SOCIAL-BASED TRUSTWORTHY DATA FORWARDING IN VEHICULAR DELAY TOLERANT NETWORKS

by

Abdulelah Alganas

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree of

Master of Applied Science (MASc)

in

Electrical and Computer Engineering

Faculty of Engineering and Applied Science

University of Ontario Institute of Technology (UOIT)

Oshawa, Ontario, Canada

March, 2011

Abstract

Vehicular ad hoc network (VANET) is an emerging new communication technology which has attracted a lot of research attention from academic community and industry. For many applications in VANETs, information has to be transmitted through multiple hops before it reaches its destination that makes it a subject to various security attacks and privacy breaches. Thus, security and privacy issues could limit its adaption by the public community.

In this study, we propose and evaluate social based trustworthy data forwarding scheme for VANET. First, by using social network analysis techniques, we provide a framework to strategically deploy Road-Side Units (RSUs) infrastructure in order to improve reliability, efficiency, and high packet delivery for VANET. It is based on multiple social centrality assessments of street network which help in placing RSUs at high social intersections. This social placement of RSUs will dramatically improve data dissemination as the opportunity of contacting vehicles increase while costs of RSU deployment can be kept under control. Second, we propose a secure and privacy-preserving message forwarding protocol, which utilizes RSUs to forward messages between vehicles. The protocol takes advantage of high performance capability of RSUs to store and forward messages to their destinations, where these RSUs utilize re-encryption technique to form a mix network to provide adequate privacy for senders and receivers. Then detailed analysis in terms of security, message overhead, delivery ratio, and average delay are performed to evaluate the efficiency and effectiveness of our proposed scheme. Lastly, we tackled the security and privacy challenges existing in social-aware data diffusion by proposing an efficient vehicle social evaluation (EVSE) scheme. Our scheme enables each vehicle to show its authentic social evaluation to others while not disclosing its past location information. As a result, it can meet the prerequisites for the success of social aware data diffusion in VANETs.

Acknowledgements

I would like to express my deep and sincere gratitude to my supervisor Prof. Xiaodong Lin for his kindness, encouragement, continuing guidance, and support during my research. From him, I learned valuable lessons in writing and organizing papers, and doing research. It was an honor for me to work with him.

I also appreciate my co-supervisor Prof. Ali Grami for his valuable advice and suggestions. I also thank him for his efforts and time spent in providing me insightful and detailed comments which have greatly improved the quality of this work.

Table of Contents

Abstract ii

Acknowledgements iii

Chapter 1 Introduction 1

1.1 Background and Motivation 1

1.2 Objectives and Methodology 4

1.2.1 Contributions 6

1.3 Thesis Organization 7

Chapter 2 Security and Privacy in VANETs 8

2.1 Introduction 8

2.2 Related Works 8

2.2.1 Presence of Infrastructure in VANETs 8

2.2.2 Security and Privacy in VANETs 9

2.2.3 Centrality Measures in Networks of Urban Streets 11

2.3 Attack Models in VANETs 12

2.4 Security Requirements in VANETs 13

Chapter 3 Social-based Trustworthy Data Forwarding Protocol 15

3.1 System Model 15

3.2 Social-Based Trustworthy Data Forwarding Protocol 17

3.2.1 RSUs 18

3.2.1.1 Weighted Undirected Graph-Based Street Map Model 19

3.2.1.2 Social-Based RSU Deployment 20

3.2.2 RSUs Based Mixing Network Using Re-encryption for Anonymous Communication 23

3.2.2.1 Re-encryption Based on ElGamal 24

3.2.3 Social-Based Data Forwarding Protocol 25

3.2.3.1 System Initialization Phase 25

3.2.3.2 Message Generation Phase 26

3.2.3.3 Message Forwarding Phase 26

3.2.3.4 RSUs Re-encryption and Mixing Phase 27

3.2.3.5 Message Retrieving Phase 29

3.3 Security Analysis 30
3.4 Performance Evaluation 31
3.4.1 Simulation Setup 35
3.4.2 Simulation Results 38
Chapter 4 An Efficient Vehicle Social Evaluation Scheme with Location Privacy Preservation for Vehicular Communications 43
4.1 Introduction and Motivation 43
4.2 Models and Design Goal 45
4.2.1 System Model 45
4.2.2 Security Model 47
4.2.3 Design Goal 47
4.3 Bilinear Pairing Technique 48
4.4 Proposed Efficient Vehicle Social Evaluation Scheme with Location Privacy Scheme 49
4.4.1 System Initialization 49
4.4.2 Social Witness Collection 50
4.4.3 Vehicle Social Evaluation 53
4.5 Security Analysis 55
4.6 Performance Evaluation 56
4.6.1 Simulation Setup 56
4.6.2 Simulation Results 58
Chapter 5 Conclusions and Future Work 60
5.1 Summary 60
5.2 Contributions 61
5.3 Future Work 62
References 63

List of Figures

Figure 3-1. Network architecture 17

Figure 3-2. Representing roads map into a graph 20

Figure 3-3. Complete city map graph 22

Figure 3-4. Vertices are coded based on their centrality 22

Figure 3-5. Hexagonal grid overlay for RSUs placement 23

Figure 3-6. RSUs-based mix network 28

Figure 3-7. Retrieving messages from an RSU 30

Figure 3-8. Simulation framework 34

Figure 3-9. City of Oshawa region considered for simulation 35

Figure 3-10. SUMO and OMNET++ exchanging data online 38

Figure 3-11. Avarage delivery ratio 39

Figure 3-12. Average messages overhead 40

Figure 3-13. Message delay metrics 41

Figure 3-14. Forwarding hops metrics 41

Figure 4-1. System model under consideration 46

Figure 4-2. Time is slotted for achieving location-privacy preserving social witness collection in VANETs 50

Figure 4-3. Simulation area 57

Figure 4-4. Vehicle mobility model 57

Figure 4-5. Social evaluation 59

Figure 4-6. Average Diffusion Delay 59

List of Tables

Table 3-1 SUMO parameters 36

Table 3-2 INETMANET framework parameters 37

Table 3-3 Simulation scenarios 37

Table 4-1 Simulation settings 58

List of Abbreviations

DoS	Denial of Service
DTN	Delay Tolerant Network
EVSE	Efficient Vehicle Social Evaluation
IVC	Inter Vehicle Communication
OBU	On-board Unit
PKI	Public Key Infrastructure
RSU	Road-Side Unit
SA	Sub-Area
SES	Social Evaluation Server
TA	Trusted Authority
TPD	Tamper Proof Device
V2I	Vehicle to Infrastructure communication
V2V	Vehicle to Vehicle communication
VANET	Vehicle Ad-hoc Network
WAVE	Wireless Access in Vehicular Environment

Chapter 1

Introduction

1.1 Background and Motivation

Delay Tolerant Networks (DTNs) are a type of networks that are exposed to disruption, disconnection, and long delay [1]. DTNs rely on participating nodes to traverse packets to their destinations by using store and forward techniques. Since these nodes are in constant mobility along with constrains in power and memory recourses, end-to-end communication cannot be guaranteed between source and destination. Consequently, traditional routing protocols are not applicable to operate directly on DTNs as they are challenged with high latency, frequent disconnections, high error probability, and limited node longevity [2]. Therefore, DTNs have gained significant research attention directed at designing efficient routing algorithms [1] [3]. Simultaneously, emerging class of applications, referred to as Delay Insensitive Applications (e.g. messaging, file transfer, and data dissemination) are designed to utilize the nature of DTN.

In recent years, Vehicular Ad-Hoc Network (VANET), which is a special form of DTN, has raised growing research interest from both academia and industry, mainly to its great potential to enhance safety and comfort of drivers. VANET is distributed and self-organized data communication network build upon communication among nearby vehicles, and among vehicles and nearby road-side communication devices [4]. In VANETs, vehicles are equipped with On-Board Units (OBU) that enable communications from Vehicles-to-Vehicles (V2V) and also from Vehicles to fixed Roadside Infrastructure (V2I). The fixed roadside infrastructure is a collection of Road-Side Units (RSU) that are placed alongside roads to relay and forward messages to vehicles as well as to backbone network. Vehicular communication has enabled a variety of applications to improve road safety and traffic efficiency as well as to increase driver‘s comfort on the road. Safety applications that extend driver's horizon of perception (e.g, Warnings for traffic jams, icy roads, and road accidents) and comfort applications which promote quality of driving (e.g, route selection, information access, and weather information) are examples of VANET services. For many vehicle applications, information has to be transmitted through multiple hops before it reaches its destinations. For instance, when a vehicle wants to send a message to other vehicles in different parts of the city, it may use the help of passing-by vehicles and RSUs to store and forward message to its destination. Hence, efficient data forwarding is crucial to success in VANET deployment.

RSUs can enhance the throughput and reliability of Vehicular DTN by creating additional contact opportunities among mobile nodes that never meet [5]; Intuitively, it can be helpful for data forwarding in Vehicular DTN through wide deployment of RSUs. However, RSUs are expensive devices, and they will not be widely available especially in the early stage of VANET deployment. Thus, how to strategically deploy RSUs becomes vital to improve packet forwarding in VANETs while keeping the cost of deployment and installation of RSUs under control.

In reality, vehicles are driven by people and people tend to travel in order to get to an array of places to do their studying, working, shopping … etc, which are spatially distributed in a city. Therefore, travel patterns are originated from the needs to access locations where activities take place rather than the need for mobility per se. Metropolitan areas with different activity centers will have a great influence on travel patterns as they increase the number of commuters. Moreover, vehicles in VANET tend to move within predefined linear patterns (roads/streets) which are controlled by speed limits and traffic lights. Drivers are more likely to travel on roads that provide fast and easy access to activity centers around city. Further, as GPS navigation becomes even more popular, drivers tend to choose the best route to drive to their destinations, for example, the shortest, quickest, or safest routes. Therefore, these travel patterns (vehicle mobility model) can be used to help derive an effective strategy for deploying RSUs at some highly social traffic areas. Therefore, RSUs can effectively assist the data forwarding in VANETs and at the same time with better cost control. Furthermore, user sensitive information, such as traveling route, speed, position, and license plate, has to be protected in order for Vehicular DTN to gain wide spread by public community. User identity should remain anonymous while their vehicles help in forwarding messages.

Finally, deploying and testing VANET is costly and time consuming. Hence, simulation is sole alternative before actual implementation. In VANETs, vehicular environment imposes new issues and requirements to simulations. In particular how to simulate traffic jams, road rules, environmental conditions, constrained map topology, drivers' driving behavior, and vehicle accidents. The results of VANET simulation are heavily influenced by the quality of employed mobility model. Currently, most network simulators do not provide suitable mobility models for VANET; however, there exist some road traffic simulators designed to generate realistic vehicles mobility. Thus, we can use road traffic simulator to generate realistic mobility traces based on a real city map with environmental conditions, and then feed them to a network simulator. However, the lack of built-in control interface, which allows both simulators to exchange control data in real time, makes building up a realistic VANET simulation environment very challenging. Therefore, extending bi-directionally coupled road traffic and network simulators, in which road traffic affects network traffic and vice versa, are important to validate the proposed data forwarding scheme.

1.2 Objectives and Methodology

The thesis first gives an overview of packet forwarding in Vehicular DTN and its potential application areas of VANETs. Afterwards contributions to the topic of packet forwarding in VANETs are made in the areas of RSUs deploying, privacy preservation in packet forwarding, and experimental simulation.

The first objective of this thesis is to propose a framework for deploying RSUs based on centrality measures on weighted urban streets network. In order to choose high social intersections on streets map, different centrality measures will be calculated on a hexagonal grid overlay over the map of the city of interest with predetermined activity centers, then RSUs will be deployed on chosen number of intersections with high sociality. This novel framework will improve the efficiency of VANET by increasing throughput and decreasing cost.

The second objective of this thesis is to design a privacy preserving message forwarding protocol which utilizes social characteristics of RSUs. The proposed protocol takes advantage of high performance capability of RSUs to store and forward messages to their destinations, while applying cryptographic construction of mix network with re-encryption to provide adequate privacy for senders and receivers through transforming RSUs deployed at those highly social spots to a mix network.

The third objective is to evaluate the scheme by means of simulation. OMNET++ [6] had been used as network simulator while SUMO [7] was used as traffic simulator. Simulation has been conducted in a small area of the city of Oshawa with auto generated realistic vehicle routes. We made some vehicles send messages and compared our protocol to a simple flooding method and other topology based routing protocols.

The final objective is to improve social-aware data diffusion by proposing an efficient vehicle social evaluation (EVSE) scheme with location privacy preservation for VANET. The proposed EVSE scheme is based on an efficient group signature, which enables each vehicle to show its authentic social evaluation to others while not disclosing its past location information.

1.2.1 Contributions

This research focus on developing a framework achieves privacy and security for data forwarding in vehicular delay tolerant networks. Specifically, the main contributions of this research are three folds:

- A security infrastructure for VANETs is introduced, where RSUs are deployed at high social intersections based on multi-social centrality measures. Then, these RSUs utilize a re-encryption technique to form a mix network which provides adequate privacy for multi-hop data forwarding.
- A realistic VANET simulation framework is developed, where road traffic simulator is coupled with network simulator. In specific, we provide vehicles with GPS-like functionality in order to model the influence of road traffic into network traffic and vice versa. Also realistic vehicle traces for the map of city of Oshawa were generated.
- A location privacy-preserving social evaluation model with time slotting technique is presented, where each vehicle can request a social evaluation server (SES) to obtain its social evaluation in a new time slot according to its social witnesses collected in the previous time slot. SES can evaluate a vehicle's sociality, but cannot identify the vehicle's past location information.

1.3 Thesis Organization

This thesis consists of five chapters. Chapter 1 presents an introduction to this work and the other chapters are organized as follows:

- Chapter 2: In this chapter, a number of packet forwarding protocols in vehicular DTN are surveyed, and their features, advantages, and disadvantages are outlined. While a considerable number of packet forwarding protocols exist in literature, using social based approaches are relatively new to the VANET environment.
- Chapter 3: This chapter describes a framework for social based RSUs deployment in details. It explains the novel social based message forwarding protocol, and describes privacy preserving technique in details. It also provides deep analyses to our proposed protocol performance with comparison to other VANET protocols.
- Chapter 4: This chapter depicts the efficient vehicle social evaluation (EVSE) scheme with location privacy preservation for VANET. It details the structure of an efficient group signature, which enables each vehicle to show its authentic social evaluation to others while without disclosing its past location information.
- Chapter 5: This chapter briefly summarizes the key outcomes of our scheme, and offers some suggestions for future directions of this work.

Chapter 2

Security and Privacy in VANETs

2.1 Introduction

The advances in wireless technology have enabled vehicles to talk with each other or with roadside infrastructure. Using both V2V and V2I communications not only drivers' safety can be enhanced but also their comforts. Securing VANET is mandatory prior to its deployment. Hence, VANET has gained a lot of attention from research community.

The reminder of this chapter is organized as follows. In Section 2.2, we review related works. Then, we describe security threat and requirements in Sections 2.3 and 2.4.

2.2 Related Works

2.2.1 Presence of Infrastructure in VANETs

RSUs have greatly improved the connectivity in VANETs [8, 5]. Aiming to classify VANETs infrastructure, Banerjee *et al.* [9] showed the influence of relays, meshes, and wired base stations on mobile networks by performing extensive experimental and analytical studies. They conducted their study in a large scale vehicular network where they deployed relays, meshes, and wired-base stations in areas of interest to temporarily store and forward packets to passing by vehicles until they reach their final destinations. In the study, they conclude that introduction of infrastructure in VANETs greatly enhances its performance. Many related works take advantage of the presence of infrastructure in VANETs to achieve privacy requirements.

2.2.2 Security and Privacy in VANETs

Security and privacy issues in VANETs have received extensive research attention from both academia and industry.

IEEE Working Group issued IEEE 1609.2-2006 [10] standard for wireless access in vehicular environment- security services for applications and management messages. The standard covers a range of security services to be used in the Wireless Access in Vehicular Environments (WAVE) such as the format of the security messages and the choice of the cryptosystem. It provides mechanisms to authenticate and encrypt messages that are sent to vehicles or road-side infrastructure. The standard promotes anonymity in which driver's private information is preserved; however, it does not provide any detailed approach to achieve privacy requirements.

The studies in [11,12] discussed general security and privacy requirements that can satisfy security architecture of VANETs. They outlined attacking models, security requirements, and properties of Inter Vehicle Communication (IVC) systems; however, they did not provide any solution to fulfill these requirements. Raya *et al.* in [13] proposed that each vehicle should acquire a large number of private and public key pairs (around 43,800 pairs) along with their corresponding public key certificates. When sending traffic related messages, vehicles randomly choose a key pair at a time to sign each message. To meet drivers' privacy requirements, vehicles use pseudo ID in each public certificate instead of real identity information. Furthermore, these pseudo IDs have short life times and are changed after several uses, which prevent linking them to sending vehicles. This scheme well preserves drivers' privacy; however, vehicles require a large storage capacity to store all their security information. Moreover, the scheme also imposes management overhead on Trust Authority (TA) as it should keep track of all vehicles pseudo IDs and their corresponding key pairs.

Aiming to overcome aforementioned issues Lin *et al.* in [14] proposed a group signature-based scheme. In their scheme, vehicles are arranged in groups where all vehicles in a group share a group public key, yet every vehicle has its unique private key. A sending vehicle signs messages using its private key, while receiving vehicles can use group public key to verify if messages are indeed from a legitimate group member or not. Vehicles can report malicious messages to TA, which can use it secret key to trace the real identity of the sender. The drawbacks of this scheme are: *i*) TA has to renew keys for all vehicles within a group when revoking one of its members, and *ii*) Verifying group signature requires a high degree of computation comparing to traditional Public Key infrastructure (PKI).

Many researchers utilize RSUs to achieve security and privacy requirements in VANETs. Lu *et al.* [15] proposed an efficient conditional privacy preserving scheme, called ECPP. In the scheme privacy is classified in three levels. First, vehicles use anonymous certificates issued by RSUs to communicate where no privacy is defined. Second, messages are anonymously authenticated, so vehicle identity is hidden to other vehicles; however, an attacker can reveal real identity by collecting messages. Third, vehicle identity is only traceable by trusted authority (TA). All levels depend on RSUs to issue temporarily certificates. In the scheme, TA has the highest priority in which it is able to recover both vehicle real identity and certificate issuer (RSU) at any level. Freudiger *et al.* in [16] proposed a concept of mix-zone to protect location privacy of vehicles. They defined the mix-zone as the area in transmission range of an RSU. All vehicles within a mix-zone share a secret key provided by the RSU. Inside the mix-zone all messages are encrypted using the shared secret key, while vehicles use their public keys to encrypt messages when leaving a mix-zone. Therefore, an attacker cannot associate vehicle identity before and after passing through a mix-zone, yet other legitimate vehicles still can link identities as they have the same secret key.

2.2.3 Centrality Measures in Networks of Urban Streets

Aiming to recognize properties of streets network Crucitti *et al*. [17] investigated the visualization and characterization of city structure based on centrality measures. They used several centrality indices such as closeness, betweenness, straightness, and information centrality to capture structural properties of a city, and its relevant dynamics like vehicular flows. The city map was presented in primal approach in which crossroads turned into vertices and street segments into edges. They have shown that each centrality index capture a different social aspect of the city map. However, they only considered geographical topology of the map, while ignoring all possible metrics in the map. Unlike above approach Jiang et al. [18] used dual representation of street network in a graph, in which they turned named streets into vertices and intersections into edges. They introduced centrality measures to rank the states of each individual street in a city map. In this approach important streets are easily distinguished; however, it is a pure spatial approach where street network metrics are ignored.

2.3 Attack Models in VANETs

The followings are definitions of several typical attacks in VANETs:

- *DoS attack*: attackers consume all the bandwidth of the channel by continuously sending a large number of dummy messages. It can bring the network down and prevents vehicles from communicating with each other. Moreover, in more sophisticated attacks, messages may have invalid signatures, so vehicles spend a long time verifying invalid signatures which impose delays in legitimate messages.
- *Privacy attack*: a global attacker can collect private information such as vehicle's identity, location, and speed information by observing messages within a region. Thorough information analysis, attacker can detect vehicle movements which impose potential privacy infringement.
- *Impersonation attack*: an attacker pretends to be another vehicle to send malicious messages into the network. Moreover, an attacker could also pretend to be an RSU to fool other vehicles to forward their messages.
- *Message alteration attack:* attackers may modify their identity related information such as speed, driving direction, and location in order to deny their involvements in accidents.

- *Fake messages attack*: an attacker sends false information about road conditions such as accidents and traffic jams in order to mislead other vehicles.

2.4 Security Requirements in VANETs

VANETs should meet the following security requirements in order to withstand the above-mentioned attacks.

- *Authentication*: the identity of a vehicle should be verified in order to distinguish a legitimate vehicle from an unauthorized vehicle. Public key certificate is commonly used to authenticate the identity of the user.
- *Integrity*: it is important in VANETs to verify that messages have not been altered during transmission. Most popular approach to ensure integrity in VANETs is the use of a hash function in which a digest value of the message is sent together with the original message.
- *Availability*: a network should be equipped with adequate mechanisms to withstand DoS and consistently and continually provide services to its legitimate users.
- *Privacy*: messages sent by vehicles may contain private information that can identify the real identity of the vehicle. People concern about their privacy, and they are not willing to reveal their private information to third parties. Therefore, a secure mechanism should be employed in order to prevent an unauthorized party from acquiring vehicles private information.

- *Non-repudiation*: ability to prevent a sender vehicle from denying the generation of a messages or denying the content of a message. This requirement is important for VANETs especially in case of accidents.

Chapter 3

Social-based Trustworthy Data Forwarding Protocol

In this chapter, we introduce a novel social-based trustworthy data forwarding protocol for VANET. First, we formalize the system model adopted by our routing protocol. Then, we present the network model by introducing social based deployment for vehicular roadside infrastructure. Afterwards, we describe our design objectives and possible applications. Finally, we conclude with full description of secure and privacy-preserving data forwarding protocol.

3.1 System Model

VANET can be extended to support Delay Tolerant Network (DTN) applications by utilizing vehicles to provide connectivity under challenged scenarios with unstable links and where a contemporaneous end-to-end path may never exist. Intuitively, deploying RSUs in high social intersections, which vehicles drive by most frequently, will progressively enhance the probability of message delivery. Providing highly reliable and privacy-preserving message forwarding protocol is the goal of this work. In our protocol, vehicles rely on high social RSUs to store and forward messages to their destination.

The network infrastructure is based on vehicles-to-vehicles (V2V) and also vehicles to fixed Roadside infrastructure (V2I) communications, shown in Figure 3-1. In our scenario, all vehicles and RSUs have their own unique characteristics:

- **Vehicles**: they are characterized with high mobility. In our scenario, each vehicle is equipped with On-Board Unit (OBU) which allows it to communicate wirelessly in ad-hoc fashion; however, these OBUs have constrains in their resources (e.g. buffer and small sending range). Some of these vehicles might be equipped with GPS where the route that the vehicle takes is predetermined. In general, vehicles will assist forwarding messages if they have sufficient storage, otherwise, they will not help in forwarding new messages.
- **Road-side Units (RSUs)**: they are stationary units which have enormous storage, high transmission rate and range and sufficient processing power. In our design, RSUs are connected through backbone network, so any packet received by an RSU will be broadcast to all other RSUs. The main responsibility of RSU is to temporarily store messages until they are retrieved by their intended receivers. RSUs are expensive devices which prevent deploying them on every intersection in a city, especially, in the early stages of VANET deployment; therefore, we utilize social centrality measures to find out some high social intersections, named social spots, and then strategically deploy RSUs at these social spots. We also assume that each RSU contains a tamper proof device (TPD) to securely store all received messages and allow authorized message recipients to retrieve their messages.

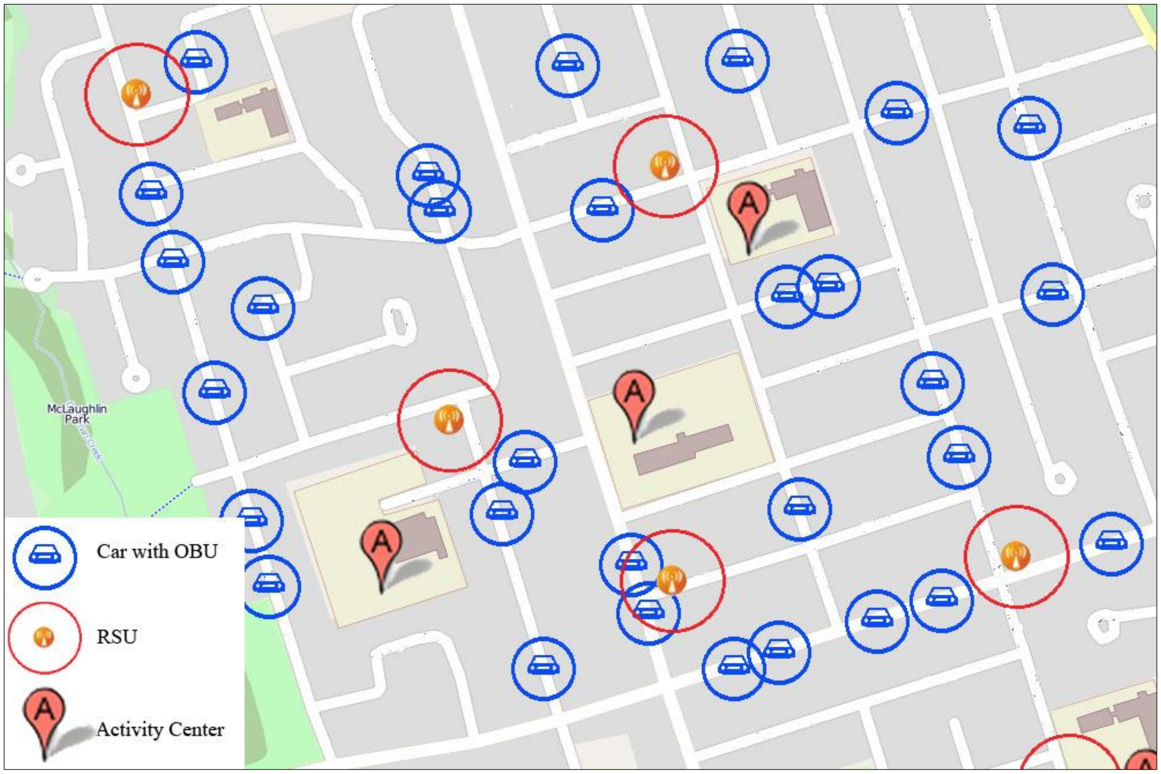


Figure 3-1. Network architecture

3.2 Social-Based Trustworthy Data Forwarding Protocol

In this subsection, we describe our proposed social-based trustworthy data forwarding protocol for VANETs. The proposed protocol works as follows: when a vehicle has a message to send, it first enquires its GPS to determine if there is a close RSU positioned on its route. On the one hand, if a close RSU exists on its route, it carries on the message until it hands the message over to the RSU. On the other hand, if RSUs do not exist on the route from the sending vehicle to the destination or far away from vehicle, it uses other vehicles assistance to deliver messages to an RSU. When an RSU receives a message, it utilizes MIX network formed by social spots to replicate message on all other

RSUs which in return preserve the identity of sender and receiver. Later, intended receiving vehicle can retrieve message from any RSUs in city.

3.2.1 RSUs

People tend to travel in order to get to activities such as studying, working, shopping … etc which are spatially distributed in a city. Therefore, travel patterns are originated from the needs to access locations where activities take place rather than the need for mobility. The followings are examples of usual activities in a city which highly affect urban travel patterns:

- Daily commuting trips from and to work place. These trips are periodic on regular basis.
- School run: parents taking their children to or from school by personal cars. These trips are also periodic on regular basis.
- Work related trips which include meetings, customers' service, sales, etc.
- Recreational trips which include shopping, touring, personal affairs.

Streets which contain or provide fast, short, or easy access to major activity centers have a great influence on travel patterns as they become the primary choice for street users. Therefore, placing RSUs in intersections, which provides easy access to these streets, maximizes the overall effectiveness of RSUs as they become in contact with higher number of streets users.

From above observation, we propose activity based multi-centrality assessment for deploying RSUs, in which RSUs are placed in high social intersections that provide efficient reachability to activity centers around city.

3.2.1.1 Weighted Undirected Graph-Based Street Map Model

Urban streets network can be represented as a primal graph G = (V, E), a mathematical entity defined by a pair of finite set of vertices V = $\{v_1, v_2, .., v_n\}$ and edges E = $\{v_i v_j\}\ where\ j, j\ \in \{1,2, ... n\}$. In our design, vertices v_i represent intersections between two or more roads, while a road that links two intersections represents undirected weighted edge $e(i, j)$, shown in Figure 3-2. For computational simplicity, edges are undirected in which no distinction between a pair of vertices connected by an edge; therefore, all streets in our design are turned into bidirectional streets. In the graph, a vertex will be referred to by its order i in the set V (1≤ i ≤ n), and two vertices v_i, v_j are adjacent or connected if there is an edge $e(i, j) \in E$. A graph is connected if there is a path $\{v_i v_j\}$ for every $v_i v_j\ \in V$, which is the case on streets network. We use m and n to donate the number of vertices and edges, respectively.

The full weighted graph G = (V, E, W) is defined by triple sets V, E and W. The set W is a set of E elements being numerically weighted with a value that indicates the strength of (i, j) for every$e\ (i, j) \in E$. In our design, we use average travel time as an edge weight, which acquired from dividing street length by street speed limit. A graph G = (V, E, W) can be described by using two matrices: first, adjacency matrix A = $\{a_{i,j}\}$, which structure as follows:

$$a_{i,j} = \begin{cases} 1 & if\ v_i, v_j \in E \\ 0 & otherwise \end{cases}$$

Second, weight matrix W={ w_{ij} }, a N × N matrix whose entry w_{ij} which represents metric value of (i, j) edge for every $e(i, j) \in E$.

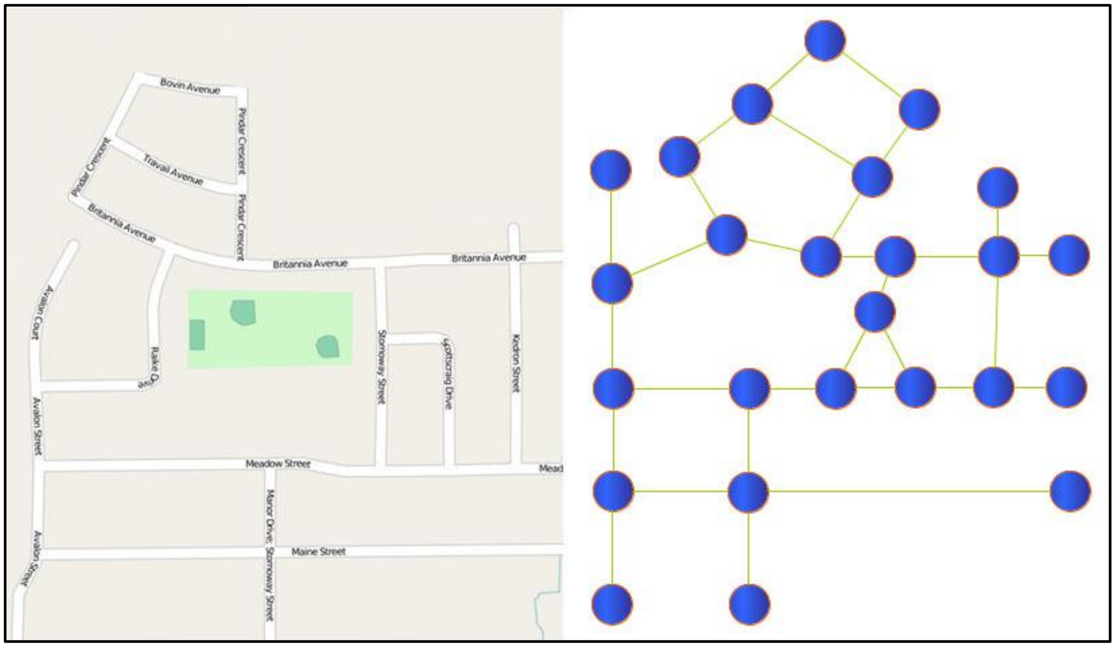


Figure 3-2. Representing roads map into a graph

3.2.1.2 Social-Based RSU Deployment

We employ social network analysis to determine the importance of every intersection in the city map by means of their frequent traverse to other intersections and activity centers, and also their closeness to activity centers. The proposed method is based on the four following steps:

1. By utilizing Geographic Information System (GIS), we identify locations of popular activity centers in the city map (e.g. shopping malls, schools, government offices, sky towers…etc). In GIS, these locations are stored as (X, Y coordinates);

therefore, we use Euclidian Distance to assign every activity center to its closest main intersection (vertex). These vertices that are closest to activity centers are grouped in a subset called activity centers gates V_g.

2. Using social network analysis techniques, we evaluate the centrality and importance of every vertex in a graph with relevance to activity centers. The following are centrality measures adapted in our scheme:

Overall Betweenness Centrality $\boldsymbol{C_B}$: calculates the occurrence of a vertex in shortest paths among all other vertices on the graph:

$$C_b(v) = \sum_{x \neq y \neq v \in V} \delta_{xy}(v) , \qquad (1)$$

where $\delta_{xy}(v)$ denotes the number of shortest paths between $x, y \in V$ that passes through vertex v.

Activity Based Betweenness Centrality $\boldsymbol{C_{ab}}$: calculates the occurrence of a vertex in shortest paths among activity centers gates and all other vertices on the graph.

$$C_{ab}(v) = \sum_{x \neq y \neq v.\ x,v \in V,\ \ y \in V_g} \delta_{xy}(v) , \qquad (2)$$

where $\delta_{xy}(v)$ denotes the number of shortest paths between $x \in V\ and\ y \in V_g$ that passes through vertex v.

Activity Based Closeness Centrality $\boldsymbol{C_c}$: calculates nearness of a vertex v_i to activity centers gates in the graph.

$$C_{ca}(v_i) = \frac{N-1}{\sum_{j=1}^{N} d\left(v_i, v_{g(j)}\right)}\ , \qquad (3)$$

where N is number of activity centers gates in graph, and $d(v_i, v_{g(j)})$ is the shortest distance between vertex v_i and activity center gate $v_{g(j)}$.

3. For simplicity, every vertex is color coded based on the average of its centrality measures within the graph, shown in Figure 3-4.

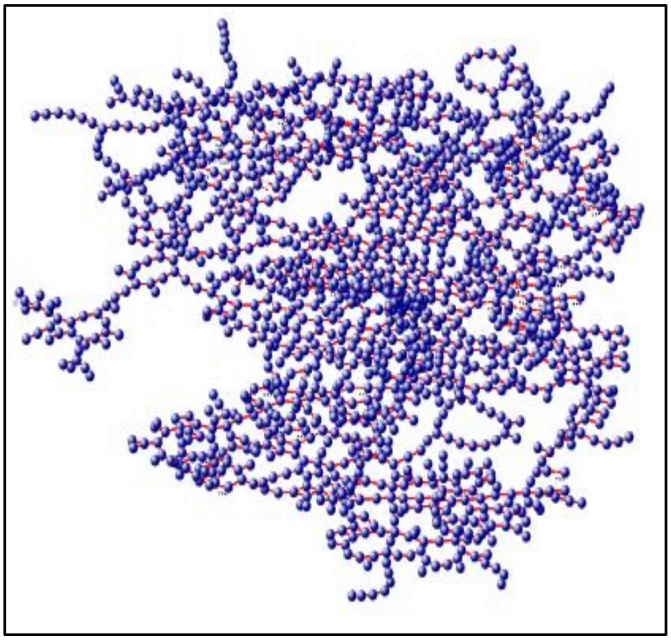


Figure 3-3. Complete city map graph

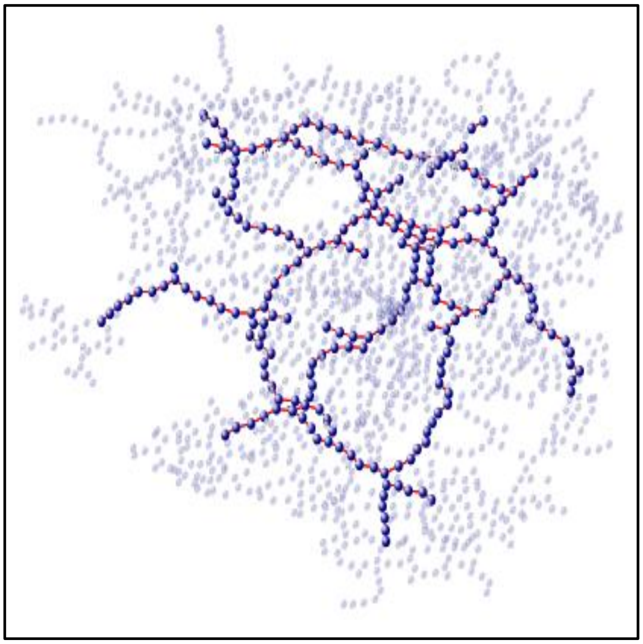


Figure 3-4. Vertices are coded based on their centrality

4. We use a hexagonal grid overlay over the graph to divide it into relatively equal small areas. Then, we elect vertices with highest average social centrality in every hexagonal to place RSUs, shown in Figure 3-5. As a result, RSUs are ho-

mogeneously distributed over city to serve different areas, while every RSU maximizes the number of contact opportunities within its area.

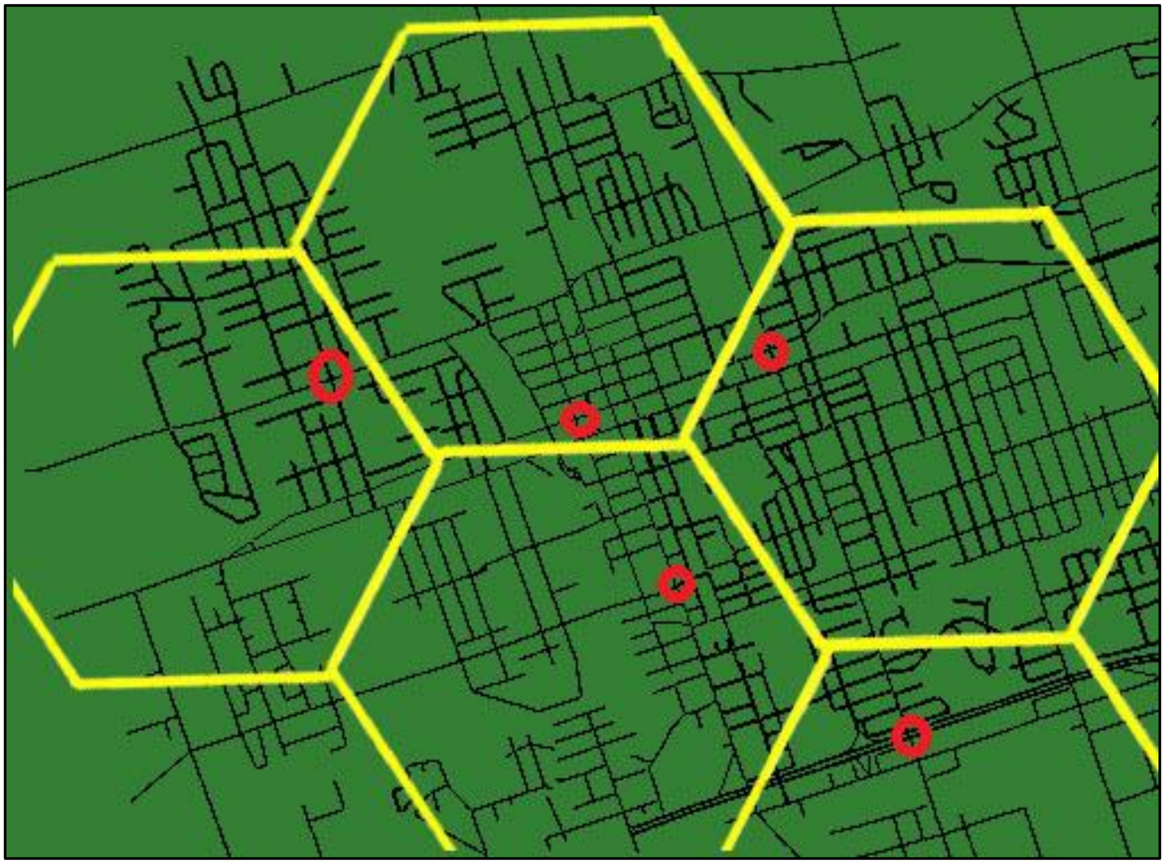


Figure 3-5. Hexagonal grid overlay for RSUs placement

3.2.2 RSUs Based Mixing Network Using Re-encryption for Anonymous Communication

Since the locations of RSUs are fixed, an adversary can easily eavesdrop in transmission channel among RSUs to analyze traffic in order to identify sender, receiver, and message contents. To overcome this problem, we utilize social RSU deployment to construct a mix-network with no-key re-encryption to protect senders and receivers privacy.

In our design, every RSU acts as a mix node, which receives encrypted messages and re-encrypt them in order to send them to other RSUs in random order at given threshold. By doing this, an adversary cannot correlate output messages with input messages within RSUs.

3.2.2.1 Re-encryption Based on ElGamal

Having a homomorphic property, in which $E[a] \times E[b] = E[ab]$ for group operator ×, has made ElGamal [19] a good choice of re-encryption as we can re-factor ciphertext without knowledge of public key [20]. Re-encryption is a function that takes a ciphertext for a message m which is encrypted under destination public key, and transforms it into another ciphertext for the same message m. The re-encryption function in our design is constructed to run without knowledge of the associated public key.

Let G denotes multiplicative cyclic group of order q with published generator g. The following is the cryptosystem:

- **Key Generation**: Private Key PR = x, Public Key PK= y = g^x mod q, where $0 < x < q$. Each vehicle has a unique Public Key which can be used as vehicle identifier. Furthermore; all Tamper Proof Devices (TPDs) within RSUs are assigned with same Private key PR_{TPD} and Public Key PK_{TPD}.
- **Encryption:** Inputs are message m, destination vehicle public key y, TPD public key PK_{TPD}, and three random number $k, k' and\ k''$ (where $0 < k, k', k'' < q - 1$), Outputs are the computed six values $c_1, c_2, c_3, c_4, c_5, and\ c_6$, where $c_1 = g^k\ mod\ q, c_2 = my^k\ mod\ q, c_3 = g^{k'},\ c_4 = y^{k'}, c_5 = g^{k''}, and\ \ c_6 = y.PK_{TPD}^{k''}$

- **Decryption**: inputs are ciphertext $C = (c_1, c_2, c_3, c_4)$ and vehicle secret key x, output is $\frac{c_2}{c_1^x} = \frac{my^k \, mod \, q}{(g^k \, mod \, q\,)^x} = \frac{my^k \, mod \, q}{y^k \, mod \, q} = m$
- **Re-encryption:** inputs is $(c_1, c_2, c_3, c_4, c_5, c_6)$, output is $(cc_1, cc_2, cc_3, cc_4, cc_5, cc_6) = \left(c_1c_3, c_2c_4, {c_3}^{k_1}, {c_4}^{k_1}, g^{k_2},\ y.PK_{TPD}^{k_2}\right) =$ $\left(c_1(g)^{k'}, c_2(y)^{k'}, (g^{k'})^{k_1}, (y^{k'})^{k_1}, g^{k_2},\ y.PK_{TPD}^{k_2}\right) =$ $\left((g)^{k\,k'}, (my)^{k\,k'}, (g)^{\,k'k_1}, (y)^{\,k'k_1}, g^{k_2},\ y.PK_{TPD}^{k_2}\right),\ k_1 \; and \; k_2$ are re-encryption factor which is random from {1… q-1}.

3.2.3 Social-Based Data Forwarding Protocol

Our proposed protocol consists of five phases: *i)* system initialization phase, *ii)* message generation phase, *iii)* message forwarding phase, *iv)* RSUs re-encryption and mixing phase, and *v)* message retrieving phase:

3.2.3.1 System Initialization Phase

In system initialization phase, a Trusted Authority (TA) performs the following steps:

Step 1: It deploys RSUs around city based on the proposed activity based multiple social centrality measurement. RSUs are connected to backbone network to ensure fast data dissemination among RSUs. They should be recognized and trusted by passing vehicles.

Step 2: Every participating vehicle should be registered in the system in order to get a pair ElGamal [19] private encryption key PR = x and public encryption key PK= g^x mod q in same published group generator g. Vehicles should acquires public keys of recipients to whom they intend to communicate. Furthermore, all TPDs within RSUs are assigned with the same Private key PR_{TPD} and Public Key PK_{TPD}.

3.2.3.2 Message Generation Phase

Assume that vehicle $v_s$wants to send a message M to vehicle v_d, yet source vehicle does not know the exact location of target vehicle. However, the source vehicle v_s uses the public key of target vehicle v_d to encrypt the message and TPD public key PK_{TPD} to encrypt destination ID as following:

$$m = (c_1, c_2, c_3, c_4, c_5, c_6) = \left(g^k mod\ q, my^k\ mod\ q,\ g^{k'}, y^{k'}, g^{k''}, y.PK_{TPD}^{k''}\right).$$

$$where\ y\ is\ public\ key\ of\ destenation\ vehicle\ v_d and\ 0 < k, k', k'' < q - 1$$

3.2.3.3 Message Forwarding Phase

As RSUs are placed in high social intersections, the possibility for an intended recipient to come in contact with an RSU is very high. Therefore, sending vehicles utilize this quality of RSUs by asking passing by vehicles to help forward the message to the closest RSU, where receiving vehicle can retrieve the message in later time. Specifically, the sending vehicle invokes Algorithm 1 to forward message M.

```
procedure Message forwarding
when $v_s$ has message packet m to send, it calculate expected travel time to the nearest RSU, $T_r$ ,in its route. ($T_r \geq \infty$ if vehicle $v_s$ has no RSU on its route)
    if ($T_r < thershold$ ) then
        $v_s$waits until it drive by and forwards the message m to RSU
    else If ($T_r > thershold$ ) or ($T_r == \infty$) then
        if $v_s$ detects a nearby vehicle $v_i$ that can help to forward the message m to an RSU then
            $v_s$ forwards the message m to $v_i$
        end if
    end if
end  procedure
```

Algorithm 1. Message Forwarding Algorithm

If the packet message *m* is successfully forwarded to an RSU, this phase is ended.

3.2.3.4 RSUs Re-encryption and Mixing Phase

When a packet message **m** is received by an RSU, it performs the two following steps:

Step 1: TPD recovers the message intended destination ID by decrypting $c_5 and\ c_6$ using its private key PR_{TPD} as follows:

$$\frac{c_6}{c_5^{PR_{TPD}}} = \frac{PK_{TPD}^{k''}}{\left(g^{k''}\right)^{PR_{TPD}}} = y$$

After recovering destination public key, TPD stores the message as (c_1, c_2) in secured database using destination public key as index for messages.

Step 2: It re-encrypts the message *m*= $(c_1, c_2, c_3, c_4, c_5, c_6)$ by using its public key Pk_{TPD} and randomly choosing two re-encryption factors $k_1 and\ k_2, where\ 0 < k_1, k_2 < q - 1$ as follows:

$$(cc_1, cc_2, cc_3, cc_4, cc_5, cc_6) = \left(c_1 c_3, c_2 c_4, {c_3}^{k_1}, {c_4}^{k_1}, g^{k_2}, y.PK_{TPD}^{k_2}\right)$$

$$= \left(c_1 (g)^{k'}, c_2 (y)^{k'}, (g^{k'})^{k_1}, (y^{k'})^{k_1}, g^{k_2}, y.PK_{TPD}^{k_2}\right)$$

$$= \left((g)^{k\,k'}, (my)^{k\,k'}, (g)^{\,k'k_1}, (y)^{\,k'k_1}, g^{k_2}, y.PK_{TPD}^{k_2}\right)$$

Step 3: it sends re-encrypted messages to other RSUs in a random order at a given threshold. By doing this, we prevent an adversary from correlating output messages with input messages. For example, as shown in Figure 3-6, after the re-encryption on two input messages, I-1 and I-2, to RSU *R*, the adversary cannot link two out-going messages O-1 and O-2 to I-1 and I-2.

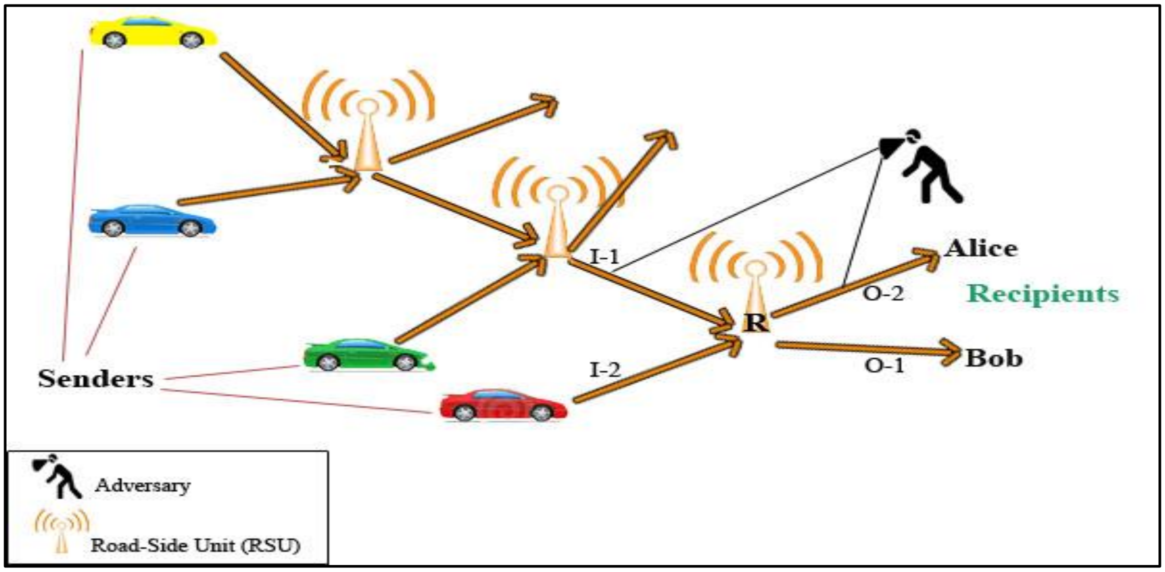
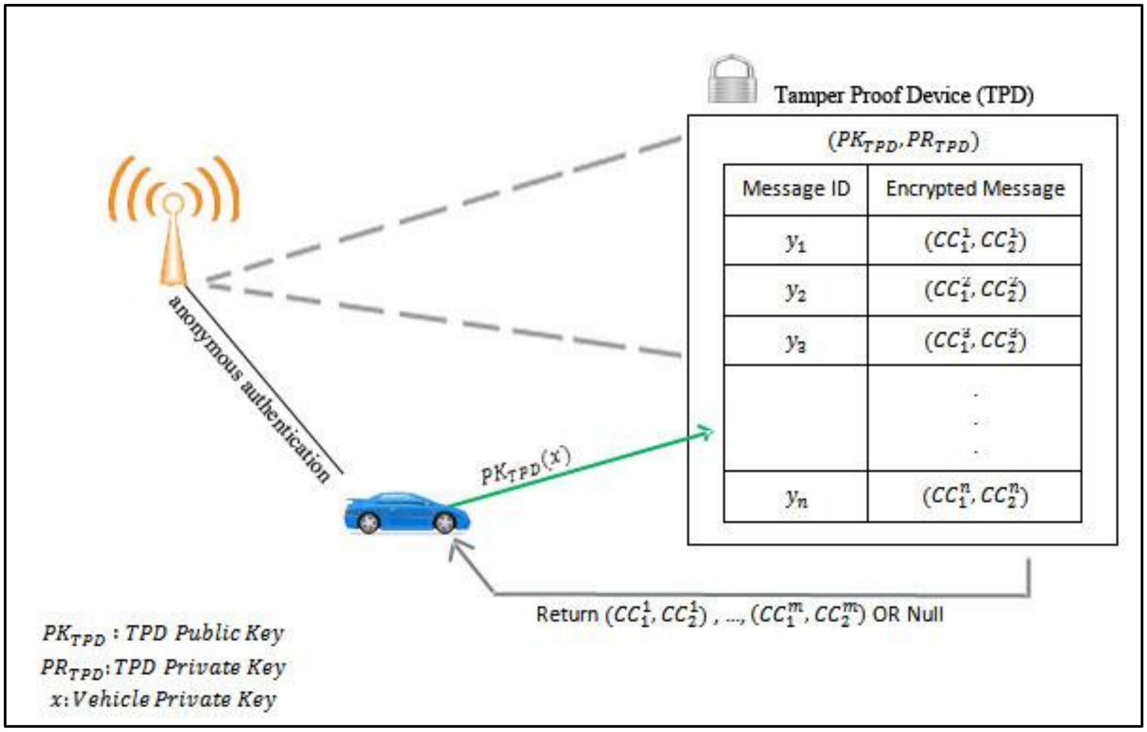


Figure 3-6. RSUs-based mix network

3.2.3.5 Message Retrieving Phase

When driving by an RSU, the vehicle first establishes a secure channel via an anonymous authentication protocol [15]. Then, the vehicle encrypts its private key by using the public key of RSU's TPD and submits the encrypted key to the TPD of the RSU as shown in Figure 3-7. Afterwards, the TPD will search through the message database resided in the TPD by using the vehicle's key and find out whether there are any messages destined for the vehicle. If not, the TPD retunes a null. If yes, the TPD will return the list of messages destined for the vehicle through the established secure channel between the vehicle and the RSU, and then send a management message to remove the delivered messages from all other RSUs. Afterwards, the vehicle can try to decrypt every encrypted message received from the RSU in order to retrieve its messages. Decryption performed is as follows:

$$\frac{cc_2}{(cc_1)^x} = plain\, m$$


Tamper Proof Device (TPD)
(PK_{TPD}, PR_{TPD})
anonymous authentication
$PK_{TPD}(x)$
Return (CC_1^1, CC_2^1) , ..., (CC_1^m, CC_2^m) OR Null
PK_{TPD} : TPD Public Key
PR_{TPD}: TPD Private Key
x: Vehicle Private Key

Message ID	Encrypted Message
y_1	(CC_1^1, CC_2^1)
y_2	(CC_1^2, CC_2^2)
y_3	(CC_1^3, CC_2^3)
	. . .
y_n	(CC_1^n, CC_2^n)

Figure 3-7. Retrieving messages from an RSU

3.3 Security Analysis

We analyzed the security for our proposed scheme in terms of following aspects: message analysis attack and message tracing attack.

Message analysis: in our proposed scheme, a sending vehicle v_s encrypts messages into $m = (c_1, c_2, c_3, c_4, c_5, c_6) = \left(g^k mod\ q, my^k\ mod\ q,\ g^{k'}, y^{k'}, g^{k''}, y.PK_{TPD}^{k''}\right)$ using destination vehicle v_d public key y and randomly chosen re-encryption factors $0 < k, k', k'' < q - 1$,yet without knowing destination secret key x. Therefore, an adversary will not be able to recover plain text message from m as decryption requires knowledge of intended receiver's private key x. Therefore, our proposed scheme is resistant to packet analysis attack.

Message traceability: here we consider that an adversary is able to eavesdrop in the vehicle-to-vehicle or vehicle-to-RSU communications. First, message destination is encrypted which prevents an adversary from knowing the destination information. Second, RSUs infrastructure utilizes re-encryption technique in which a received message $m = \left(g^{k} mod\ q, my^{k}\ mod\ q,\ g^{k'}, y^{k'}, g^{k''}, y.PK_{TPD}^{k''}\right)$ will be transformed into another form $\left((g)^{k\,k'}, (my)^{k\,k'}, (g)^{\,k'k_1}, (y)^{\,k'k_1}, g^{k_2}, y.PK_{TPD}^{k_2}\right)$, where $k_1\, and\, k_2$ are random re-encryption factor$s$ chosen from $0 < k_1, k_2 < q - 1$. Therefore, upon reaching an RSU, an adversary will not be able to recover sender's identity as message exchanged within RSUs are not linkable.

3.4 Performance Evaluation

The results of VANET simulation are heavily influenced by the quality of employed mobility model. Most of standalone network simulators use random waypoint mobility model as mobility model of choice. In this model, nodes move freely in random directions, which do not reflect car movements in real world scenarios. Fortunately, transportation and traffic engineering communities have been investigating and modeling realistic vehicles movements, where they have well established road traffic simulation tools. Therefore, using bi-directionally coupled road traffic simulator with an event-based network simulator, in which road traffic affects network traffic and vice versa, provides a realistic simulation for VANET.

We conducted our simulation using OMNET++ 4.1 [6] together with its INET-MANET framework extension as network simulator, while SUMO [7] microscopic road traffic simulation package as traffic simulator. OMNET++ is a discrete event network simulator which is composed of reusable intercommunicating models written in C++. INETMANET framework is a package of OMNET++ models that represent various internet layers and protocols for modeling wireless communication in ad-hoc networks. Finally, SUMO is a microscopic road traffic simulator that performs simulation of vehicles movements in big roads map with real structure (e.g. multiple lanes, traffic lights, and speed limits); it provides traffic control interface to give access and control for running simulation.

We use Veins [21] (Vehicle in Network Framework) to bi-directionally couple OMNET++ with SUMO. Veins creates a TCP connection between both simulators to allow dynamic and online interaction during the simulation. Using this connection, simulators can interact with each other by sending a series of commands (e.g. speed, position, reroute ... etc) during small time-steps to influence individual vehicles movements and resulted network traffic. For example, SUMO triggers the simulation for one timestep, then sends the resulted mobility trace to OMNET++ which triggers updates for nodes position and simulates network traffic; OMNET++ then buffers commands and proceeds to the next timestep.

Unfortunately, Veins does not implement all available commands in SUMO traffic control interface, which limits the interaction with mobility trace. Therefore, we had to extend Veins framework to provide more control commands to serve the purpose of simulate our proposed data forwarding protocol for VANET. Specifically, we provide

GPS like functionality to nodes in OMNET++, so a node knows its complete route information at any given time interval which allows it to judge if it will by-pass an RSU or not. Moreover, we implemented an interface to translate SUMO map coordinates into OMNET++ playground coordinates in order to efficiently deploy RSUs infrastructure in the simulation. The complete simulation framework is shown in Figure 3-8.

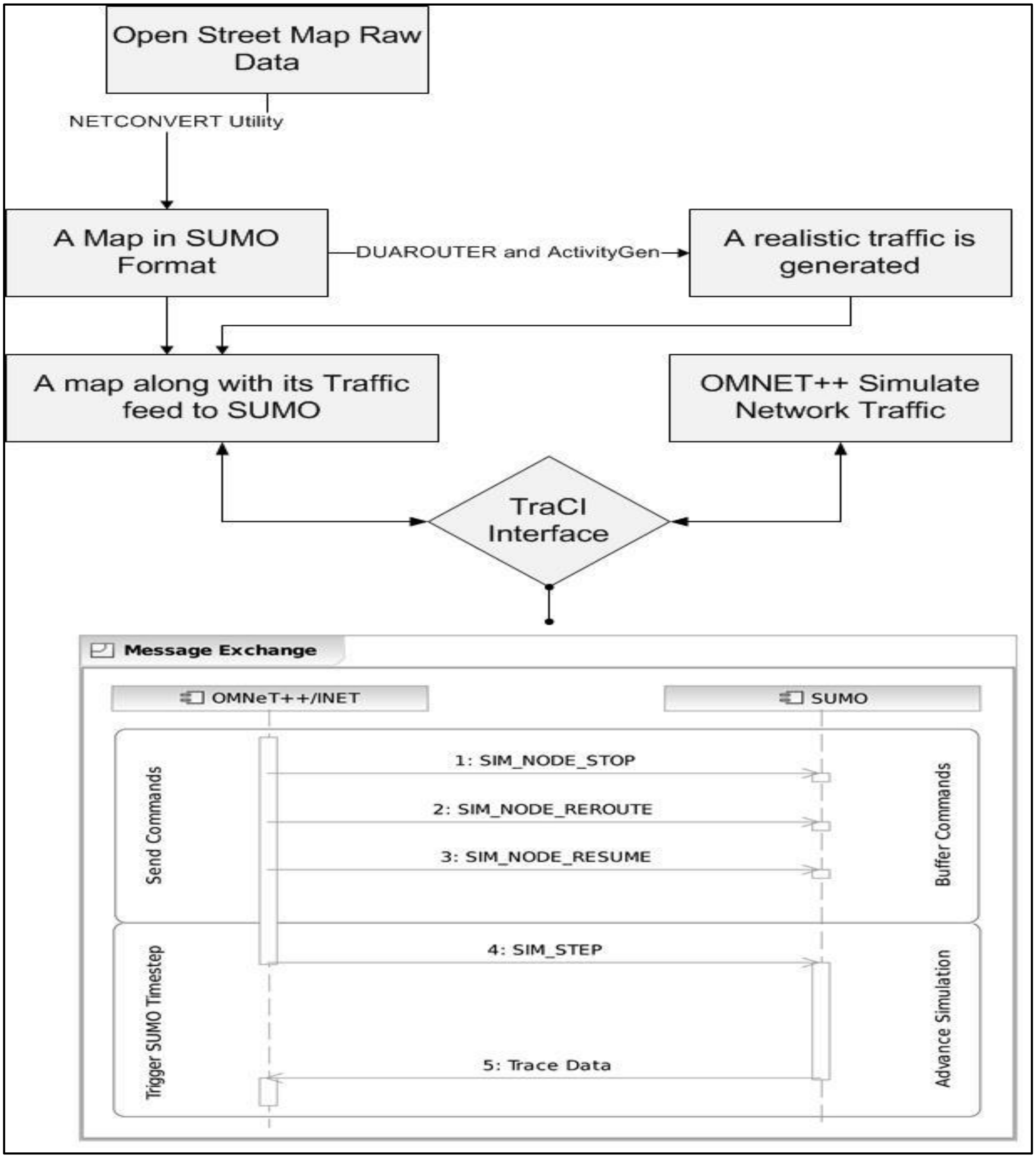


Figure 3-8. Simulation framework

3.4.1 Simulation Setup

Map layout: for the purpose of this simulation, we used a city of Oshawa with a region of 11 km × 8 km to serve the roads layout, as shown in Figure 3-9. The map data were taken from publicly available Openstreetmap[1] project. The map data includes all roads attributes such as speed limits, lanes count, stop signs, road type, and driving direction. We were able to convert raw map data into a street network that is understandable by SUMO, while preserving all road attributes. We achieved map conversion by using a utility called *netconvert* that is included with SUMO package.

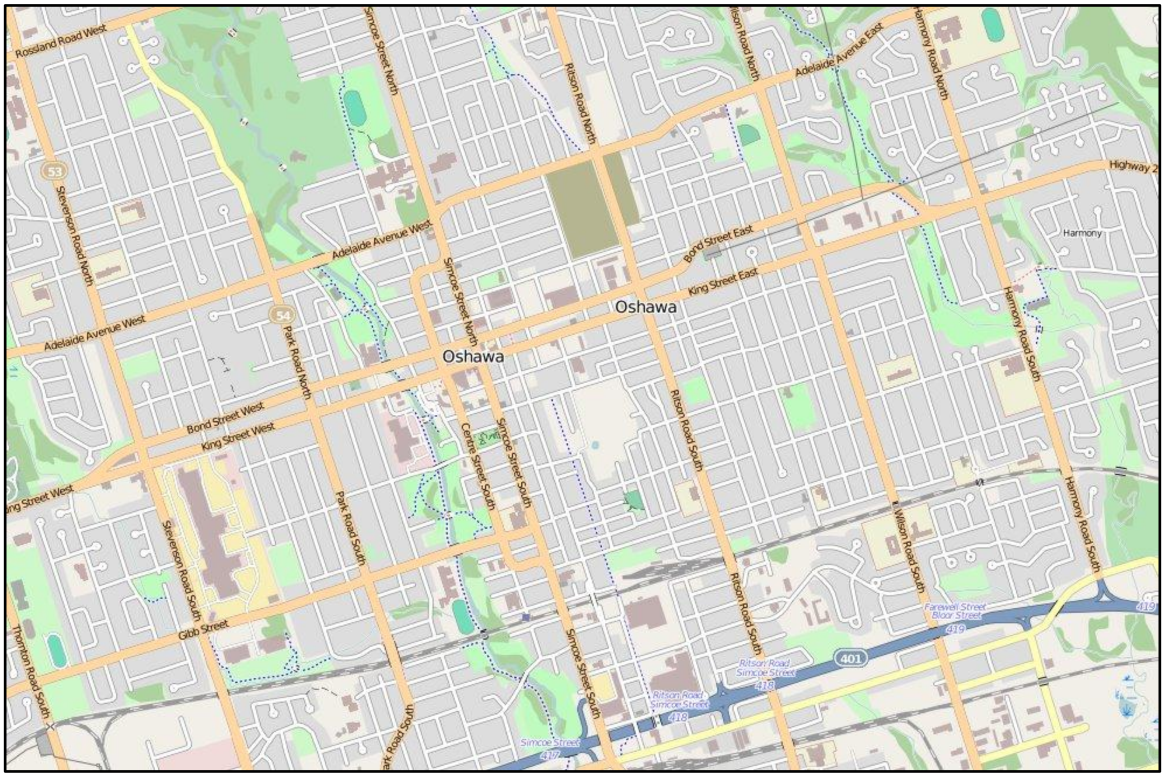


Figure 3-9. City of Oshawa region considered for simulation

[1] http://www.openstreetmap.org/

Artificial Mobility Traces: most realistic car movements are generated from real trace files that are collected from real world measurements. Since real world traces are not available, especially for the city of Oshawa, we manually generated trace files for vehicle movements based on sumo microsimulation models. Specifically, we generated three sets of trace files, where each set contains traces for 200 vehicles. In the traces, vehicles trips are defined, where every vehicle departs from a random residential area, and goes to a random activity center in the city, then destines to other residential area. Vehicle routes are computed using the shortest path computation, which takes into account street length, speed limits, lane count, and street type. Each trace file captures vehicles movements in the city within 4 minutes. Moreover, for more realistic scenario, traffic obstructions are introduced during simulation time by forcing random vehicles to stop for 20-70 seconds. By doing this, we force following vehicles to reroute around traffic or stuck on it.

Vehicles: The following table shows the vehicles parameters that are used by SUMO to represent vehicles and driving behavior.

Maximum Vehicle Speed	14m/s
Vehicle Acceleration	2.5m/s^2
Vehicle deceleration	4.6m/s^2
Vehicle length	5m
Driver imperfection	0.5

Table 3-1 SUMO parameters

Network configuration: all communications were approximated to resemble IEEE 802.11p protocol. The details of parameters setting that used to parameterize INETMANET framework models are described in Table 3-2:

Network Layer Interfaces to transport layer: TCP, UDP, echo/ping, RSVP	arp.retryCount	3
	arp.retryTimeout	1s
	arp.cacheTimeout	100s
WiFi Link layer NIC implements an 802.11 network interface card in ad-hoc mode	mac.address	auto
	mac.bitrate	11Mbps
	radio.transmitterPower	2mW
	radio.thermalNoise	-110dBm
	radio.pathLossAlpha	1.9
	radio.snirThreshold	3dB
	radio.sensitivity	-85dBm
Channel Control Info used radio interfaces of nodes at transmissions	carrierFrequency	2.4GHz
	channelcontrol.pMax	2mW
	channelcontrol.sat	-80dBm
	channelcontrol.alpha	1.9
Message Related Parameters Defines parameters for packets that are exchanged between communicating parties	Message Size	100Kb
	Message TTL	Close to simulation time
	Buffer Size	50Mb

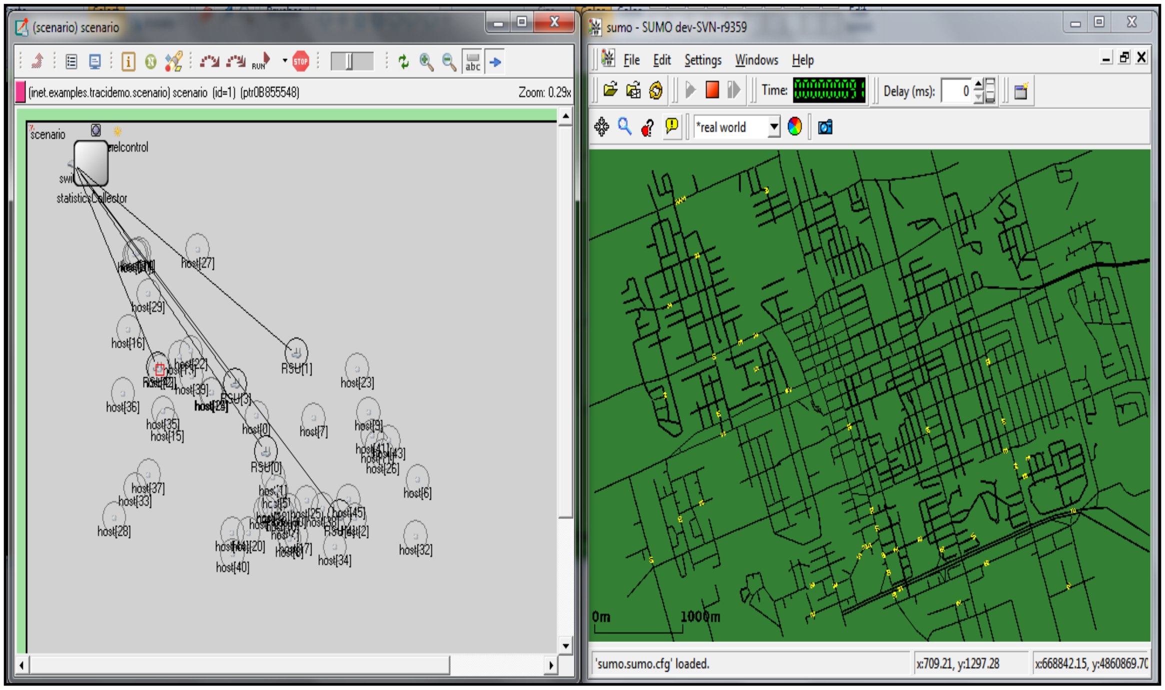
Table 3-2 INETMANET framework parameters

In order to fully estimate our proposed protocol performance, four different scenarios are simulated.

Scenario 1	No RSU deployment, cars send messages using epidemic routing with large buffer size 1000MB (nodes will have sufficient memory to help forward any message).
Scenario 2	No RSU deployment, cars send messages using epidemic routing with limited buffer size 1MB (around 10 messages).
Scenario 3	Random RSU deployment, cars send messages using our proposed protocol.
Scenario 4	Social-based RSU deployment, cars send messages using our proposed protocol.

Table 3-3 Simulation scenarios

For each scenario, we run the simulation for 5 minutes (based on average traveling time for vehicles to complete their trips where vehicles departs at random intervals), and average performance result are reported using over 5 runs with five different trace files. Figure 3-10 shows road traffic and network simulators running side by side.



'sumo.sumo.cfg' loaded.

Figure 3-10. SUMO and OMNET++ exchanging data online

3.4.2 Simulation Results

Delivery Ratio: Figure 3-11, shows the average delivery in the four different scenarios. In Scenario 1, the delivery ratio is high (around 93%) as all vehicles help in forwarding messages, and also messages have long Time-to-Live (close to simulation time). However, when we limit vehicles available buffer (Table 3-3), delivery ratio dropped as less vehicles are helping in forwarding messages. We can also observe that social based RSU deployment (Section 3.2.1.2) can achieve a much better delivery ratio than a random RSU deployment, as more vehicles will be driving by RSUs in simulation area. In brief, Epidemic routing in Scenario 1 achieves high delivery ratio at expense of increased use of resources such as buffer space, bandwidth, and transmission power, where our routing protocol in Scenario 4 achieved efficient delivery with minimum use of recourses.

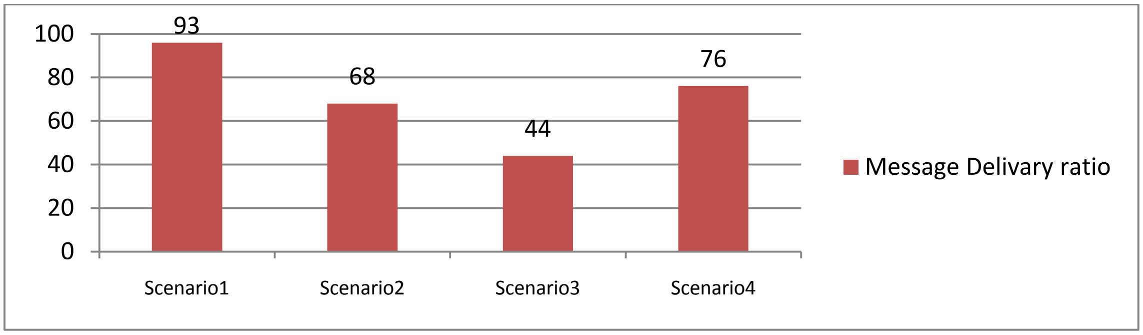


Figure 3-11. Avarage delivery ratio

Message overhead: Figure 3-12 illustrates the message overhead for each scenario. In Scenario 1, the message overhead is massive as vehicles within sending range exchange all messages in their buffer; however, the messages overhead in Scenario 2 drops dramatically as buffer size is small which limits the number of exchange messages. From the same figure, we can also see that the message overhead in Scenario 4 is larger than Scenario 3 as more vehicles are willing to help in forwarding messages because the likelihood of driving by an RSU is higher. However, for both Scenarios 3 and 4, the message overhead is still very lower comparing to Scenario 1, epidemic routing.

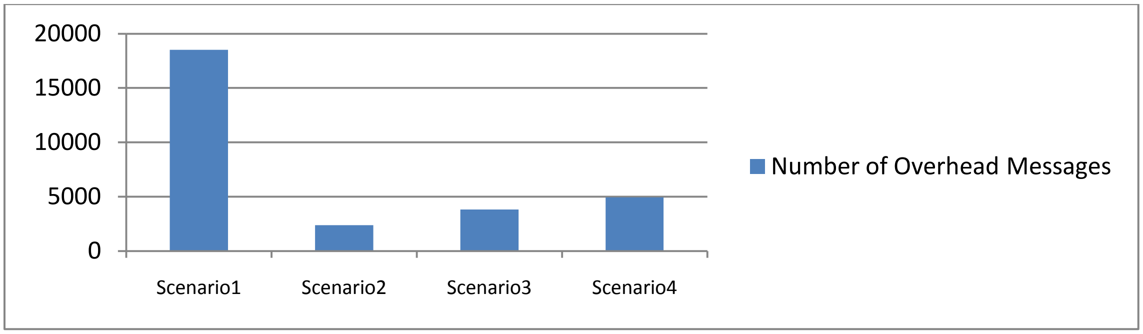


Figure 3-12. Average messages overhead

Average Delay: Figure 3-13 depicts the message delay measures for different scenarios in multiple runs. In Scenario 1, we can see that mean delay is much lower than all other scenarios as the number of duplicated messages increases which makes the opportunity to meet destinations much faster. In Scenarios 3 and 4, messages are forwarded and temporarily stored in RSUs which achieves high delivery, yet it has an impact on delay. However, this delay is manageable by delay tolerant applications that require high delivery ratio. Another observation is that social based RSUs deployment has lower delay than random RSUs deployment, as the likelihood for a destination to pass by social RSU is much higher. Briefly, although Epidemic routing in Scenario 1 achieves minimum delivery delay, it consumes too much recourses such as bandwidth, battery, and buffer space as nodes continuously replicate and transmit messages; however, our proposed protocol demonstrated efficient trade-off between delivery delay and resource consumption,

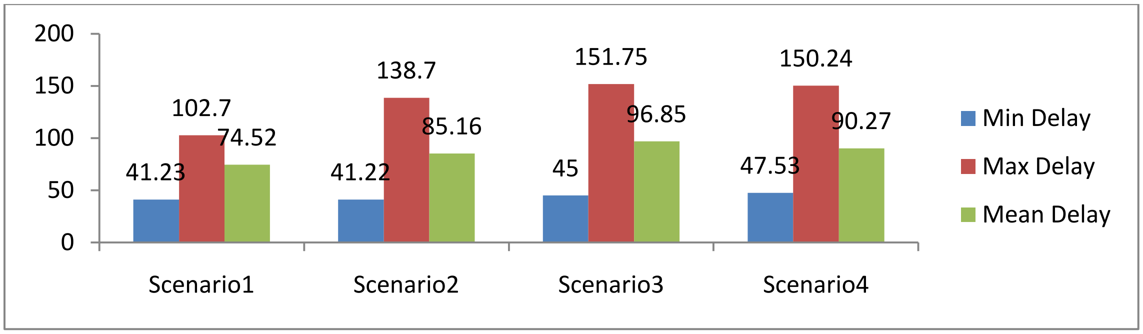


Figure 3-13. Message delay metrics

Number of forwarding hops: Figure 3-14 shows hops metrics for each scenario. In Scenario 1, the number of hops that a message can traverse to reach destination is larger than all other scenarios as vehicles have infinite buffer that can carry a large number of messages; however, when the buffer size is limited as in Scenario 2, the number of hops that a message traverse to reach a destination drops dramatically as vehicle reach their buffer limits and stop helping in forwarding messages. In Scenarios 3 and 4, the number of hops that messages traverse is much lower as the goal for vehicles is to forward messages to closest RSU which later ignores duplicated messages.

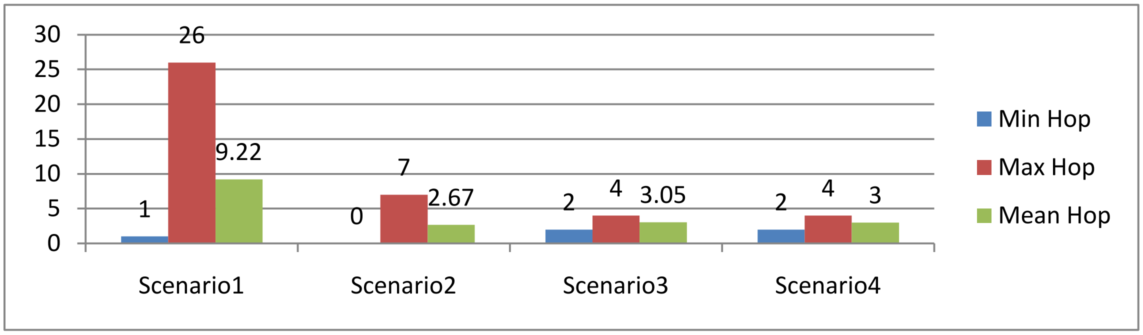


Figure 3-14. Forwarding hops metrics

In summary, our proposed Social-Based Data Forwarding Protocol can achieve efficient data delivery with low messages overhead. It imposes delay on message delivery; however, this delay is acceptable for many delay tolerant application that requires high delivery ratio.

Our proposed protocol meets the following security requirement. It guarantees message integrity as all messages are encrypted prior to sending. It also provides adequate privacy preservation for senders and receivers as it utilize mix network technique in RSUs infrastructure.

In the next chapter, we propose an efficient vehicle social evaluation (EVSE) scheme, which enables each vehicle to show its authentic social evaluation to others while without disclosing its past location information. As a result, it can meet the prerequisites for the success of social aware data diffusion in VANETs.

Chapter 4

An Efficient Vehicle Social Evaluation Scheme with Location Privacy Preservation for Vehicular Communications

4.1 Introduction and Motivation

Vehicular Ad Hoc Network (VANET), as a special mobile ad hoc network, has been increasingly recognized as an ideal solution to the improvement of road safety [22]. In a typical VANET, each vehicle is equipped with wireless On Board Unit (OBU) device, which allows vehicles to communicate not only with each other, but also to the Roadside Units (RSUs), i.e., wireless infrastructure deployed along the roadside. Through hybrid vehicle-to-vehicle (V-2-V) and vehicle-to-RSU (V-2-I) communications, VANET can make better the transportation's safety and efficiency by sharing the potential emergency situations and traffic jams to all vehicles. In addition to the safety-related applications, VANET can also offer many promising non-safety-related applications on the road. Information dissemination is one of the important non-safety-related applications in VANETs, which utilizes the vehicle's mobility and RSU's storage to help store-carry and forward data packets to their destinations [23]. However, due to the high mobility of vehicles, it is very hard to maintain the end-to-end connections, and thus the performance of information dissemination cannot be guaranteed. To cope with this issue, many efforts have been made on opportunistic forwarding to improve the performance of dissemination, including social-aware data diffusion in VANETs [24,25]. In a social-aware data diffusion, a source does not select any nodes it contacts as the relays to help disseminate packets. Instead, only those nodes with high social centrality, i.e., those which have more chances to contact other nodes, are selected to disseminate packets. As a result, the delay of data diffusion can be reduced.

In spite of the performance improvement in social-aware data diffusion, several new security and privacy challenges will be encountered in a VANET environment. First, since a vehicle claims its *high centrality* by itself without any security guarantee [25], a low centrality vehicle could lie its centrality, and the performance in social-aware data diffusion could suffer deterioration. Second, the location privacy is one of the important privacy requirements in VANETs [26], if a vehicle provides all of its past *authentic contact information* (including contact time, contact location) to show its high sociality, the location privacy of the vehicle will then be violated. Therefore, how to effectively tackle these security and privacy challenges is key to the success of social-aware data diffusion in VANETs.

Motivated by the mentioned above, in this thesis, we propose an E̲fficient V̲ehicle S̲ocial E̲valuation (EVSE) scheme with location privacy preservation for VANET. The proposed EVSE scheme is based on an efficient group signature [27], which enables each vehicle to show its *authentic social evaluation* to others while without disclosing its past location information. Specifically, the contributions of this paper are twofold: First, we present a location privacy-preserving social evaluation model with time slotting technique, where each vehicle can request a Social Evaluation Server (SES) to obtain its social evaluation in a new time slot according to its social witnesses collected in the previous time slot. SES can evaluate a vehicle's sociality, but cannot identify the vehicle's past location information. Second, we also develop a custom simulator built in Java to examine the performance of social-aware data diffusion consolidated by the proposed EVSE scheme.

The remainder of this chapter is organized as follows. In Section 2, we introduce the system model, security model and design goal. In Section 3, we review the bilinear pairing techniques which serve the base of the proposed scheme. Our proposed EVSE scheme is presented in Section 4, followed by its security analysis and performance evaluation in Section 5 and Section 6, respectively. Finally, we draw our conclusions in Section 7.

4.2 Models and Design Goal

In this section, we formalize the system model, security model, and identify our design goal.

4.2.1 System Model

We consider a single-authority VANET which consists of a trusted authority (TA), a social evaluation server (SES), a large number of vehicles, denoted by $\mathcal{V} = \{V_1, V_2, \cdots\}$, and some RSUs, denoted by $\mathcal{R} = \{R_1, R_2, \cdots\}$, as shown in Figure 4-1.

• TA: TA is a trustable and powerful entity, whose duty is to initialize the whole system, including registering SES, deploying RSUs, and granting a family of pseudo-IDs to each vehicle for achieving location privacy on the road.

- SES: SES is subordinated by TA, whose duty is to provide the *social evaluation service* to vehicles. Since a large number of vehicles may request the *social evaluation service*, SES should be also trustable and powerful.

- RSUs $\mathcal{R} = \{R_1, R_2, \cdots\}$: RSUs are deployed at some social areas. When a vehicle visits them, they will provide the witnesses to attest the vehicle's activities. In addition, RSUs can directly communicate with SES. Therefore, when vehicles request the *social evaluation service* from the SES, RSUs also act as relay nodes to help forward the transmission between vehicles and SES.

- Vehicles $\mathcal{V} = \{V_1, V_2, \cdots\}$: Vehicles move in some areas, each vehicle $V_i \in \mathcal{V}$ is equipped with OBU device, which allows vehicles to communicate not only with each other for helping disseminate data, but also to RSUs for collecting social witnesses.

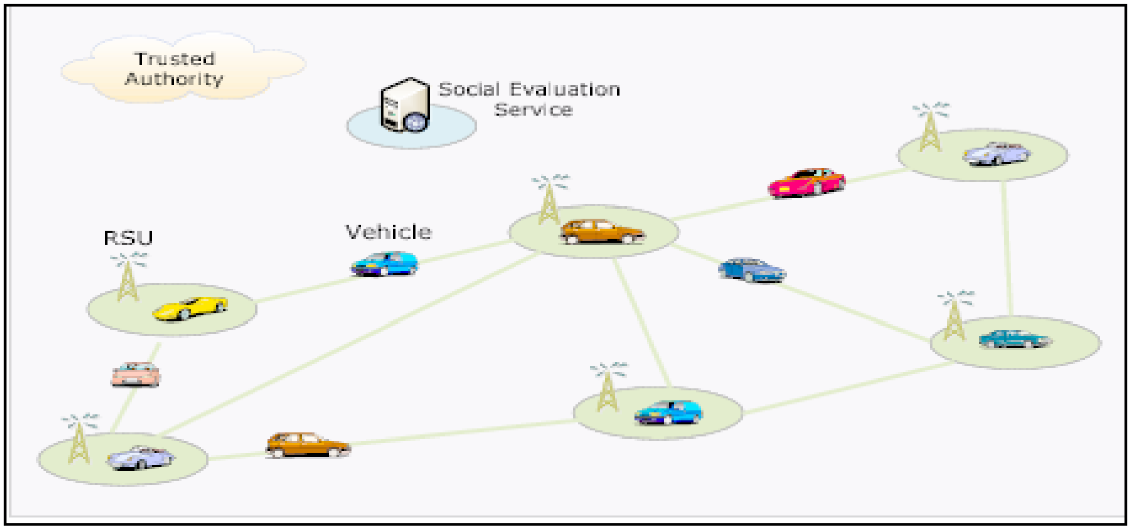


Figure 4-1. System model under consideration

4.2.2 Security Model

In our security model, we mainly focus on how to protect a vehicle's location privacy when it requests SES for the *social evaluation service* and when it shows its high sociality to other vehicles in the social-aware data diffusion phase on the road. Specifically, we consider a *privacy-curious* adversary, which does not actively attack vehicles for obtaining their location information. Instead, it moves on the road to passively eavesdropping a vehicle's social witnesses. In addition to the *privacy-curious* adversary, we consider SES is also *privacy-curious*, i.e., it is curious about vehicle's location, though it faithfully evaluates vehicle's sociality. Note that, in our current work, we only consider a local *privacy-curious* adversary which is interested in identifying vehicle location information, but only has a local communication view.

4.2.3 Design Goal

To resist the above *privacy-curious* adversary, our design goal is to develop an efficient vehicle social evaluation scheme with location privacy preservation for VANET. Specifically, the following desirable properties should be achieved.

• *The proposed scheme should protect a vehicle's real identity when SES evaluates its sociality.* Since VANET is implemented in civilian scenarios, the real identity is very sensitive to the drivers [28]. As a result, a vehicle's real identity should not be disclosed to SES.

• *The proposed scheme should protect the locations that a vehicle visited when SES evaluates the vehicle's sociality.* Since SES is *privacy-curious*, when it evaluates a vehicles's sociality, it may be curious about a vehicle's past location information. Therefore, the location information that a vehicle visited in the past should be also concealed from SES. However, to avoid the double-count in social evaluation, if more than one witnesses indicate the same location that the vehicle visited, these witnesses should be linked, though the real location information is still unknown.

With the above properties, a vehicle can show its sociality to other vehicles while protecting its location privacy on the road. As a result, an efficient social-aware data diffusion can be achieved in VANETs.

4.3 Bilinear Pairing Technique

Let $\mathbb{G}$, $\mathbb{G}'$ and $\mathbb{G}_T$ be three multiplicative cyclic groups of the same prime order q, and g, g' be the generators of $\mathbb{G}$, $\mathbb{G}'$, respectively. There exists a homomorphism ψ from $\mathbb{G}$ to $\mathbb{G}'$ such that $g = \psi(g')$. Suppose $\mathbb{G}$, $\mathbb{G}'$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e: \mathbb{G} \times \mathbb{G}' \rightarrow \mathbb{G}_T$ such that $e(g, g') \neq 1_{\mathbb{G}_T}$ and $e(u^a, v^b) = e(u, v)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $u \in \mathbb{G}$, $v \in \mathbb{G}'$. We refer to [27,29] for a more comprehensive description of pairing technique, and complexity assumptions.

Definition 1 A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter κ as input, and outputs a 7-tuple $(q, \mathbb{G}, \mathbb{G}', \mathbb{G}_T, g, g', e)$, where q is a κ-bit prime number, $\mathbb{G}, \mathbb{G}', \mathbb{G}_T$ are three groups with order q, $g \in \mathbb{G}$, $g' \in \mathbb{G}'$ are two generators with the homomorphism relation $g = \psi(g')$, and $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map, i.e., $e(g, g') \neq 1_{\mathbb{G}_T}$.

4.4 Proposed Efficient Vehicle Social Evaluation Scheme with Location Privacy Scheme

In this section, we present our efficient vehicle social evaluation (EVSE) scheme with location privacy preservation for VANETs, which mainly consists of the following three parts: system initialization, social witness collection, and vehicle social evaluation.

4.4.1 System Initialization

In the system initialization, the TA initializes the system parameters in an offline manner, and registers vehicles, RSUs and SES as well. Specifically, the TA runs the following steps.

Step 1. Given the security parameter κ, the bilinear parameters $(q, \mathbb{G}, \mathbb{G}', \mathbb{G}_T, g, g', e)$ are first chosen, where $|q| = \kappa$. Then, TA selects a random number $\gamma \in \mathbb{Z}_q^*$ as the *master key*, and computes the corresponding public key $w = g'^{\gamma} \in \mathbb{G}'$. In addition, TA chooses a secure symmetric encryption algorithm $\mathbf{Enc}()$, and two cryptographic hash functions H and H_0, where $H: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$ and $H_0: \{0,1\}^* \rightarrow \mathbb{G}'^2$. In the end, TA sets the public system parameters $params$ as $(q, \mathbb{G}, \mathbb{G}', \mathbb{G}_T, g, g', e, w, \mathbf{Enc}(), H, H_0)$.

Step 2. For the SES, TA generates its private key $A_0 = g^{\frac{1}{\gamma + H(SES)}} \in \mathbb{G}$, which is used for signing the vehicle's social attestation.

Step 3. TA divides a whole area $\mathcal{A}rea$ into n sub-areas $\mathcal{A}rea = \{SA_1, SA_2, \cdots, SA_n\}$, and deploys an RSU R_i at each $SA_i \in \mathcal{A}rea$, which can be identified by passing-by vehicles. For each RSU R_i at SA_i , TA generates its private key $sk_i = (x_i, A_i)$, where $x_i \in \mathbb{Z}_q^*$, and $A_i = g^{\frac{1}{\gamma + x_i}} \in \mathbb{G}$, which is used by RSU R_i for signing vehicle's social witness.

Step 4. When a vehicle $V_i \in \mathcal{V}$ registers itself in the system, TA grants a family of pseudo-IDs $PID = \{pid_0, pid_1, \cdots\}$, and the corresponding private key $S_i = g^{\frac{1}{\gamma + H(pid_i)}}$ for each pid_i. It is worth noting that pid_0 is used by V_i to collect the social witnesses, and V_i periodically changes its other pseudo-IDs $PID/\{pid_0\}$ for achieving the location privacy on the road.

4.4.2 Social Witness Collection

To achieve the location-privacy preserving social witness collection, the time should be slotted, As shown in Figure 4-2. At each time slot T_i, e.g., one day, $V_i \in \mathcal{V}$ only uses a subset pseudo-IDs $PID_i \subset PID$, and discards them in the next slot. The sociality of these pseudo-IDs PID_i in slot T_i is evaluated by the vehicle's activities in the previous time slot T_{i-1}. In the following, we describe the procedure of the social witness collection in detail.

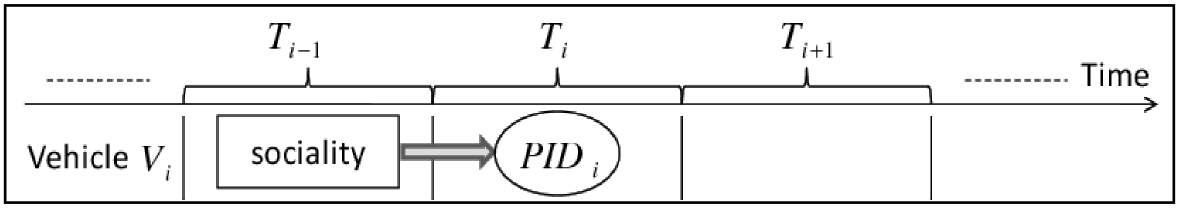


Figure 4-2. Time is slotted for achieving location-privacy preserving social witness collection in VANETs

Assume the vehicle $V_i \in \mathcal{V}$ continually moves in the area $\mathcal{A}rea$ in time slot T_{i-1}. When V_i visits a sub-area $SA_j \in \mathcal{A}rea$, it contacts the RSU R_j in SA_j for collecting the social witness. Specifically, the following steps will be executed by V_i and R_j.

Step 1. V_i picks up the current timestamp t_c, and uses the pseduo-ID pid_0 and the private key $S_0 = g^{\frac{1}{\gamma + H(pid_0)}}$ to make an ID-based signature $\sigma = (\alpha, \beta)$ as

$$\alpha = H(t_c||r), \quad \beta = S_0^{x+\alpha} = \left(g^{\frac{1}{\gamma + H(pid_0)}}\right)^{x+\alpha}$$

where $x \in \mathbb{Z}_q^*$ is a random number, and $r = e(g, g')^x \in \mathbb{G}_T$ [30]. Then, V_i sends the request $\sigma||t_c||pid_0$ to the RSU R_j for authentication.

Step 2. After receiving $\sigma||t_c||pid_0$, RSU R_j checks

$$\alpha \overset{?}{=} H\big(t_c||e(\beta, g'^{H(pid_0)}w)e(g, g')^{-\alpha}\big)$$

If it holds, R_j accepts the request, and executes the next step; otherwise, R_j rejects the request. The correctness is as follows:

$$\begin{aligned}
& e(\beta, g'^{H(pid_0)}w)e(g, g')^{-\alpha} \\
= \quad & e\left(\left(g^{\frac{1}{\gamma + H(pid_0)}}\right)^{x+\alpha}, g'^{H(pid_0)+\gamma}\right)e(g, g')^{-\alpha} \\
= \quad & e(g, g')^{x+\alpha}e(g, g')^{-\alpha} = e(g, g')^x = r
\end{aligned}$$

Step 3. To provide the location privacy-preserving social witness of vehicle V_i with group signature [27], R_j first obtains the generators

$$(u', v') = H_0(w||pid_0||T_{i-1}) \in \mathbb{G}'^2$$

with the pseudo-ID pid_0 in time slot T_{i-1}, then computes their images $u = \psi(u')$ and $v = \psi(v')$. Then, R_i chooses a random number $\lambda \in \mathbb{Z}_q^*$ and computes:

$$T_1 = u^\lambda, T_2 = A_j v^\lambda, \delta = x_j \lambda \mathrm{mod} q$$

From the random numbers $r_1, r_2, r_3 \in \mathbb{Z}_q^*$, R_j computes the helper values:

$$\begin{aligned} \pi_1 &= u^{r_1}, \pi_3 = T_1^{r_2} \cdot u^{-r_3} \\ \pi_2 &= e(T_2, g')^{r_2} \cdot e(v, w)^{-r_1} \cdot e(v, g')^{-r_3} \end{aligned}$$

After computing $c = H(w||pid_0||T_{i-1}||t_c||T_1||T_2||\pi_1||\pi_2||\pi_3)$, RSU R_j further calculates $s_1 = r_1 + c\lambda \text{mod} q, s_2 = r_2 + cx_j \text{ mod } q, s_3 = r_3 + c\delta \text{ mod} q$, and forms the social witness as

$$W_j = (pid_0, T_{i-1}, c, T_1, T_2, s_1, s_2, s_3)$$

In the end, the RSU R_j sends the social witness W_j back to vehicle V_i.

Step 4. After receiving the social witness $W_j = (pid_0, T_{i-1}, c, T_1, T_2, s_1, s_2, s_3)$, vehicle V_i can check its validity as follows,

- Compute $(u', v') = H_0(w||pid_0||T_{i-1})$ and their images $(u, v) \in \mathbb{G}$;
- Compute the helper data (π_1, π_2, π_3) as

$$\begin{aligned} \pi_{1'} &= u^{s_1}/T_1^c, \pi_{3'} = T_1^{s_2} \cdot u^{-s_3} \\ \pi_{2'} &= e(T_2, g')^{s_2} \cdot e(v, w^{s_1} g'^{s_3})^{-1} \cdot (e(T_2, w)/e(g, g'))^c \end{aligned}$$

- Check if $c = H(w||pid_0||T_{i-1}||t_c||T_1||T_2||\pi_{1'}||\pi_{2'}||\pi_{3'})$, and accept the social witness W_j accordingly. The correctness is as follows:

$$\begin{aligned} \pi_{1'} &= u^{s_1}/T_1^c = u^{r_1 + c\lambda}/u^{c\lambda} = u^{r_1} = \pi_1 \\ \pi_{3'} &= T_1^{s_2} \cdot u^{-s_3} = T_1^{r_2 + cx_j} \cdot u^{-r_3 - c\delta} = T_1^{r_2} \cdot u^{-r_3} = \pi_3 \\ \pi_{2'} &= e(T_2, g')^{s_2} \cdot e(v, w^{s_1} g'^{s_3})^{-1} \cdot (e(T_2, w)/e(g, g'))^c \\ &= e(T_2, g')^{r_2 + cx_j} e(v, w)^{-r_1 - c\lambda} e(v, g')^{-r_3 - c\delta} \\ &\quad \cdot e(T_2, g')^{\gamma c}/e(g, g')^c \\ &= e(T_2, g')^{r_2} e(v, w)^{-r_1} e(v, g')^{-r_3} = \pi_2 \end{aligned}$$

After getting the social witness in sub-area SA_j, vehicle V_i moves to other subareas and utilizes the same procedure to collect the social witnesses there.

4.4.3 Vehicle Social Evaluation

Suppose that vehicle V_i collected l social witnesses $W = \{W_1, W_2, \cdots, W_l\}$ in time slot T_{i-1}. At the beginning of time slot T_i, vehicle V_i first chooses a subset pseudo-IDs $PID_i = \{pid_{i1}, pid_{i2}, \cdots, pid_{im}\}$, which will be used in time slot T_i, and then submits these pseudo-IDs and social witnesses W to SES for social evaluation. Specifically, the following steps will be executed between vehicle V_i and SES.

- V_i first chooses a random number $x \in \mathbb{Z}_q^*$, uses its pseudo-ID pid_0, the private key $g^{\frac{1}{\gamma+H(pid_0)}}$, and SES's identity to compute $r = e(g, g')^x$, and α, β, c_1 and c_2, where

$$\begin{aligned} \alpha &= H(W||PID_i||r), \beta = \left(g^{\frac{1}{\gamma+H(pid_0)}}\right)^{x+\alpha} \\ c_1 &= \left(w \cdot g'^{H(SES)}\right)^x, c_2 = \mathbf{Enc}_r(\alpha||\beta||pid_0||W||PID_i) \end{aligned}$$

Then, V_i submits $c_1||c_2$ to SES via an RSU it contacted on the road.

- After receiving $c_1||c_2$ relayed by RSU, SES first uses its private key $A_0 = g^{\frac{1}{\gamma+H(SES)}}$ to compute

$$e(c_1, A_0) = e\left(g^{\frac{1}{\gamma+H(SES)}}, \left(w \cdot g'^{H(SES)}\right)^x\right) = r$$

and then uses r to decrypt $\alpha||\beta||pid_0||W||PID_i$ from c_2.

If $\alpha = H\left(W||PID_i||e(\beta, g'^{H(pid_0)}w)e(g, g')^{-\alpha}\right)$, SES accepts the social evaluation request. Then, SES evaluates V_i's sociality in time slot T_{i-1} by invoking the Algorithm 2 with input of (W, PID_i). Finally, SES sends the output $\widetilde{PID}_i$ of Algorithm 2 back to V_i via RSU.

```
procedure Vehicle social evaluation
Input: social witnesses $W = \{W_1, W_2, \cdots, W_l\}$ in time slot $T_{i-1}$ and Pseudo-IDs $PID_i = \{pid_{i1}, pid_{i2}, \cdots, pid_{im}\}$ used in time slot $T_i$
Output: social-evaluated pseudo-IDs $\widetilde{PID}_i$ used in time slot $T_i$
    set the social evaluation $\mathbf{se} = 0$, and $\mathbb{P} = \phi$, $\widetilde{PID}_i = \phi$
    $\boldsymbol{for}$ $x := 1$ to $l$ do
        check the validity of $W_x = (pid_0, T_{i-1}, c, T_1, T_2, s_1, s_2, s_3)$
        compute $(u', v') = H_0(w||pid_0||T_{i-1}) \in \mathbb{G}'$ and $P_x = e(T_2, u')/e(T_1, v')$
        If social witness $W_x$ is valid, and $P_x$ is different from any element in $\mathbb{P}$ do
            set $\mathbf{se} = \mathbf{se} + 1$ and $\mathbb{P} = \mathbb{P} \cup \{P_x\}$
        end if
    end for
    for $y := 1$ to $m$ do
        generate a signature $\sigma_{iy}(pid_{iy}||\mathbf{se})$ on pseudo-ID $pid_{iy}$ and social value se
        set $\widetilde{PID}_i = \widetilde{PID}_i \cup \{pid_{iy}||\mathbf{se}||\sigma_{iy}\}$
    end for
    return $\widetilde{PID}_i$
end prosedure
```

Algorithm 2 Vehicle social evaluation

- After receiving these social-evaluated pseudo-IDs $\widetilde{PID}_i$ from SES, vehicle V_i can use these pseudo-IDs $\{pid_{i1}||\mathbf{se}||\sigma_{i1}, pid_{i2}||\mathbf{se}||\sigma_{i2}, \cdots, pid_{im}||\mathbf{se}||\sigma_{im}\}$ in time slot T_i. Since V_i will not disclose its past location information when it shows its sociality to other vehicles, V_i is willing to help with forwarding packets. As a result, social-aware data diffusion can be implemented in VANETs.

4.5 Security Analysis

In this section, we analyze the security properties of the proposed EVSE scheme. Specifically, our analysis will focus on how the proposed EVSE scheme can achieve vehicle's location privacy in social evaluation.

• *The proposed EVSE scheme can protect a vehicle's real identity.* In the system initialization, TA grants a family of pseudo-IDs $PID = \{pid_0, pid_1, \cdots\}$ to each vehicle, and each vehicle periodically changes its pseudo-IDs on the road, so vehicle's real identity can be protected. Although a vehicle uses the same pseudo-ID pid_0 to collect social witnesses from RSUs and gain social evaluation from SES, the real identity also cannot be revealed from pid_0.

• *The proposed EVSE scheme can protect a vehicle's past location information.* In the proposed EVSE scheme, each social witness W_j is the group signature [27], which asserts a vehicle really visited a subarea, but does not reveal the real subarea. Therefore, the vehicle's past location information can be protected. In addition, since the group signature [27] has the ability to link two social witnesses $W_j^{(1)}, W_j^{(2)}$ signed by the same RSU R_j in the same time slot T_{i-1}, i.e., $P_j^{(1)} = e(T_2^{(1)}), u')/e(T_1^{(1)}, v') = P_j^{(2)} = e(T_2^{(2)}), u')/e(T_1^{(2)}, v') = e(A_j, u')$. As a result, it can avoid the double-evaluation in SES's privacy-preserving social evaluation.

Based on the above analysis, the proposed EVSE scheme can enable a vehicle to show its authentic sociality to other vehicles while protecting its location privacy on the road, i.e., a local *privacy-curious* adversary cannot identify a vehicle's past location information from sociality.

4.6 Performance Evaluation

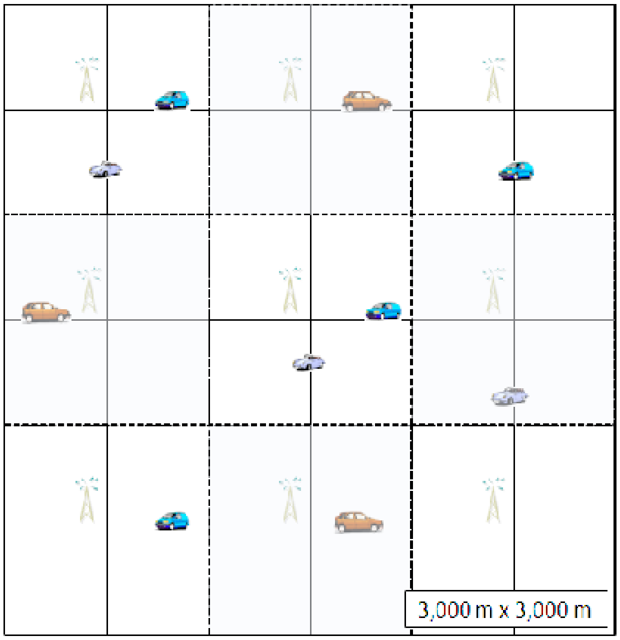
In this section, we use a custom simulator built in Java to study the effectiveness of social-aware data diffusion in VANETs. The performance metric used in the evaluation is the average diffusion delay (ADD), which is defined as the average time between when a packet is generated and when it is successfully disseminated to some deployed RSUs.

4.6.1 Simulation Setup

In the simulation, an interest area of $3{,}000 \times 3{,}000\ m^2$ is first divided into 9 sub-areas, where each sub-area has an RSU with transmission radius of 500 meters, as shown in Figure 4-3. In addition, 100 vehicles with transmission radius of 60 meters are moving in the area.

Mobility model. In VANETs, the social evaluation of a vehicle is highly contingent upon the mobility of the vehicle. In our simulation, we model the following mobility pattern of vehicles. Let D_0 denote the decision that a vehicle stays at the current sub-area, and D_1 be the decision that the vehicle leaves the current sub-area to another one. Each vehicle stays at its current sub-area for 2 minutes, and then makes the decision D_1 with probability ρ, and the decision D_0 with the probability $1-\rho$, as shown in Figure 4-4.

Once a decision is determined, a vehicle will choose a destination and move there by following the map-based shortest path routing with average velocity 20 km/h. In addition, when a vehicle is ready to leave its current sub-area, it will contact the deployed RSU for social witness collection.



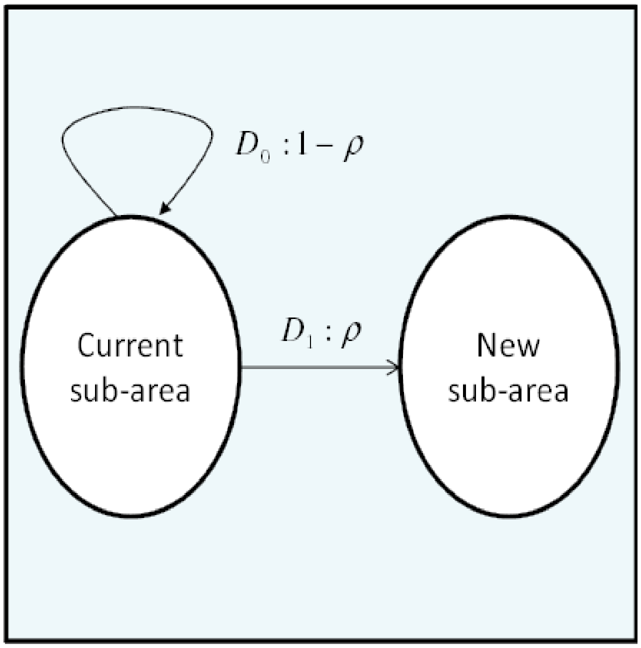


Figure 4-3. Simulation area

Figure 4-4. Vehicle mobility model

To verify the social-aware data diffusion in VANETs, we equally divide the total 100 vehicles into 5 groups $\mathcal{G} = \{\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4, \mathcal{G}_5\}$, and the vehicles in the same group $\mathcal{G}_i \in \mathcal{G}$ have the same probability ρ_i on decision D_1. Then, based on the above mobility model, we statistically test the average social evaluation of each group, and check the corresponding ADD in terms of different group's data diffusion. The detailed parameter settings are summarized in Table 4-1.

Parameter	Setting
Simulation area	$3{,}000 \times 3{,}000\text{m}^2$
Number of sub-areas	9
Number of vehicles in $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4, \mathcal{G}_5$	20,20,20,20,20
Decision D_1 probability $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$	$10\%, 30\%, 50\%, 70\%, 90\%$
Transmission radius of RSU, vehicles	500 m, 60 m
Average velocity of vehicles	20 km/h

Table 4-1 Simulation settings

Let the time slot be one hour in the simulation. After the social witness collection in the first time slot, we calculate the social evaluation of each vehicle at the beginning of the second time slot. Then, a source $\mathbf{s}$ randomly generates a packet, and requests the passing-by vehicles with different social evaluations for data diffusion to 5 randomly chosen RSUs with 5-copy, 10-copy, and 15-copy disseminations. For each case, we run the simulation till the packet is successfully disseminated to 5 chosen RSUs in the area, and the average performance results over 20 runs are reported.

4.6.2 Simulation Results

Figure 4-5 shows the social evaluation of different groups within one hour, in which with the increase of probability ρ on decision D_1, the average social evaluation will increase. This result confirms that the high mobility, i.e., a vehicle often moves to new sub-areas, can receive high social evaluation. Figure 4-6 shows the average diffusion delay (ADD) of different group's data diffusion. From the figure, we can see, when a high-social vehicle disseminates the packet, i.e., a vehicle in $\mathcal{G}_5$, the ADD is obviously low, which demonstrates the effectiveness of social-aware data diffusion in VANETs. In addition, by comparing the average diffusion delay in 5-copy, 10-copy, and 15-copy disseminations, we can also conclude the multi-copy dissemination can further reduce the ADD.

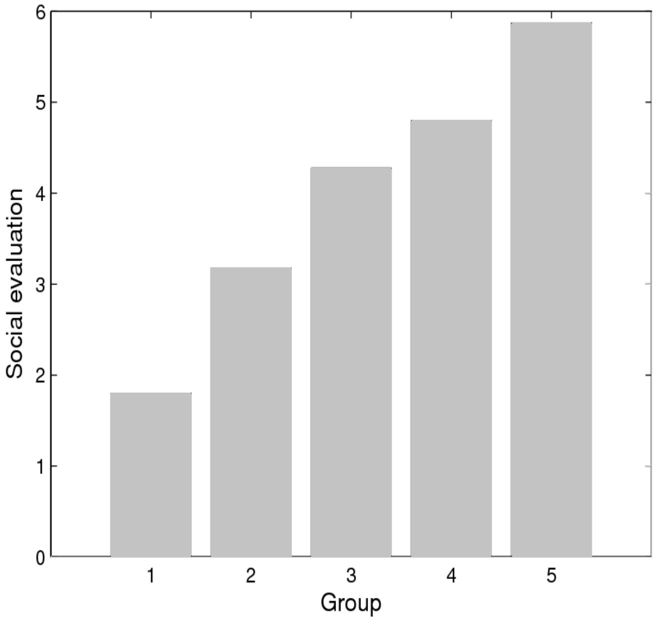


Figure 4-5. Social evaluation

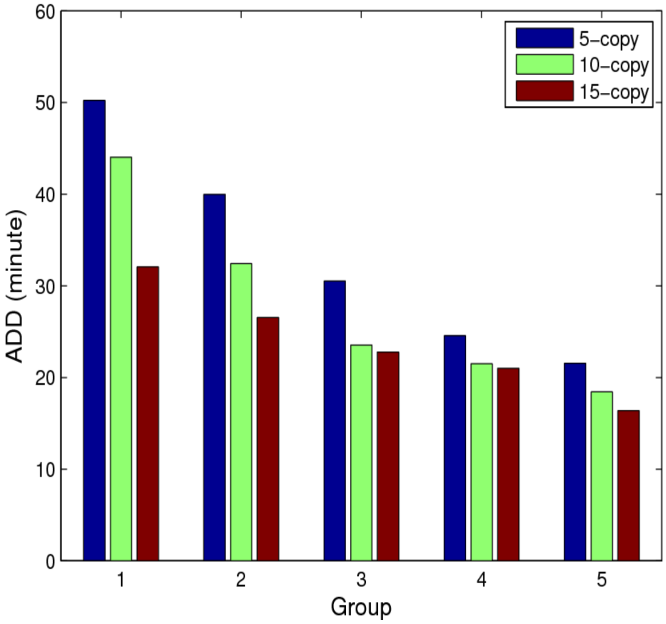


Figure 4-6. Average Diffusion Delay

Chapter 5

Conclusions and Future Work

In this chapter, we give a brief summary; followed by key contributions, and finally conclude with the future work.

5.1 Summary

This study presented a social-based trustworthy data forwarding framework in vehicular delay tolerant networks. First, we proposed a method of deploying RSUs based on social centrality measures on urban streets network. Our social centrality measures were based on human activities within a city. This novel method has improved forwarding efficiency in VANETs by increasing throughput while keeping costs of deploying RSUs under control. Second, we designed a privacy preserving message forwarding protocol which utilizes the social characteristics of RSUs to deliver messages to their destinations while preserving communicating parties' privacy. The proposed protocol takes advantage of high performance capability of RSUs to store and forward messages to their destinations, while applying cryptographic construction of mix network with re-encryption to provide adequate privacy for senders and receivers by transforming RSUs deployed at those highly social spots into a mix network. We evaluated our proposed scheme by means of simulation. We extended a framework that links microscopic road traffic simulator (SUMO) with discrete event network simulator (OMNET++) to provide realistic scenario to test our protocol in normal city environment. The simulation demonstrated that our proposed scheme can achieve good delivery ratio, while providing tolerable end-to-end delay. Finally, we have presented an efficient vehicle social evaluation (EVSE) scheme with location privacy preservation for VANET. Based on the efficient group signature technique, the proposed EVSE scheme has been identified to be not only capable of evaluating a vehicle's sociality without disclosing the vehicle's past location information, but also able to avoid the double-count in social evaluation. As a result, it can support social-aware data diffusion in privacy-preserving VANET environments. Through extensive performance evaluations, we have demonstrated that the social-aware data diffusion consolidated by the proposed EVSE scheme can achieve better efficiency in terms of average diffusion delay.

5.2 Contributions

The major contributions of this thesis can be summarized as follows:

- A novel social activities based multi-centrality assessment for deploying RSUs at high social intersections was proposed. Specifically, we described three social centrality measures: *i)* overall betweenness centrality to evaluate importance of every intersection in the graph. *ii)* Activity based betweenness to determine the importance of intersections in regards to accessing activity centers in a city. *iii)* Activity based closeness centrality which evaluates the importance of each intersection in regard to their fast reachability to activity centers around the city.
- Privacy preserving message forwarding protocol for vehicular DTN was introduced. This protocol achieved high transmission reliability by utilizing the nature

of Social RSUs, which were passed by a large number of vehicles, to temporarily store and forward messages. Meanwhile, it preserved senders and receivers privacy by building up a mix network from RSUs which also acted as re-encryption server.

- A realistic VANET simulation was performed by extending a framework that bidirectionally couples road traffic simulator with network simulator. During the simulation, vehicles were provided with GPS like functionality which allowed them to know their routes at any given time during the simulation. Also realistic vehicle traces for the map of the city of Oshawa were generated.
- An efficient vehicle social evaluation (EVSE) scheme, which enables each vehicle to show its authentic social evaluation to others while without disclosing its past location information was proposed. As a result, it met the prerequisites for the success of social-aware data diffusion in VANETs.

5.3 Future Work

. Real world vehicles traces should be collected and used to further validate scheme before real world implementation. Currently, there are many vehicle applications, and each application has its own security and privacy requirement. Another future research is to come up with mechanism that satisfies applications specific requirements.

References

[1] Z. Zhang, “Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges,” *IEEE Communications Surveys and Tutorials*, Vol.8, No.1, 2006, pp. 24–37

[2] J. Shen, S. Moh, and I. Chung, “Routing Protocols in Delay Tolerant Networks: A Comparative Survey,” In *Proc*. the 23rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008), Shimonoseki, Japan, July 2008, pp. 1577 - 1580

[3] E. P.C. Jones and P. A.S. Ward, “Routing strategies for delay-tolerant networks,” *ACM Computer Communication Review (CCR)*,2006. [Online]. Available http://www.ieice.org/explorer/ITC-CSCC2008/pdf/p1577 P2-46.pdf.

[4] M. Fiore, J. Haerri, F. Filali, and C. Bonnet,”Vehicular Mobility Simulation for VANETs,” in *Proc. 40th IEEE Annual Simulation Symposium (ANSS-40 2007),* Norfolk, Virginia, USA, Mar. 2007, pp.301-309

[5] W. Zhao, Y. Chen, M. H. Ammar, M. Corner, B. N. Levine, and E. Zegura, “Capacity Enhancement using Throwboxes in DTNs,” In *Proc. IEEE Intl Conf on Mobile Ad hoc and Sensor Systems (MASS)*, Vancouver, British Columbia, Canada, Oct. 2006, pp.31-40

[6] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," In *Proc. the First International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2008’)*, Brussels, Belgium, Mar. 2008, pp.1-10

[7] D. Krajzewicz, M. Bonert, and P. Wagner, “The open source traffic simulation package sumo,” in *RoboCup 2006 Infrastructure Simulation Competition*, Bremen, Germany, 2006, pp. 1–10

[8] V. Balakrishnan, and S. Madden, “A measurement study of vehicular internet access using in situ Wi-Fi networks,” in *Proc. ACM 12th annual international conference on Mobile computing and networking*, Sep. 2006, pp. 50–61

[9] N. Banerjee, M. D. Corner, D. Towsley, and B. N. Levine, “Relays, base stations, and meshes: enhancing mobile networks with infrastructure,” in *Proc. 12th an-*

nual international conference on Mobile computing and networking 2008, New York, USA, 2008, pp. 81–91

[10] IEEE Std. 1609.2-2006, “IEEE Trial-Use Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages,” Jul. 2006. [Online]. Available http://ieeexplore.ieee.org/servlet/opac?punumber=11000

[11] K. Plobl, T. Nowey, and C. Mletzko, “Towards a security architecture for vehicular ad hoc networks,” in *Proc.1st Int’l Conf. on Availability, Reliability and Security (ARES’06),* Vienna, Austria, Apr. 2006, pp.374–381

[12] A. Aijaz, B. Bochow, D. Florian, A. Festag, M. Gerlach, R. Kroh, and L. Tim, “Attacks on inter vehicle communication systems—An analysis,” in *Proc. the 3rd International Workshop on Intelligent Transportation (WIT 2006),* Hamburg, Germany, Mar. 2006, pp. 189–194

[13] M. Raya and J. Hubaux, “The security of vehicular ad hoc networks”, in *Proc. 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005),* Alexandria, Virginia, USA, Nov. 2005, pp. 11-21

[14] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *IEEE Journal on Selected Areas in Communications,* Vol. 25, No. 8, Oct. 2007, pp. 1569-1589

[15] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proc. the IEEE International Conference on Computer Communications (INFOCOM’08),* Phoenix, Arizona, USA, April., 2008, pp. 1229–1237

[16] J. Freudiger, M. Raya, and M. Feleghhazi, “Mix zones for location privacy in vehicular networks,” in *Proc. the First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS ’07),* Vancouver, British Columbia, Canada, Aug. 2007

[17] P. Crucitti, V. Latora, and S. Porta, “Centrality measures in spatial networks of urban streets,” Physical Rev. E (Statistical, Nonlinear, and Soft Matter Physics), Vol. 73, No. 3, Mar. 2006, pp. 36125

[18] B. Jiang and C. Claramunt, “A Structural Approach to the Model Generalization of an Urban Street Network,” GeoInformatica, Vol. 8, June 2004, pp. 157-171

[19] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. Inf. Theory, Vol. 31, No. 4, Jul. 1985, pp. 467–472

[20] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, “Universal reencryption for mixnets,” in Proc. Cryptographers’ Track at the RSA Conference (CT-RSA), San Francisco, California, USA, 2004, pp.163–178

[21] C. Sommer, Z. Yao, R. German, and F. Dressler, “Simulating the Influence of IVC on Road Traffic using Bidirectionally Coupled Simulators,” in *Proc. 27th IEEE Conference on Computer Communications (IEEE INFOCOM 2008): Mobile Networking for Vehicular Environments (IEEE MOVE 2008),* Phoenix, AZ, USA,, April. 2008, pp. 1–6

[22] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: a secure and privacy preserving protocol for vehicular communications” *IEEE Transaction on Vehicular Technology*, Vol. 56, No. 6, 2007, pp. 3442-3456

[23] R. Lu, X. Lin, and X. Shen, “Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks,” in *Proc. INFOCOM*, San Diego, California, USA, Mar. 2010, pp. 1–9

[24] Y. Zhang and J. Zhao, “Social network analysis on data diffusion in delay tolerant networks,” In *Proc. the 10th ACM international symposium on Mobile ad hoc networking and computing*, New Orleans, Louisiana, USA, 2009, pp. 345–346

[25] W. Gao, Q. Li, B. Zhao, and G. Cao, “Multicasting in delay tolerant networks: a social network perspective,” In *Proc. the 10th ACM international symposium on Mobile ad hoc networking and computing*, New Orleans, Louisiana, USA, 2009, pp. 299–308

[26] R. Lu, X. Lin, X. Liang, and X. Shen, “Sacrificing the plum tree for the peach tree: A socialspot tactic for protecting receiver-location privacy in vanet,” in *Proc. IEEE Globecom’10*, Miami, Florida, USA, December. 2010, pp.1-5

[27] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *Proc.* The *11th ACM conference on Computer and communications security Security* Washington DC, USA,, Oct. 2004, pp. 166–177

[28] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM 2008*, Phoenix, Arizona, USA, April 2008

[29] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Crypto*, LNCS, Vol. 2139, 2001, pp. 213-229

[30] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. Adv. Cryptology—Asiacrypt, ser*. LNCS, Vol, 3788, 2005, pp. 515-532