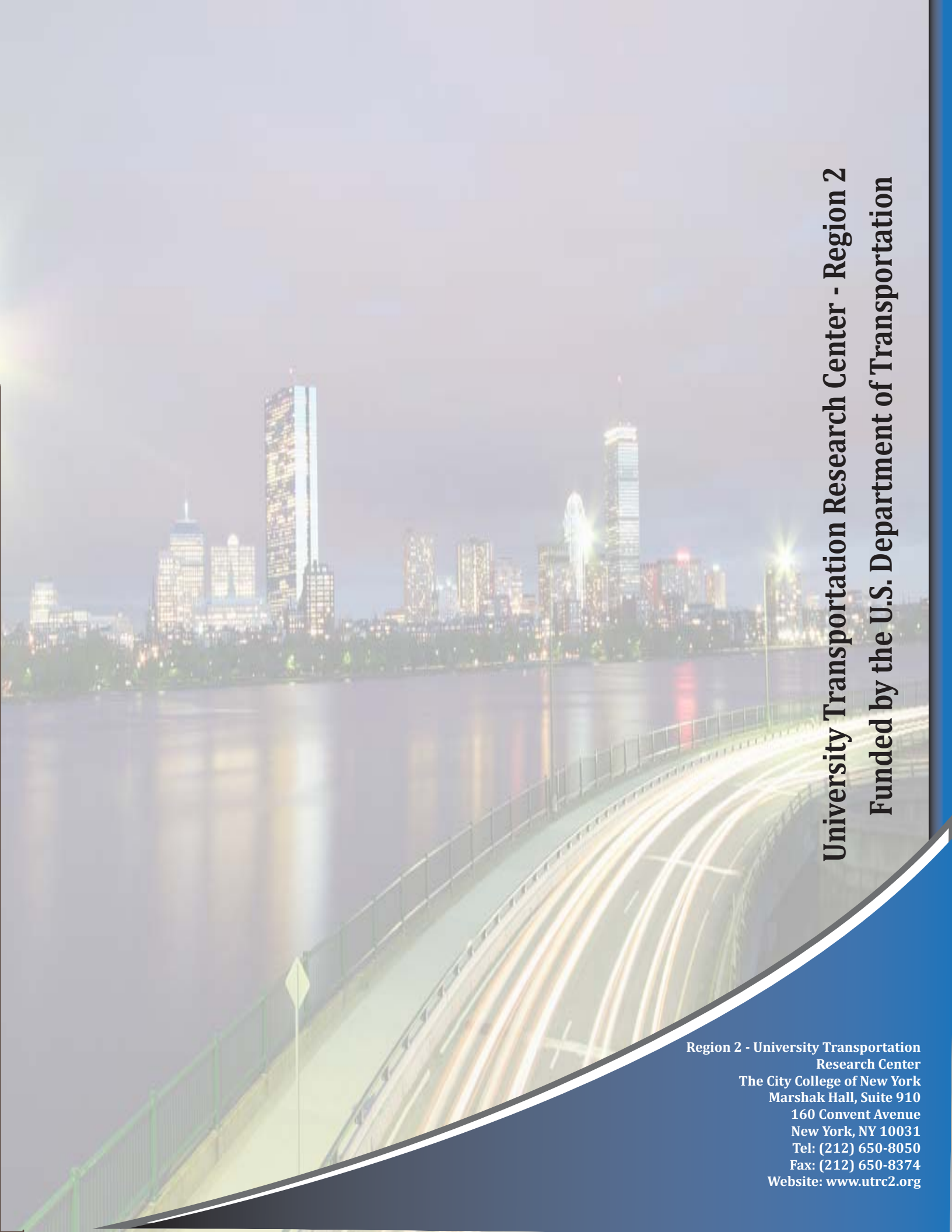
This research project has resulted in training opportunities for the NYIT graduate students to be involved in academic research in cyber security and wireless networks, and more specifically how to use network simulation software to simulate cyber attacks and countermeasures in vehicular networks. The four Master's students actively participated in this research project, and none of them had any prior experience working with NS-3 network simulator. At the completion of their research work, they were trained to be able to work on the NS-3 network simulator independently. We would acknowledge US Department of Transportation and particularly the Region II University Transportation Research Center (UTRC) for the generous support that was offered to us to conduct this research.

References:

- [1] M. Zhao, J. Walker, and C.-C. Wang, "Security Challenges for the Intelligent Transportation System," in *Proceedings of the First International Conference on Security of Internet of Things*, Kollam, India, 2012.
- [2] Wenjia Li, Houbing Song, "ART: an Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", *IEEE Transactions on Intelligent Transportation Systems*, vol.17, no. 4, pp. 960-969, April 2016.

- [3] H. Sedjelmaci and S. M. Senouci, "A new Intrusion Detection Framework for Vehicular Networks," in *Proceedings of 2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, 2014, pp. 538-543.
- [4] S. Chang, Y. Qi, H. Zhu, J. Zhao and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103-1114, June 2012.
- [5] Y. Guo, S. Schildt and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular Delay Tolerant Networks," in *Proceedings of 2013 Fifth International Conference on Communication Systems and Networks (COMSNETS)*, Bangalore, India, 2013, pp. 1-7.
- [6] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia and C. X. Mavromoustakis, "A Cooperative Watchdog System to Detect Misbehavior Nodes in Vehicular Delay-Tolerant Networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7929-7937, Dec. 2015.
- [7] Yao, Yuan, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou. "Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI." *IEEE Transactions on Mobile Computing*, May 2018.
- [8] Benslimane, Abderrahim, and Huong Nguyen-Minh. "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks." *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475-6488, July 2017.
- [9] Yang, Zhe, Kan Yang, Lei Lei, Kan Zheng, and Victor CM Leung. "Blockchain-based Decentralized Trust Management in Vehicular Networks." *IEEE Internet of Things Journal*, 2018.
- [10] Rawat, Danda B., Gongjun Yan, Bhed Bahadur Bista, and Michele C. Weigle. "Trust On the Security of Wireless Vehicular Ad-hoc Networking." *Ad Hoc & Sensor Wireless Networks* 24, no. 3-4 (2015): 283-305.
- [11] M. C. Chuang and J. F. Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks," in *IEEE Systems Journal*, vol. 8, no. 3, pp. 749-758, Sept. 2014.
- [12] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan and V. C. M. Leung, "A Context-Aware Trust-Based Information Dissemination Framework for Vehicular Networks," in *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 121-132, April 2015.
- [13] Kerrache, Chaker Abdelaziz, Nasreddine Lagraa, Carlos T. Calafate, Juan-Carlos Cano, and Pietro Manzoni. "T-VNets: A novel Trust architecture for Vehicular Networks using the standardized messaging services of ETSI ITS." *Computer Communications* 93 (2016): 68-83.
- [14] Sedjelmaci, Hichem, and Sidi Mohammed Senouci. "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks." *Computers & Electrical Engineering* 43 (2015): 33-47.
- [15] Kumar, Neeraj, and Naveen Chilamkurti. "Collaborative trust aware intelligent intrusion detection in VANETs." *Computers & Electrical Engineering* 40, no. 6 (2014): 1981-1996.
- [16] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," in *IEEE Access*, vol. 4, no. , pp. 9293-9307, 2016.
- [17] N. Haddadou, A. Rachedi and Y. Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3657-3674, Aug. 2015.
- [18] NS-3 (a discrete-event network simulator for internet systems) [Available online:] <https://www.nsnam.org/>
- [19] OpenStreetMap. [Available online:] <https://www.openstreetmap.org/>
- [20] SUMO: Simulation of Urban Mobility. [Available online:] <http://www.sumo.dlr.de/userdoc/Tools/Main.html>
- [21] Camp, Tracy, Jeff Boleng, and Vanessa Davies. "A survey of mobility models for ad hoc network research." *Wireless communications and mobile computing* Vol. 2, no. 5, pp. 483-502, September 2002.

- [22] Broch, Josh, David A. Maltz, David B. Johnson, Yih-Chun Hu, and Jorjeta Jetcheva. "A performance comparison of multi-hop wireless ad hoc network routing protocols." In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pp. 85-97. ACM, 1998.
- [23] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003. <https://www.ietf.org/rfc/rfc3561.txt>
- [24] Wikipedia, Packet Dropping Attack. https://en.wikipedia.org/wiki/Packet_drop_attack
- [25] Li, Wenjia, Jonathan Voris, and N. Sertac Artan. "Security, trust, and privacy for cloud computing in Transportation Cyber-Physical Systems." *Data Security in Cloud Computing*, Chapter 5, IET Press, 2017.

The background of the slide is a long-exposure photograph of a multi-lane highway bridge at night. The bridge has a green metal guardrail on the left side. In the distance, across a body of water, is a city skyline with several illuminated skyscrapers, including the Freedom Tower. The lights from the bridge and the city are reflected in the water. The sky is dark with some light clouds.

University Transportation Research Center - Region 2 Funded by the U.S. Department of Transportation

Region 2 - University Transportation
Research Center
The City College of New York
Marshak Hall, Suite 910
160 Convent Avenue
New York, NY 10031
Tel: (212) 650-8050
Fax: (212) 650-8374
Website: www.utrc2.org