

**SECURE CONDITIONAL PRIVACY SCHEME  
FOR POSITION BASED ROUTING IN  
VEHICULAR AD HOC NETWORKS**

**A DISSERTATION**

*Submitted in partial fulfillment of the  
requirements for the award of the degree  
of*

**INTEGRATED DUAL DEGREE**

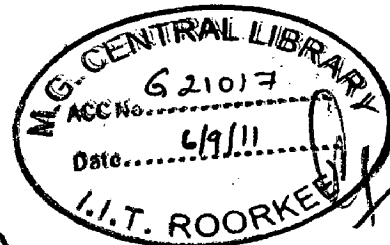
**in**

**COMPUTER SCIENCE AND ENGINEERING**

**(With Specialization in Information Technology)**

**By**

**AKSHAT KUMAR**



**DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE  
ROORKEE -247 667 (INDIA)  
JUNE, 2011**

## CANDIDATE'S DECLARATION

---

I hereby declare that the work being presented in the dissertation work entitled "Secure Conditional Privacy Scheme for Position Based Routing in Vehicular ad hoc Networks" towards the partial fulfillment of the requirement for the award of the degree of **Integrated Dual Degree in Computer Science and Engineering (with specialization in Information Technology)** and submitted to the **Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, India** is an authentic record of my own work carried out during the period from May, 2010 to May, 2011 under the guidance and provision of **Dr. Manoj Misra, Professor, Department of Electronics and Computer Engineering, IIT Roorkee.**

I have not submitted the matter embodied in this dissertation work for the award of any other degree and diploma.

Date: June, 2011

Place: Roorkee

  
(AKSHAT KUMAR)

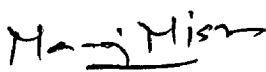
## CERTIFICATE

---

This to certify that the declaration made by the candidate above is correct to the best of my knowledge and belief.

Date: June, 2011

Place: Roorkee

  
**Dr. Manoj Misra**  
**Professor,**  
**E&CE Department**  
**IIT Roorkee, India**

## ACKNOWLEDGEMENTS

---

I would like to take this opportunity to extend my heartfelt gratitude to my guide and mentor **Dr. Manoj Misra**, Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, for his trust in my work, his able guidance, regular source of encouragement and assistance throughout this dissertation work. I would state that the dissertation work would not have been in the present shape without his inspirational support and I consider myself fortunate to have done my dissertation under him.

I also extend my sincere thanks to **Dr. S.N. Sinha**, Professor and Head of the Department of Electronics and Computer Engineering for providing facilities for the work.

I would like to thank all my friends who supported and encouraged me to finish this work.

Finally, I would like to say that I am indebted to my parents for everything that they have given to me. I thank them for sacrifices they made so that I could grow up in a learning environment. They have always stood by me in everything I have done, providing constant support, encouragement, and love.

**AKSHAT KUMAR**

## LIST OF FIGURES AND TABLES

---

Figure 1.1	Vehicular ad hoc network .....	1
Figure 3.1	System Design .....	16
Figure 4.1	Car Agent Implementation.....	27
Figure 5.1	Average Message Loss Ratio in city scenario .....	34
Figure 5.2	Average Message Loss Ratio in Highway Scenario .....	34
Figure 5.3	Average Message Delay in City Scenario .....	35
Figure 5.4	Average Message Delay in Highway Scenario.....	36
Figure 5.5	Impact of Traffic Load on Signature Verification Delay.....	37
Table 3.1	Message Format for OBU .....	18
Table 3.2	Message Format for RSU.....	21
Table 5.1	Simulation Configuration.....	31
Table 5.2	Vehicle Profiles.....	32
Table 5.3	Byte Overhead Comparison between GSIS and the proposed scheme.....	33

## ABSTRACT

---

A Vehicular ad hoc network (VANET) is a decentralized ad-hoc network, formed of vehicles acting as highly mobile nodes. Due to its applicability in traffic safety applications, it has caught the attention of researchers. VANETs are expected to support not only safety applications but diverse infrastructure-based commercial services as well. The requirement of a communication system that ensures vehicle to vehicle communication, efficient transmission of vehicle generated announcements and proper routing in a highly dynamic environment must be satisfied before service oriented VANETs can be successfully deployed. This poses many new research challenges, especially on the aspects of security and user's privacy.

In this dissertation, the design requirements in the aspects of security and privacy preservation between communicating devices in VANETs are identified. A secure and privacy preserving scheme based on digital signature techniques is then proposed which not only guarantees the requirement of security and privacy but can also provide desired traceability of each vehicle in the case where the identity of the message sender has to be revealed by the authority. Extensive simulation is conducted to verify efficiency and effectiveness of the proposed scheme in various scenarios under different road systems. Finally the thesis is concluded by pointing out some open issues and possible direction of future research relating to privacy and security in VANETs.

---

# CONTENTS

---

<b>CANDIDATE’S DECLARATION</b> .....	<b>i</b>
<b>ACKNOWLEDGEMENTS</b> .....	<b>ii</b>
<b>LIST OF FIGURES AND TABLES</b> .....	<b>iii</b>
<b>ABSTRACT</b> .....	<b>iv</b>
<b>TABLE OF CONTENTS</b> .....	<b>v</b>
<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1 Vehicular ad hoc networks.....	1
1.2 Motivation.....	2
1.3 Problem Statement.....	3
1.3.1 Problem Description .....	3
1.4 Organization of Dissertation.....	3
<b>CHAPTER 2: LITERATURE REVIEW</b> .....	<b>5</b>
2.1 Network Architecture.....	5
2.2 VANET Characteristics .....	5
2.3 VANET Applications.....	7
2.3.1 Public Safety Applications.....	7
2.3.2 Comfort Applications.....	7
2.3.3 Traffic Management Applications .....	8
2.3.4 Traveler Information Support Applications.....	8

2.4	Routing in VANETs .....	9
2.3.1	Topology-based Routing Protocols.....	9
2.3.2	Position-based Routing Protocols .....	10
2.5	Security in VANETs .....	11
2.5.1	Security Attacks in VANETs.....	12
2.6	Privacy Preserving Schemes in VANETs.....	13
2.7	Research Gaps.....	14

**CHAPTER 3: PROPOSED SCHEME FOR PRIVACY PRESERVATION IN VANETS ..15**

3.1	System Architecture .....	15
3.2	Problem Formulation .....	16
3.2.1	Communication between OBUs .....	16
3.2.2	Communication between RSUs and OBUs .....	17
3.3	Security Protocol between OBUs .....	17
3.4	Security Protocol between OBU and RSU .....	21

**CHAPTER 4: IMPLEMENTATION DETAILS.....24**

4.1	Design and Development of Basic Simulation System .....	24
4.1.1	Vehicle Registration Module .....	24
4.1.2	Vehicle Database .....	25
4.1.3	Vehicles (or OBUs).....	25
4.1.4	Tracking Manager .....	28
4.2	Libraries and APIs used .....	29
4.2.1	Encryption and Digital Signature Libraries .....	29
4.2.2	NCTUns Packet APIs .....	29

<b>CHAPTER 5: RESULTS AND DISCUSSION .....</b>	<b>31</b>
5.1 Simulation Setup.....	31
5.1.1 Mobility Model .....	31
5.1.2 Vehicle Profiles.....	32
5.1.3 Metrics Used .....	32
5.2 Performance Evaluation.....	33
5.2.1 Byte Overhead and Average Signature Verification Delay .....	33
5.2.2 Impact of Traffic Load.....	34
5.2.2.1 Impact of Traffic Load on Average Message Loss Ratio .....	34
5.2.2.2 Impact of Traffic Load on Average Message Delay.....	35
5.2.2.3 Impact of Traffic Load on Signature Verification Delay.....	37
 <b>CHAPTER 6: CONCLUSION AND FUTURE WORK .....</b>	 <b>38</b>
6.1 Suggestions for future work.....	39
 <b>REFERENCES.....</b>	 <b>40</b>



# CHAPTER 1

## INTRODUCTION

---

### 1.1 Vehicular ad hoc Networks

With the sharp increase of vehicles on roads in the recent years, driving has not stopped from being more challenging and dangerous. The roads are saturated with vehicles, proper driving guidelines are hardly respected, and drivers often lack enough attention causing more and more traffic related problems every day. The advances in wireless technologies provide opportunities to utilize these technologies in support of advanced vehicle safety applications. While the major objective has clearly been to improve the overall safety of vehicular traffic, promising traffic management solutions and on-board entertainment applications are also expected to be provided [14].

The advanced and wide deployment of wireless communication technologies along with the increase in the number of vehicles equipped with wireless transceivers to communicate with other vehicles have resulted in growth of a special class of wireless networks, known as vehicular ad hoc networks or VANETs [14]. Vehicular Ad hoc Network (VANET), a subclass of mobile ad hoc networks (MANETs), is a promising approach for the intelligent transportation system (ITS) and is expected to improve traffic quality and provide a more convenient driving environment for the general populace.

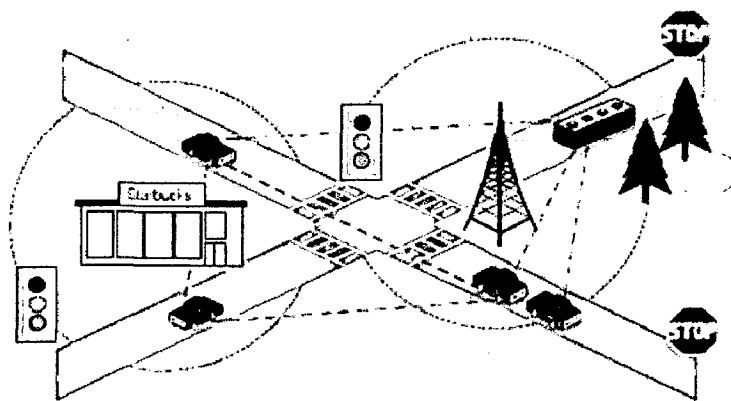


Figure 1.1: Vehicular ad hoc network <sup>[14]</sup>

Even though VANETs is a subclass of MANETs, still most of the existing routing protocols for MANETs do not apply well to VANETs because VANETs represent a particularly challenging class of MANETs. They are distributed, self-organizing communication networks formed by moving vehicles, and are thus characterized by very high node mobility and limited degrees of freedom in mobility patterns.

## **1.2 Motivation**

The creation of a VANET is significant to traffic management and roadside safety. Unfortunately, deployment of a service oriented VANET has its own set of challenges, the most significant of which are security and location privacy. As a special implementation of mobile ad hoc networks, a VANET could be subjected to many security threats, which will lead to increasing malicious attacks and service abuses. It is obvious that any malicious behavior of users, such as a modification and replay attack on the disseminated messages, could be fatal to other users. Hence, conditional privacy preservation must be achieved in the sense that user-related private information, including the driver's name, license plate, speed, position and traveling routes, as well as their relationships (and other information which is transmitted in periodic beacon messages), has to be protected, while the authorities should be able to reveal the identities of message senders in case of a traffic event dispute, such as a crime/car accident scene investigation, which can be used to look for witnesses. Therefore, it is critical to develop a suite of elaborate and carefully designed security mechanisms to achieve security and conditional privacy preservation in VANETs before they can practically be launched.

However, only a very limited number of previously reported studies have tackled the security and privacy issues of VANETs, in spite of its ultimate importance. In this dissertation, the problem of security assurance and conditional privacy preservation in vehicular communication applications is addressed. The proposed scheme deals with the issues of both security and conditional privacy in VANETs through a cryptographic approach. We introduce a secure and privacy preserving protocol for VANETs through use of digital signature based techniques.

## **1.3 Problem Statement**

The aim is to develop and implement a secure conditional privacy scheme (with vehicle position tracking possible only by authorized entities) for position based routing protocols in vehicular ad hoc networks (VANETs).

### **1.3.1 Problem Description**

Location based routing protocols for vehicular ad hoc networks (VANETs) require transmission of beacon packets by vehicles at periodic intervals. These beacon packets contain information about vehicle position and possibly the path which the vehicle will follow (like in Geographical Opportunistic Routing [1]). Hence by capturing these beacon packets, the position of a vehicle at different instances of time can be determined which poses a serious threat to user's privacy. But some scenarios (like police department needing to know position of a suspect vehicle) demand position tracking to be made possible.

Also, the integrity and authenticity of control information is needed to ensure proper routing.

Hence the goal stated in the problem statement can be divided into three sub-problems:

- To maintain user privacy (in terms of location) from other users in the network.
- The ability to track a vehicle (in exceptional cases by proper authorities)
- To enhance security (in terms of message integrity and authenticity) of control messages for routing.

## **1.4 Organization of Dissertation**

This report comprises of six chapters including this chapter that introduces the topic and states the problem. The rest of the dissertation report is organized as follows.

Chapter 2 provides a brief description of literature review on conditional privacy preservation in VANETs. The other topics include routing protocols for VANETs, security issues in routing in VANETs, existing privacy preserving schemes and research gaps.

Chapter 3 provides a detailed description of the proposed scheme for preserving location privacy of user while maintaining vehicle traceability by proper authorities.

Chapter 4 gives the brief description of the implementation of the proposed scheme.

Chapter 5 discusses the results and including discussion on them. It also provides as analysis on important performance parameters.

Chapter 6 concludes the work and gives the directions for future work.

# CHAPTER 2

## LITERATURE REVIEW

---

A vehicular ad hoc network (VANET) organizes and connects vehicles with one another, and sometimes with mobile and fixed location resources.

### 2.1 Network Architecture

The architecture of VANETs falls within following three categories [14]:

1. **WLAN architecture:** The network uses WLAN access points to connect to the Internet and facilitate vehicular applications. Vehicles communicate with Internet by driving by a wireless access point
2. **Pure ad hoc architecture:** This is the infrastructure-less network where nodes perform vehicle-to-vehicle communication with each other.
3. **Hybrid:** This architecture include presence of roadside communication units such as an access points and vehicles equipped with wireless networking devices, so that vehicles can take advantage of infrastructure in communicating with each other.

### 2.2 VANET Characteristics

Similar to mobile ad hoc networks (MANETs), nodes in VANETs self-organize and self-manage information in a distributed fashion without a centralized authority or a server dictating the communication. Since nodes are mobile, thus data transmission is less reliable and sub-optimal. Apart from these characteristics, VANETS possess a few distinguishing characteristics mentioned below [14], thus presenting itself as a particular challenging class of MANETs.

1. **Highly dynamic topology:** Since vehicles are moving at high speed, the topology formed by VANETs is always changing. On highways, vehicles are moving at the speed of 60 mph (25 m/sec). Suppose the radio range between two vehicles is 250 m, then the link between the two vehicles lasts at most 10 sec.

2. **Frequently disconnected network (Intermittent connectivity):** The highly dynamic topology results in frequently disconnected network since the link between two vehicles can quickly disappear while the two nodes are transmitting information. The problem is further exacerbated by heterogeneous node density where frequently traveled roads have more cars than non-frequently traveled roads. Moreover, non-rush hours only result in disparate node density, thus disconnectivity. A robust routing protocol is needed for VANETs which recognizes the frequent disconnectivity and provides an alternative link quickly to ensure uninterrupted communication.
3. **Patterned Mobility:** Vehicles follow a certain mobility pattern that is a function of the underlying roads, the traffic lights, the speed limit, traffic condition, and drivers' driving behaviors. Because of the particular mobility pattern, evaluation of VANET routing protocols only makes sense from traces obtained from the pattern. There are various VANET mobility trace generators developed for the very purpose of testing VANET routing protocols in simulation. Realistic mobility traces have been gathered from vehicles for the same purpose.
4. **Propagation Model:** In VANETs, the propagation model is usually not assumed to be free space because of the presence of buildings, trees, and other vehicles. A VANET propagation model should consider the effects of free standing objects as well as potential interference of wireless communication from other vehicles or widely deployed personal access points.
5. **Unlimited Battery Power and Storage:** Nodes in VANETs are not subject to power and storage limitation as in sensor networks, another class of ad hoc networks where nodes are mostly static. Nodes are assumed to have ample energy and computing power. Therefore, optimizing power utilization is not as relevant as it is in sensor networks.
6. **On-board Sensors:** Nodes are assumed to be equipped with sensors to provide information useful for routing purposes. Many VANET routing protocols have assumed the availability of GPS unit from on-board Navigation system. Location information from GPS unit and speed from speedometer provides good examples for sources of information that can possibly be obtained by sensors to be utilized to enhance routing decisions.

## 2.3 VANET Applications

A number of unique applications are being standardized for VANETs. VANET applications can be divided into following three categories [19]:

1. Public safety applications
2. Comfort applications
3. Traffic management applications
4. Traveler information support applications

### 2.3.1 Public Safety Applications

The objective of these applications is to improve the overall safety of the transportation infrastructure. Some examples of these applications are mentioned below:

1. **Traffic Signal Violation Warning:** The goal of this application is to reduce collisions at intersections. In this scenario, a RSU is placed near an intersection that has a traffic light. Infrastructure-to-vehicle communication is used to warn approaching vehicles of the status of the traffic light and to alert drivers of a potential light violation. When a vehicle receives a traffic signal violation warning message, computation is performed on the received data to determine if the driver is at risk of inappropriately entering the intersection and if so a warning is issued to the driver.
2. **Emergency Electronic Brake Lights:** This application provides a warning to a trailing vehicle when a vehicle in front of it applies its brakes. The emergency electronic brake light application is beneficial in situations where visibility is limited, such as poor weather conditions. The data contained in braking vehicle's broadcast message is the deceleration rate and braking vehicle's location. When trailing vehicle receives the warning, an algorithm is invoked to determine the relevance of the message and whether or not the vehicle is endangered. If so, a warning is sent to the driver. The emergency electronic brake light application significantly reduces accidents by giving the driver a warning before they are able to visually sense the danger.

### 2.3.2 Comfort Applications

These applications increase the comfort of use by adding value-added services. But these applications have a low priority than public safety applications. This category includes the following applications:

1. **Electronic Toll Collection:** This application works by enabling driver to drive through a toll booth instead of stopping by making payment through the network.
2. **Media Applications:** These include a number of entertainment features, such as transfer of music and video files for in-car entertainment.

### 2.3.3 Traffic Management Applications

These applications are focused on moving traffic flow, thus reducing congestion as well as accidents resulting from congestion, and reducing travel time. Some applications that belong to this category of VANET applications are mentioned below:

1. **Traffic monitoring:** This application can provide localized timely information regarding the traffic for several vehicles around the vehicle. This application requires each vehicle to act as a sensor (determining its current speed), as a relay (if the information is to travel for more than the direct transmission range) as well as a destination (using information from the other vehicles in the system). The information can be used to simply inform the driver or, in more complex systems to suggest alternate route
2. **Traffic light scheduling:** This application aims to reduce waiting time at a traffic light intersection by dynamic scheduling of traffic lights. This system utilizes additional information (obtained using vehicle to RSU communication), such as the length of the queues at the traffic light as well as the number of vehicles expected to arrive in the near future to the efficiency of schedules.

### 2.3.4 Traveler Information Support Applications

These applications provide updated local information, maps, and in general messages of relevance limited in space and/or time. Some applications that belong to this category of VANET applications are mentioned below:

1. **Local information:** Information such as local updated maps, the location of gas stations, parking areas, and schedules of local museums can be downloaded from selected infrastructure places or from other “local” vehicles. Advertisements, for example, gas or hamburger prices may be sent to approaching vehicles.
2. **Road warnings:** Warnings of many types (e.g., ice, oil, or water on the road, low bridges, or bumps) may easily be deployed by authorities simply by dropping a beacon in the relevant area.



## 2.4 Routing in VANETs

A routing protocol governs the way that two communication entities exchange information; it includes the procedure in establishing a route, decision in forwarding, and action in maintaining the route or recovering from routing failure.

The routing protocols for VANETs [14][15][16] can be broadly classified into three categories:

1. **Unicast Routing protocols:** These protocols are used when message is to be sent to a static destination or a single mobile vehicle. They can be classified as:
  - topology-based
  - geographic (position-based).

Complications arise when the destination is a mobile vehicle because it is more difficult to trace the location of the vehicle if it is moving.

2. **Multicast and Geocast Routing protocol:** These protocols are used when information is to be delivered to more than one location. Multicast in a VANET is defined by delivering multicast packets from a single source to all members of a multicast in a multi-hop communications. For the geocast routing, if a vehicle receives a geocast packet from neighbors, the packet should be forwarded or dropped depending on current location of vehicle. If this vehicle is located in the specific geographic region, then the geocast packet is forwarded, otherwise, the packet is dropped.
3. **Broadcast Routing protocols:** These protocols are utilized when information is to be sent to all vehicles in the network. A source vehicle sends broadcast message to all other vehicles in the network. Broadcast is important in many applications of VANET such as advertisement publicity, group discussions and route discovery. The design issue of broadcasting is how to effectively prevent packet collision (broadcast storm problem) during the broadcasting.

### 2.4.1 Topology-based Routing Protocols

These routing protocols use links' information that exists in the network to perform packet forwarding. They can further be divided into proactive (table-driven) and reactive (on-demand) routing.

1. **Proactive (table-driven):** Proactive routing carries the distinct feature that the routing information is maintained in the background regardless of communication requests. Control packets are constantly broadcasted and flooded among nodes to maintain the paths or the link states between any pair of nodes even though some of paths are never used. A table is then constructed within a node such that each entry in the table indicates the next hop node toward a certain destination.
2. **Reactive (On demand):** Reactive routing opens a route only when it is necessary for a node to communicate with another node. It maintains only the routes that are currently in use, thereby reducing the burden on the network. Reactive routings typically have a route discovery phase where query packets are flooded into the network in search of a path. Example Protocols include AODV [2].

#### 2.4.2 Position-based Routing Protocols

In geographic (position-based) routing, the forwarding decision by a node is primarily made based on the position of a packet's destination and the position of the node's one-hop neighbors (nodes that are within radio range). The position of the destination is stored in the header of the packet by the source. The position of the node's one-hop neighbors is obtained by the beacons sent periodically with random jitter to prevent collision. Geographic routing assumes each node knows its location, and the sending node knows the receiving node's location by use of GPS unit from an onboard Navigation System. Since these protocols do not exchange link state information and do not maintain established routes like topology-based routings do, they are more robust and promising in the highly dynamic environments like VANETs.

Geographic routing can be classified into two categories:

1. **Non-Delay Tolerant Network (non-DTN) Protocols:** These protocols do not consider intermittent connectivity and are only practical in densely populated VANETs. This group of protocols includes Greedy Perimeter Stateless Routing (GPSR) [3], Connectivity Aware Routing (CAR) [4] etc.
2. **Delay Tolerant Network (DTN) Protocols:** These protocols consider disconnectivity and are designed from the perspective that networks are disconnected by default. This group of protocols includes Vehicle Assisted Data Delivery (VADD) [5], Geographical Opportunistic Routing (GeOpps) [1] etc.

## 2.5 Security in VANETs

The issue of security in VANETs is particularly challenging due to the unique features of the network, such as high-speed mobility of network nodes or vehicles and the sheer size of the network. Specifically, it is essential to make sure that “life-critical safety” information cannot be inserted or modified by an attacker. While the system has to be capable of establishing the liability of drivers, it should protect their privacy as much as possible. It is obvious that any malicious user behavior, such as a modification and replay attack of the disseminated messages, could be fatal to other users.

A security system for safety message transmission in a VANET should satisfy the following requirements [7]:

1. **Authentication:** Vehicle reactions to events should be based on legitimate messages (i.e., generated by legitimate senders). Therefore we need to authenticate the senders of these messages.
2. **Verification of data consistency:** The legitimacy of messages should also be verified, because the sender can be legitimate while the message contains false data.
3. **Non-repudiation:** Drivers causing accidents should be reliably identified; a sender should not be able to deny the transmission of a message (it may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident).
4. **Privacy:** People are increasingly wary of privacy violating technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed.

Most security schemes in VANETs [7][10] employ digital signatures with encryption to satisfy the requirements of message integrity and non-repudiation. Each vehicle can have its public and private key build inside its TPD (Tamper-Proof Device) and access to these TPDs should be restricted to authorized personnel only.

Authentication is usually achieved by employing group signature techniques or by using digital certificates obtained from CAs. In the context of vehicular networks, as the trust level is equal for all legitimate certificate-holding vehicles (because the certificate verifier actually trusts the CA that issued this certificate), the creation of secure groups (with a secret group key) in the network is not justified. In addition, these groups would lose the non-repudiation property if additional measures are not taken.

### 2.5.1 Security Attacks in VANETs

The following security attacks have been recognized in VANETs [7].

1. **Bogus information:** Attackers diffuse wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves).
2. **Cheating with positioning information:** Attackers in this case use this attack to alter their perceived position, speed, direction, etc. in order to escape liability, notably in the case of an accident.
3. **ID disclosure of other vehicles in order to track their location:** This is the Big Brother scenario, where a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own cars). To monitor, the global observer can utilize the roadside infrastructure or the vehicles around its target (e.g., by using a virus that infects neighbors of the target and collects the required data). The attacker is passive. We assume that the attacker does not make use of cameras, physical pursuit, or onboard tracking devices to uncover the identity of his target; otherwise, the tracking problem becomes simpler but also more expensive and tied to few specific targets, and it can be done anyhow based on existing license plates. In fact, we assume that the attacker may use techniques like packet-sniffing to gather sufficient packets to track their victim.
4. **Denial of Service:** The attacker may want to bring down the VANET or even cause an accident. Example attacks include channel jamming by aggressive injection of dummy messages.
5. **Masquerade:** The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives.
6. **Hidden Vehicle:** In many safety messaging protocols, a vehicle broadcasting warnings will listen for feedback from its neighbors and stop its broadcasts if it realizes that at least one of these neighbors is better positioned for warning other vehicles. This reduces congestion on the wireless channel. The hidden vehicle attack consists in deceiving vehicle sending safety messages into believing that the attacker is better placed for forwarding the warning message, thus leading to silencing that vehicle and stopping the propagation of safety message.

## 2.6 Privacy Preserving Schemes in VANETs

Extensive studies have been reported on the IVC (Inter Vehicular Communication), however, most of them have focused on either the feasibility of a specific application scenario or the medium access control (MAC) layer performance analysis or various routing solutions. Very limited efforts have been made on the issues of security and privacy preservation [6][7][10].

Some of the schemes proposed for maintaining user privacy are summarized below.

Raya et al, (2005) [7] proposed a scheme in which user privacy was maintained by creating a large number of anonymous certificates in vehicles. With a pool of around 43,800 certificates, each vehicle randomly chooses one of the available certificates for signing the message at one time in order to meet the driver's privacy requirement.

Shulman et al, (2006) [8] proposed a solution in which anonymous certificates were utilized. In this scheme, the RSUs (Road Side Units) act as Certification Authorities (CA) and vehicles will frequently communicate with RSUs to get anonymous certificates. By taking advantage of a list of short-lived anonymous certificates, the privacy of the drivers was ensured and the short-lived certificates were discarded right after being used.

Lin et al, (2007) [9] proposed a group signature scheme. Digital Signatures are used to sign every message sent into the network by OBU (On-Board Unit) and RSU (Road Side Unit). So any receiver can verify the integrity and authenticity of the message. A verifier can judge whether the signer belongs to a group (to check authenticity) without knowing who the signer is in the group. The core feature of this scheme is that it provides anonymity to the signers. However, for exceptional cases, the CA can reveal the unique ID of signature's originator. So this scheme can provide position tracking, if needed by authorities.

Daza et al, (2009) [11] proposed a threshold signature scheme in which each vehicle will only calculate a part of digital signature. The rest of the signature is calculated by its one-hop neighbors and then transmitted back to sender where it assimilates the signatures and sends out the message. The main drawback of this scheme was is that it has a tradeoff between availability and unlinkability. In sparse VANETs, in order to send a message, sometimes the unlinkability requirement may be compromised.

## 2.7 Research Gaps

The following research gaps were identified after critical literature review.

1. Lack of vehicles tracking feature (in exceptional cases like an accident) in most schemes that maintain user privacy.
2. The schemes that maintain user privacy along with the feature of authorized vehicle tracking depend on some condition to be met (presence of sufficient one-hop neighbors or presence of RSUs). These conditions may not be met at all times (in sparse VANETs, there may not be sufficient one-hop nodes and it is impractical to install RSUs at every intersection in the near future).
3. Integration of user privacy and security mechanisms into routing protocols. The current security schemes focus on privacy and security of safety messages.
4. Development of a hybrid routing protocol that combines the features of delay tolerant as well as non-delay tolerant routing protocols.
5. Establishment of priority routes for safety and control messages.

# CHAPTER 3

## PROPOSED SCHEME FOR PRIVACY PRESERVATION IN VANETS

---

This chapter gives the complete architecture, design and working of the conditional privacy scheme for position-based routing protocols in VANETS which helps in maintaining user privacy while providing the facility of vehicle traceability by authorities.

### 3.1 System Architecture

The overall architecture of VANETS system considered in our dissertation includes a Certificate Management Authority (CMA), Certificate Database, vehicles equipped with OBUs (on-Board Units) running on road. The presence of RSUs (Road Side Units) is optional and not necessary for the working of the proposed scheme.

**CMA:** It is an organization responsible for certificate registration and management. In the beginning of system initialization, each vehicle and RSU (if present) has to register itself with CMA to get a set of certificates assigned to it. This entity can be divided into two sub-entities which are mentioned below.

- **Membership Manager (MM):** This entity performs the role of assigning anonymous certificates to vehicles and storing the same in the certificate database. The certificates assigned are unique to that entity only and MM ensures that no two entities share the same certificate
- **Tracking Manager (TM):** The law authorities can serve as TM for revealing the real IDs of message senders, if required, by accessing the certificate database.

**Certificate Database:** This database stores vehicle-specific information like License Plate Number, Owner's ID, Owner's Address, Date of Purchase, VIN (Vehicle Identification Number) etc. along with the corresponding certificate set that is assigned to that vehicle. The access to this database is restricted to authorities only. Access to Certificate Database is required in dispute events (such as accidents) to reveal the true identity of the signer of the message.

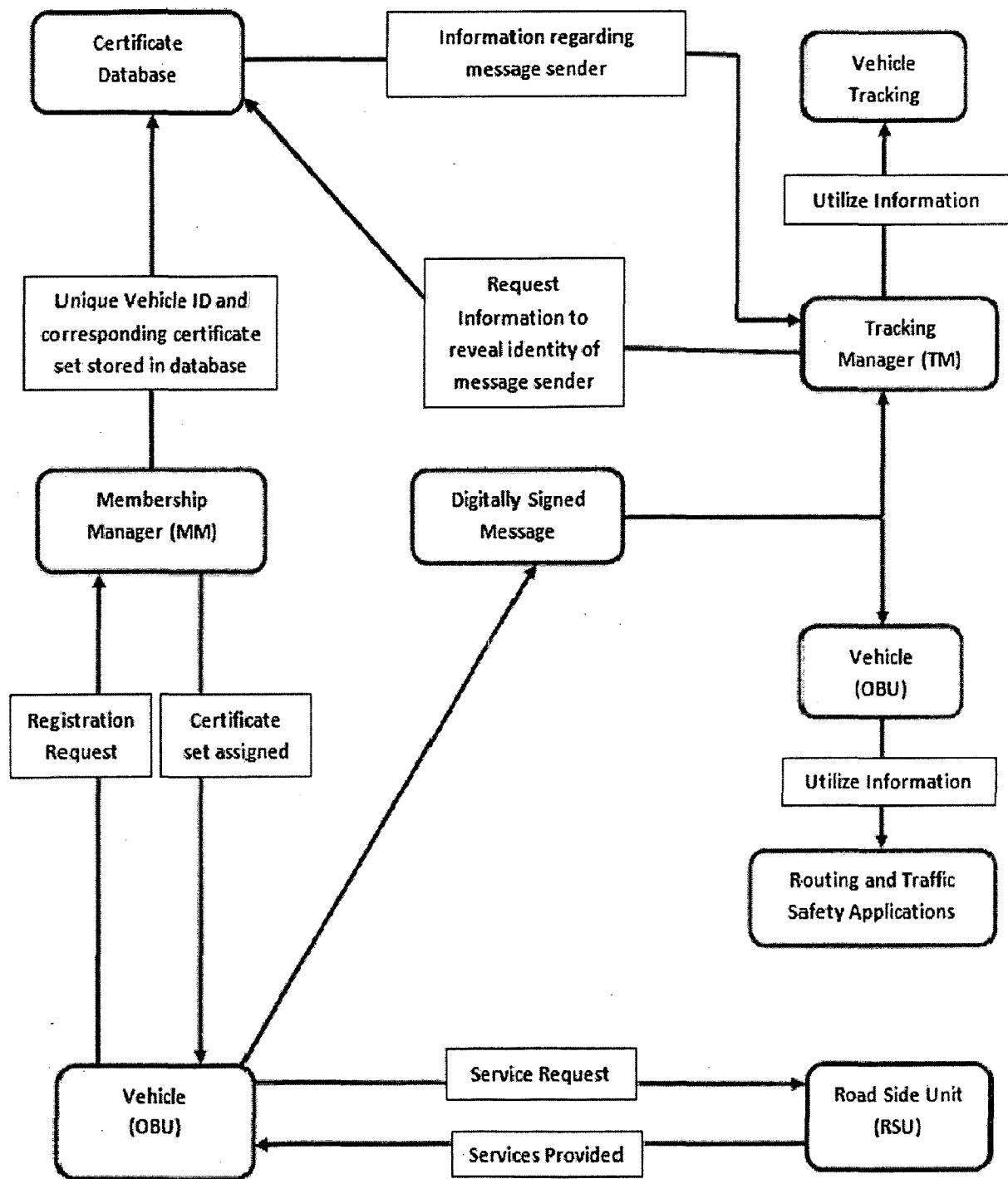


Figure 3.1: System Design



**OBU:** In our scheme, vehicles are equipped with OBUs to communicate with each other. When vehicles are on road, they regularly broadcast routine traffic-related messages, such as position, current time, direction, speed, brake status, steering angle, acceleration/deceleration, traffic conditions, traffic events, etc., to aid in routing and help drivers get a better awareness of what is going on in their driving environment and take early actions to respond to an abnormal situation. They also communicate with RSUs to request services.

**RSU:** The RSUs are installed at intersections and curves and act as a gateway to connect service provider servers and the OBUs.

The relationship between these entities is shown in the following Figure 3.1.

## **3.2 Problem Formulation**

It is assumed that each vehicle is equipped with a reliable positioning device (e.g., a GPS) and can get accurate time information. To explore the highest security level, a very critical scenario is assumed where the adversaries can intercept any message that they desire in the VANET. Furthermore, based on the fact that keeping the confidentiality of each message in IVC applications is not necessary (since everybody has the right to know the content of the message), digital signature technique is chosen to sign every message sent by the OBUs and the RSUs. Therefore, any receiver can verify the received messages and make sure of the integrity and authenticity of the messages with the nonrepudiation property. The security design is divided into the following two categories:

- 1) Security mechanisms between two OBUs, and
- 2) Security mechanisms between an RSU and an OBU.

With this, the security solutions are considered separately in these two categories due to the different design requirements, which are discussed as follows.

### **3.2.1 Communication between OBUs**

The main challenge of the communications between OBUs lies in the contradiction between the design requirements for vehicle anonymity from regular users and for traceability by the authorities. Because of this, the traditional public key encryption scheme is not suitable in signing the safety messages, because the ID information is included in the public key certificates.

Hence to counter this problem, a list of anonymous certificates is used to sign safety messages and the relationship of these certificates with their owners is kept in Certificate Database. Hence at the added cost of maintaining a certificate list, we can achieve conditional privacy in VANETs. This scheme can satisfy all other basic requirements of security in VANETs, such as message integrity and data origin authentication.

In addition to the aforementioned properties, high efficiency is desirable in IVC applications. The computational cost should be small to meet stringent communication requirement in IVC system.

### 3.2.2 Communication between RSUs and OBUs

The distinguishing feature in communication between RSUs and OBUs is that messages signed by RSUs are not subject to privacy requirement. Hence, instead of having a list of anonymous certificates, an RSU has a public key certificate installed in it which contains its unique ID and other information like RSU location, its make etc.

## 3.3 Security Protocol between OBUs

1) **Message Format:** The format of messages sent by OBU is defined in Table 3.1.

**Table 3.1**  
**Message Format for OBU**

<b>Certificate</b>	<b>Message Length</b>	<b>Payload</b>	<b>Timestamp</b>	<b>Signature</b>	<b>TTL</b>
32 bytes	4 bytes	200-300 bytes	8 bytes	160 bytes	2 bytes

The certificate field includes the randomly chosen anonymous certificate from the list of certificates assigned to that OBU.

The message payload may include the information on the vehicle's position, direction, speed, acceleration/deceleration, traffic events, etc.

The timestamp and TTL (time to live) fields are used to determine the window during which message is valid.

The signature field contains the digital signature of the first four parts of the message.

## 2) Secure OBU to OBU communication

The proposed protocol contains four phases, which are described as follows.

**Membership Registration:** During the vehicle's registration process, the MM generates a tuple  $(V_i, CS_i)$  for each vehicle  $i$ , where

$V_i$  is the tuple containing information related to vehicle  $i$ , such as License Plate Number, Owner's name, Owner's address, VIN number, date of manufacture etc.

$CS_i$  is the set of anonymous certificates assigned to  $i$

Finally, MM stores tuple  $(V_i, CS_i)$  in the certificate database.

**Signing:** Given Message  $M$ , the vehicle  $i$  signs message  $M$  before sending it out. By selecting a certificate randomly from the set of anonymous certificates, message is digitally signed by following steps.

- Insert the certificate (containing public key and identity of CA) in the first part of message.
- Store the payload (vehicle location, speed etc.) in the payload field.
- Set the timestamp value using current time and set TTL field accordingly.
- Compute the hash value of first four parts and encrypt it using private key of certificate chosen for signing the message.
- Store the digital signature in signature part of message.

**Verification:** Once the message is received, the receiver first checks if the time information in the message payload is in the allowable time window. If so, the receiving vehicle will perform signature verification by first re-computing the message hash value ( $H_{calculated}$ ) and then decrypting the included hash ( $H_{included}$ ) by using the public key included in the certificate.

If both values are equal, the receiver believes the message to be valid and from an trusted member of VANET. If not, the receiver neglects the message.

**Membership Traceability:** During dispute, a membership tracing operation is performed, where the real ID of message sender is desired. The TM accesses the database and searches for tuple  $(V_i, CS_i)$  where  $PK_M \in CS_i$ . Here  $PK_M$  is the public key included in the message  $M$ . Once the TM gets the tuple, it can provide the details about vehicle  $i$  (message sender).

### 3) Security Analysis

The use of anonymous certificates allows each vehicle to sign outgoing messages without compromising its location privacy. The security requirements of a secure conditional privacy scheme are unforgeability, anonymity, unlinkability and traceability, which will be discussed as follows.

**Unforgeability:** The property refers to the condition that only a valid member of VANET can sign the message and a valid signature cannot be forged. This is achieved by including the information about the CA (Certification Authority) encrypted by CA's private key in the certificate part of outgoing message. Since CA's public key is known to everyone, the certificate is decrypted to ensure the validity of the certificate.

**Anonymity:** Given a valid signature, it is computationally difficult for everyone except TM to identify the actual signer of the message. Assuming the use of a robust message digest algorithm, this requirement can be satisfied. Hence, the signature provides zero-knowledge about message sender, or in other words, no information is revealed by signature.

**Unlinkability:** During the verification procedure, it should be computationally hard to decide whether two valid signatures belong to the same user or different users. This use of anonymous certificates which do not contain any information about the owner of the certificate duly satisfies this requirement.

**Traceability:** The Tracking Manager (TM) can always get the real ID of message sender, provided that the message is valid. The TM can extract the sender's public key from the certificate and can access certificate database to know the information about the vehicle to which that public key has been assigned.

### 3.4 Security Protocol between OBU and RSU

#### 1) Message Format

The format for messages sent by RSUs is shown in Table 3.2.

**Table 3.2**  
**Message Format for RSU**

Certificate	Message Length	Payload	Timestamp	Signature	RSU ID	TTL
32 bytes	4 bytes	100 bytes	8 bytes	160 bytes	20 bytes	2 bytes

The certificate field includes the certificate assigned to that RSU.

The message payload may include the information on the road condition, curve warnings, local maps etc.

The timestamp and TTL (time to live) fields are used to determine the window during which message is valid.

The signature field contains the digital signature of the first four parts of the message.

The ID may include the name of the RSU, the authorized geographical region to operate, and the authorized message type

#### 2) Secure RSU to OBU communication

The communication between RSU and OBU contains two phases, which are described as follows.

**Signing:** Given Message M, the RSU signs message M before sending it out by using the certificate assigned to it. This is described in following steps.

- Insert the certificate (containing public key and identity of CA) in the certificate field of message.
- Store the payload (curve warning, weather conditions etc.) in the payload field.
- Set the timestamp value using current time and set TTL field according to the message (traffic related messages will have short TTL as compared to messages about road construction or repair)
- Compute the hash value of first four parts and encrypt it using private key of certificate chosen for signing the message.

- Store the digital signature in signature field of message.
- Insert RSU related information (region of operation, RSU location etc) in RSU ID field.

After all the information is filled out, the can be sent into the network.

**Verification:** Any vehicle receiving a message from an RSU will first guarantee that the sender is working under the authorized domain. The vehicle compares the physical location of the message sender with the location information in the RSU's ID field in order to prevent any attacker from taking the device down from one RSU and putting it elsewhere.

Also, the time information in the message payload is in the allowable time window. If so, the receiving vehicle will perform signature verification by using the same technique described in OBU to OBU communication.

### 3) Security Analysis

Using the digital signature technique, the RSU can guarantee sender authentication, message integrity and non-repudiation. Apart from these requirements, the protocol is analyzed in the following aspects.

#### **Prevention of RSU duplication attack**

The message from an RSU has an "RSU ID" field, keeping the RSU's original physical location, as well as its type, indicating the type of traffic management offered by the RSU. Upon receipt of the message, the OBU compares the physical location of the OBU with the location information in the RSU's ID field. If the distance is farther than RSU's transmission range, the OBU ignores the message. Therefore, the RSU replication attack can be defeated. Furthermore, the ID field also provides the information about the type of messages the RSU is authorized to send. If the message content does not match the type of message that the RSU is authorized to send, the message will be dropped. For example, the message containing information about "slippery road ahead due to rain" will be dropped if the RSU is only allowed to send traffic related information.

### **Prevention of Replay Attack**

With a replay attack, an adversary replays the intercepted message from an RSU in order to impersonate as a legitimate RSU. Obviously, it cannot work in the proposed protocol because of the time interval check in verification procedure. Upon receiving the message, the OBU checks the time information in the timestamp to make sure the message is in the allowable time window. If the time information included in the timestamp of the message is not reasonable, the OBU will simply drop the message.

# CHAPTER 4

## IMPLEMENTATION DETAILS

---

The simulation of the proposed scheme was done using NCTUns (National Chiao Tung University network simulator) [12] [13]. NCTUns is specially designed for VANET simulation with built-in microscopic mobility model, traffic simulator and the ability to generate a city map complete with intersections and traffic signals.

### 4.1 Design and Development of Basic Simulation System

The simulation system consisted of a road-map of 1000m X 1000m area with intersection, traffic lights and vehicles (ranging from 10-150).

The system has four main components, which are described as follows.

#### 4.1.1 Vehicle Registration Module

This module assigns the anonymous certificate set to each vehicle and ensures that no two vehicles share the same certificate.

The certificate consists of 128-bit keys and each vehicle is assigned a unique set of 128 certificates. The certificates also have information about CA (Certification Authority) to guarantee the authenticity of the certificates.

```
class Certificate  
{  
    private:  
    string CA_ID;  
    string publicKeyModulus;  
    string publicKeyExponent;  
};
```

Here, CA\_ID holds the information about Certification Authority encrypted using CA's private key (RSA [18] 128-bit encryption was used)

publicKeyModulus and publicKeyExponent hold the public key of the certificate.



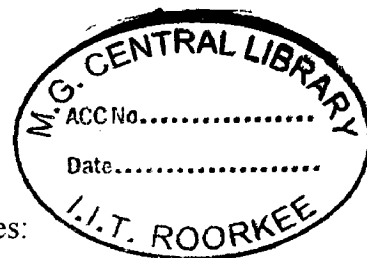
### 4.1.2 Vehicle Database

This database stores vehicle-ID along with the certificate set assigned to that vehicle.

Only two entities are allowed to access this database, which are described as follows.

**Vehicle Registration Module:** This module has write-only access to the database. It can only add entries into the database whenever there is a request for registration of a new module. It cannot read from the vehicle database.

**Tracking Manager:** This module has read-only access to the database. It is the only entity which can get vehicle-ID when provided with a valid certificate as input.



### 4.1.3 Vehicles (or OBUs)

Vehicles in the system can be broadly divided into following two categories:

#### a) Normal Vehicles

These vehicles periodically broadcast routine messages, such as position, current time, direction, speed, brake status, steering angle etc., to aid in routing and safety applications.

These vehicles run a module named CarAgent in the simulation setup which consist of following functions or sub-modules.

***void registerVehicle ( list <Certificate> certificateList )***

This function is used during start of simulation by each vehicle (or OBU) to get a list of 128 certificates assigned to it.

It also stores the corresponding vehicle-ID (License Plate Number, Owner's Name and Date of Manufacture) along with its certificate set into the vehicle database.

```
class Message  
{  
    int length;  
    Certificate vehicleCertificate;  
    DataClass payload;  
    Date date;  
    Time time;  
    Signature vehicleSignature;  
    short int TTL;  
};
```

***void receiveMessage()***

This function checks if there is space available in the receiver's buffer. If not, the packet is dropped. Else, it is stored in the back of queue.

***void calculateDigest(Message \*msg)***

This function calculates the SHA-1 digest of the message and stores it as *hash\_compute*

***void extractDigest(Message \*msg)***

This function decrypts the stored digest using public key stored in certificate field of message and stores it as *hash\_stored*

***void setCertificate(Message \*msg)***

This function randomly selects an anonymous certificate from the vehicle's certificate set and assigns it to the certificate field.

***void setPayload(Message \*msg)***

This message sets the payload (vehicle speed, direction, location etc.) which will be used for routing as well as safety and traffic management applications.

***void setTimeValues(Message \*msg)***

This message sets the timestamp (according to current time) and the TTL field (according to content of payload to indicate the window size during which message is valid).

***void setSignature(Message \*msg)***

This message calculates the SHA-1 digest of message and encrypts it using RSA encryption with the private key

***void sendMessage()***

This function sends the message into the VANET network.

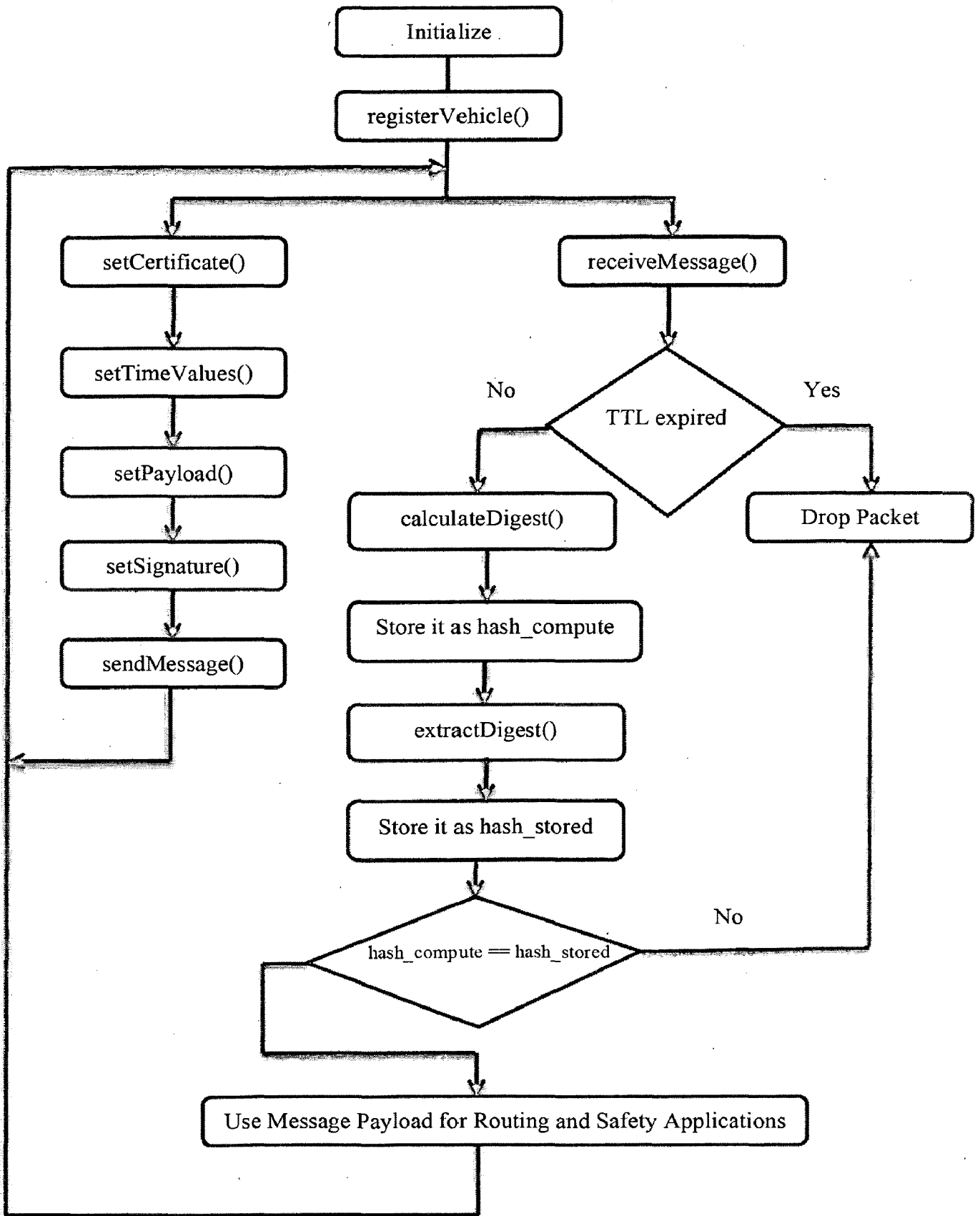


Figure 4.1: Car Agent Implementation

## b) Authorized Vehicles

These vehicles perform the same functionalities as normal vehicles in the system but with added ability to interact with Tracking Manager (TM) to disclose the real-ID of the message sender, in case of a dispute event.

These vehicles run a module named `AuthorizedCarAgent` in the simulation setup which consists of following functions or sub-modules in addition to those already defined in `CarAgent` module.

**`void getVehicleID ( Message *msg, VehicleData *vData )`**

This function is used to get information about the vehicle which sent the Message `msg`. The vehicle-related data is returned in `vData`, which is a struct of type `VehicleData`

```
struct VehicleData
{
    string licensePlateNumber;
    string ownerName;
    Date dateOfManufacture;
};
```

### 4.1.4 Tracking Manager

This entity is the only entity in the system with read-only access to Vehicle Database. It can connect securely with vehicle database and get the information about the vehicle by providing a valid certificate as input.

This entity makes use of following modules.

**`bool isValidCertificate(Certificate *certi)`**

This module verifies that the Certificate `certi` is a valid certificate issued by a trusted CA.

**`void getVehicleData(Certificate *certi, VehicleData *vData)`**

This module gets the vehicle to which the certificate (provided as input parameter) belongs by searching the vehicle database.

## 4.2 Libraries and APIs used

The following libraries and APIs were used to simulate the proposed scheme and obtain results.

### 4.2.1 Encryption and Digital Signature Libraries

The Win32 Encryption Libraries were used for generation of key-pairs, encryption and decryption using RSA, and message digest calculation using SHA-1 hashing scheme.

The following are some of the modules used for implementation of proposed scheme.

***void generateKeyPairs(int keySize, int keysToBeGenerated, list<KeyPair> output)***

This module generates public and private key pairs of size *keySize* (ranging from 32 bits to 4096 bits long).

The generated key pairs are stored in the list *output*.

The number of key pairs to be generated is specified in *keysToBeGenerated*.

***void calculateDigest(char\* input, int inputSize, char\* output)***

This module calculates SHA-1 hash value of the buffer pointed by *input* and stores the hash value in the buffer pointed by *output*.

***void Encrypt(char\* input, int inputSize, Key keyToBeUsed, char\* output)***

This module encrypts the buffer pointed by *input* using RSA encryption algorithm and stores the result in buffer pointed by *output*.

The key used is specified in *keyToBeUsed*.

***void Decrypt(char\* input, int inputSize, Key keyToBeUsed, char\* output)***

This module decrypts the buffer pointed by *input* using RSA decryption algorithm and stores the result in buffer pointed by *output*.

The key used is specified in *keyToBeUsed*.

### 4.2.2 NCTUns Packet APIs

These APIs [12] [13] provided the modules with the ability to modify the payload in the packet. They were used to integrate our message structure into routing.

The following are some modules provided in NCTUns Packet APIs that were used in implementation of proposed scheme:

*char \*pkt\_seek()*

This module returns a pointer to the data contained in the Packet Object

*int replace(char \*newData, int length)*

This module is used to replace the original data contained in the Packet object by the data contained in *newData* buffer.

# CHAPTER 5

## RESULTS AND DISCUSSION

---

The following sections discuss the performance of the proposed privacy scheme.

### 5.1 Simulation Setup

The simulator used is NCTUns [12] [13] (National Chiao Tung University network simulator), a simulator designed for VANET simulations. The simulation parameters are same as those used in GSIS [9] performance monitoring.

**Table 5.1**  
**Simulation Configuration**

<b>Simulation Scenario</b>	City Environment
<b>City Simulation Area</b>	1000m X 1000m
<b>Communication Range</b>	200m
<b>Channel Bandwidth</b>	6 Mbs
<b>Time of simulation</b>	600 sec
<b>Maximum Packet Size</b>	300 bytes
<b>Highway Simulation Area</b>	2500m X 30m
<b>Simulation Time</b>	1200 sec

#### 5.1.1 Mobility Model

The Mobility model used for simulation is a built-in mobility model in simulator itself which is a variant of random waypoint mobility model with following characteristics:-

- Restrict movement of nodes to roads only.
- Reflect changes in movement according to traffic signals
- Support for Car Following
- Support for Lane Changing

The mobility model reads the information about road networks and generates more realistic mobile node mobility using a built-in microscopic traffic simulator.

### 5.1.2 Vehicle Profiles

**Table 5.2**  
**Vehicle Profiles**

Vehicle Profile	Maximum Speed (m/s)	Maximum Acceleration (m/s <sup>2</sup> )	Maximum Deceleration (m/s <sup>2</sup> )
Profile 1	12	1.1	2.2
Profile 2	15	2.2	2.9
Profile 3	18	2.5	3.3
Profile 4	22	2.8	3.5
Profile 5	30	3.2	3.8

### 5.1.3 Metrics Used

The performance metrics considered are the average message delay and average message loss ratio, which are denoted as  $AvgD_{msg}$  and  $AvgLR$ , respectively, and are expressed as follows:

$$AvgD_{msg} = \frac{1}{N_d \cdot M_{sent\_n} \cdot K_n} \sum_{n \in D} \sum_{m=1}^{M_{sent\_n}} \sum_{k=1}^{K_n} X \left( T_{sign}^{n,m} + T_{transmission}^{n,m,k} + T_{verify}^{n,m,k} (L_{n,m,k} + 1) \right)$$

$$AvgLR = \frac{1}{N_D} \sum_{n=1}^{N_D} \frac{M_{consumed}^n}{\sum_{k=1}^{K_n} M_{arrived}^n}$$

where,

$D$  is the sample district in the simulation,



$N_D$  is the number of vehicles in D,

$M_n$  is the number of messages sent by vehicle  $n$ ,

$K_n$  is the number of vehicles within the one hop communication range of vehicle  $n$ ,

$T_{sign}^{n,m}$  is the time taken by vehicle  $n$  for signing message  $m$ ,

$n\_m\_k$  represents the message  $m$  sent by vehicle  $n$  and received by vehicle  $k$ ,

$L_{n,m,k}$  is the length of the queue in vehicle  $k$  when message  $m$  sent by vehicle  $n$  is received,

$M_{consumed}^n$  consumed represents the number of messages consumed by vehicle  $n$  in the application layer, and

$M_{arrived}^n$  represents the number of messages that are received by vehicle  $n$  in the MAC layer

Here, we only consider the message loss caused by the privacy scheme rather than the wireless transmission channel. Hence the message will be lost if the queue is full when the message arrival rate is higher than the message verification rate.

## 5.2 Performance Evaluation

Two sets of simulations were conducted to analyze the impacts of having different traffic loads and cryptographic algorithm processing speeds.

### 5.2.1 Byte Overhead and Average Signature Verification Delay

The average signature verification delay is calculated at average traffic load of 70 vehicles.

**Table 5.3**  
**Byte Overhead Comparison between GSIS and the proposed scheme**

Privacy Scheme	Certificate size (in bytes)	Signature Size (in bytes)	Other Overhead (in bytes)	Total Packet overhead (in bytes)	Average Signature Verification Delay (in ms)
GSIS	32	192	20	244	4.2
Proposed Scheme	32	160	10	202	3.6

## 5.2.2 Impact of Traffic Load

The density of the vehicles on the road is the main factor that has a major impact on the system performance, since it is related to the total number of messages received by each vehicle.

### 5.2.2.1 Impact of Traffic Load on Average Message Loss Ratio

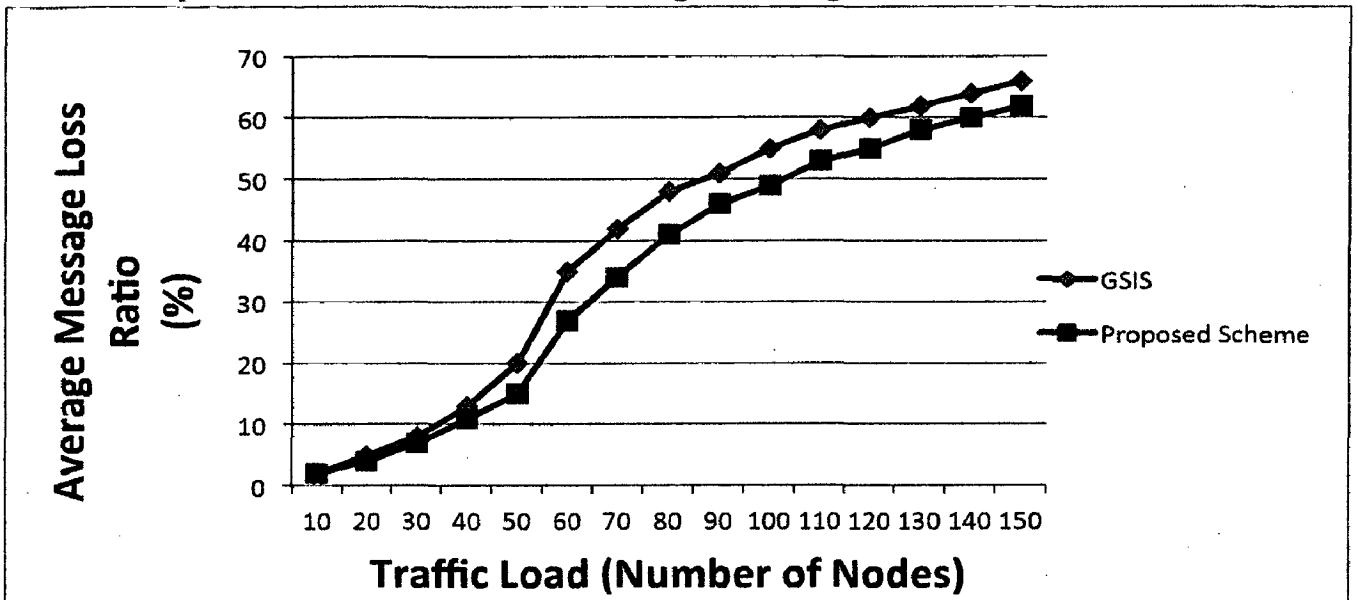


Figure 5.1 : Average Message Loss Ratio in city scenario

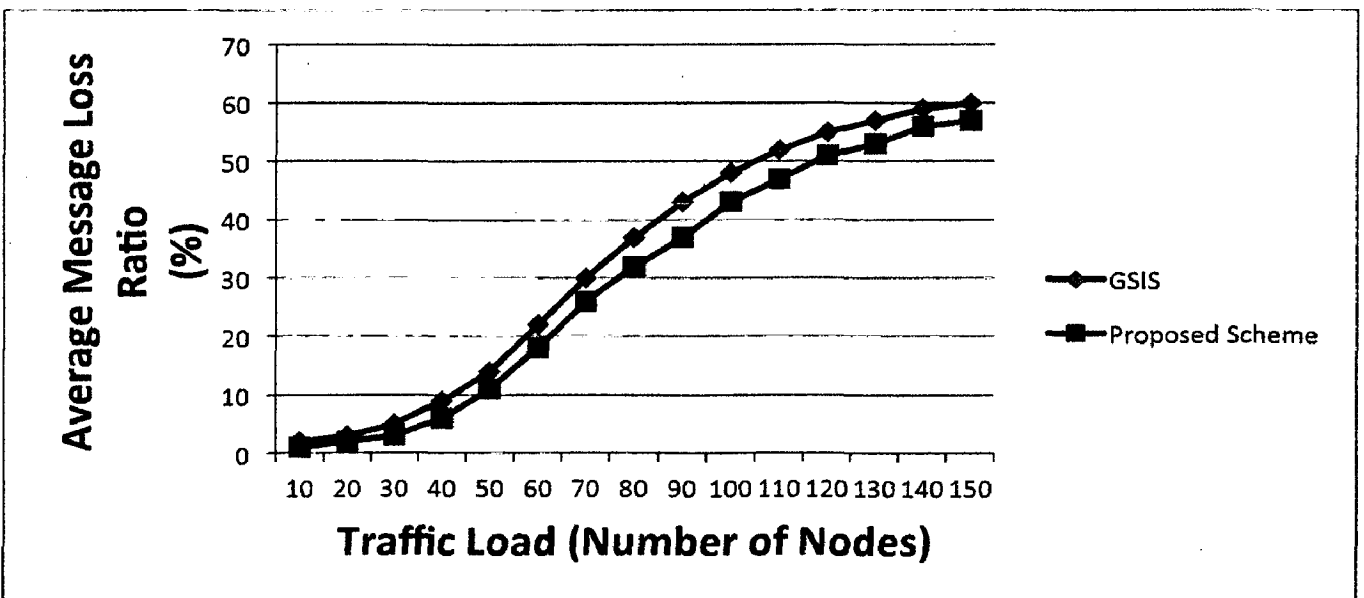


Figure 5.2 : Average Message Loss Ratio in Highway Scenario

The increase in traffic load severely affects message loss ratio (as shown in Fig. 5.1- 5.2), reaching as high as 65% when traffic load is up to 150. However such traffic load can be experienced whenever there is severe traffic jam. In this situation, it is acceptable is a large number of messages are dropped because most of the messages are repeatedly sent by each vehicle.

The improvement in average message loss ratio by the proposed scheme over GSIS (ranging from 2% – 8%) is achieved because of following reason:

- **Small packet overhead:** Since proposed scheme imposes a much lesser byte overhead in message as compared to GSIS (202 bytes as compared to 244 bytes), more messages can be stored in the queue at the receiver’s end. Hence, fewer messages will be dropped.
- **Small signature verification delay:** Due to lesser amount of time taken for signature verification (to ensure message integrity), the messaged will be processed faster and therefore messages will be emptied from the queue at a faster rate, hence an improvement in average message loss ratio.

### 5.2.2.2 Impact of Traffic Load on Average Message Delay

It was seen that with increasing traffic load, the message end to end delay does not change much (around 30 ms), which is smaller than maximum allowable message end to end transmission latency (100 ms). The results are shown in Fig. 5.3-5.4.

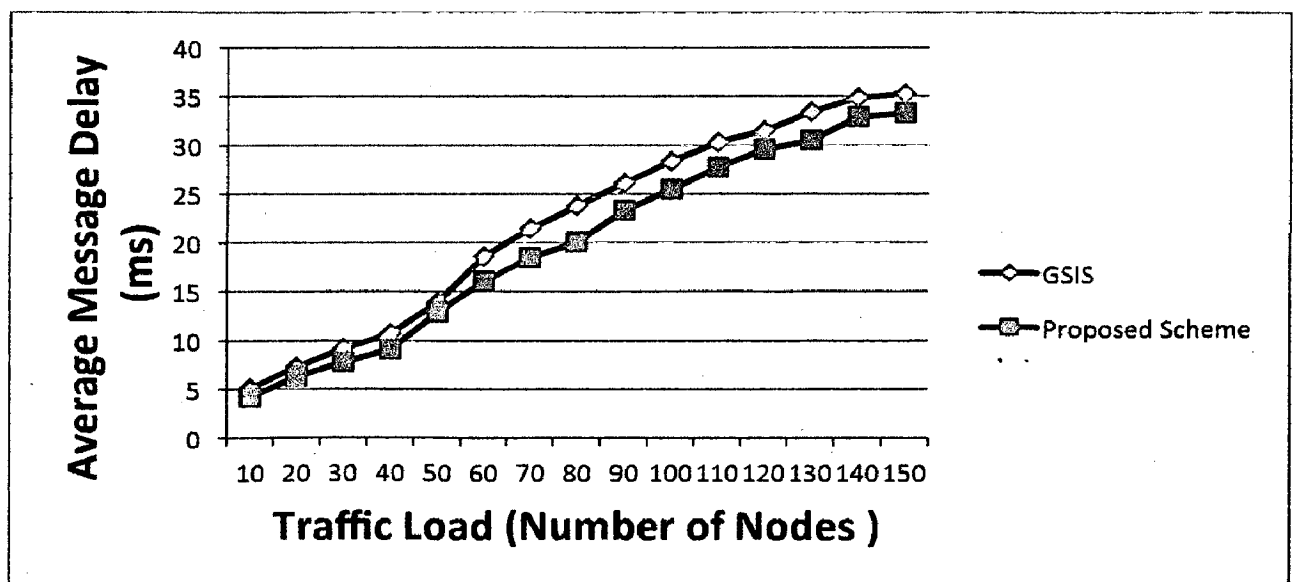


Figure 5.3 : Average Message Delay in City Scenario

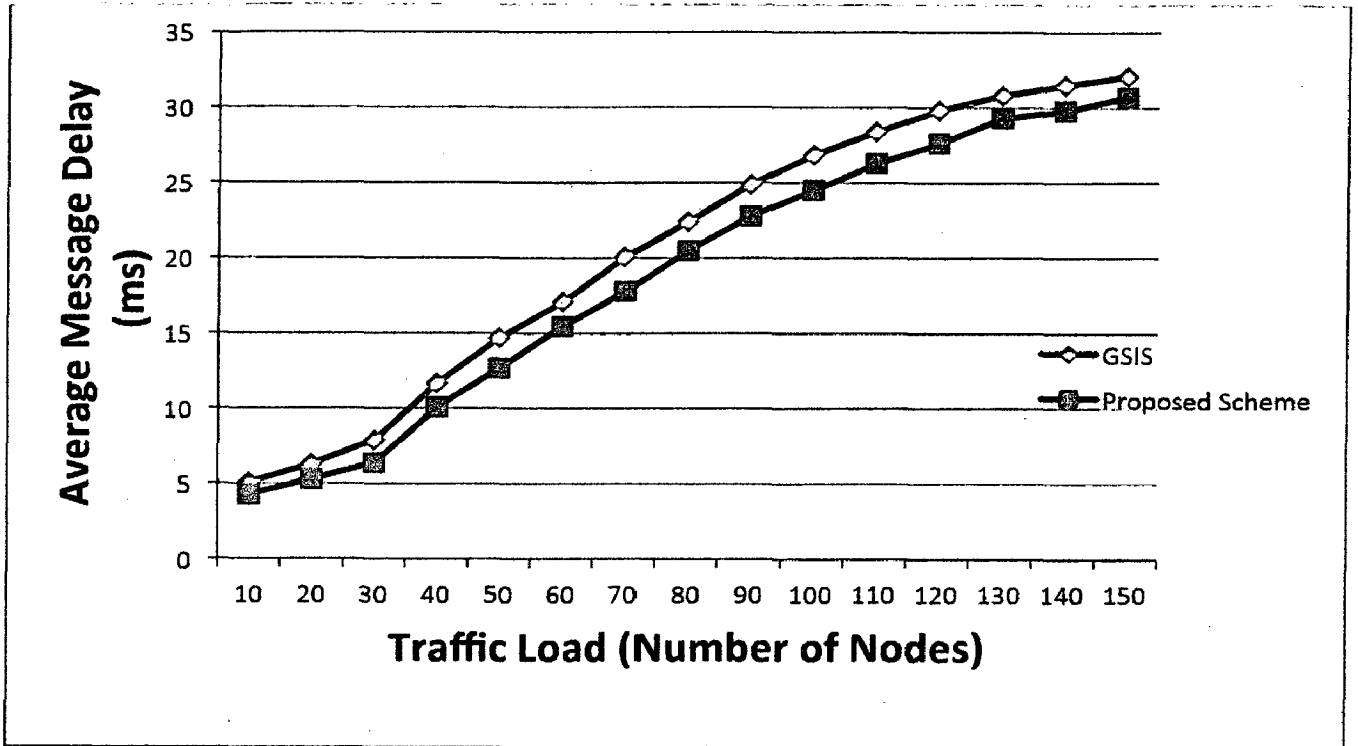


Figure 5.4 : Average Message Delay in Highway Scenario

The improvement in average message delay (ranging from 0.8 to 3.7 ms) as compared to GSIS was achieved because of following reasons:

- **Small signature verification delay:** Due to lesser amount of time taken for signature verification (to ensure message integrity), the messages will be processed faster and hence message end to end delay will be improved.
- **Small packet overhead:** Due to lesser byte overhead employed by proposed scheme, the time taken in message signing (encryption) will be reduced, resulting in faster message processing and hence improvement in average message delay.

### 5.2.2.3 Impact of Traffic Load on Signature Verification Delay

Another important factor that determines the performance of a security protocol is the latency taken by the cryptographic operations in the protocol. The signature verification delay (to ensure integrity of messages) was found to range from 1.5 to 8.4 ms. The results are shown in Fig. 5.5.

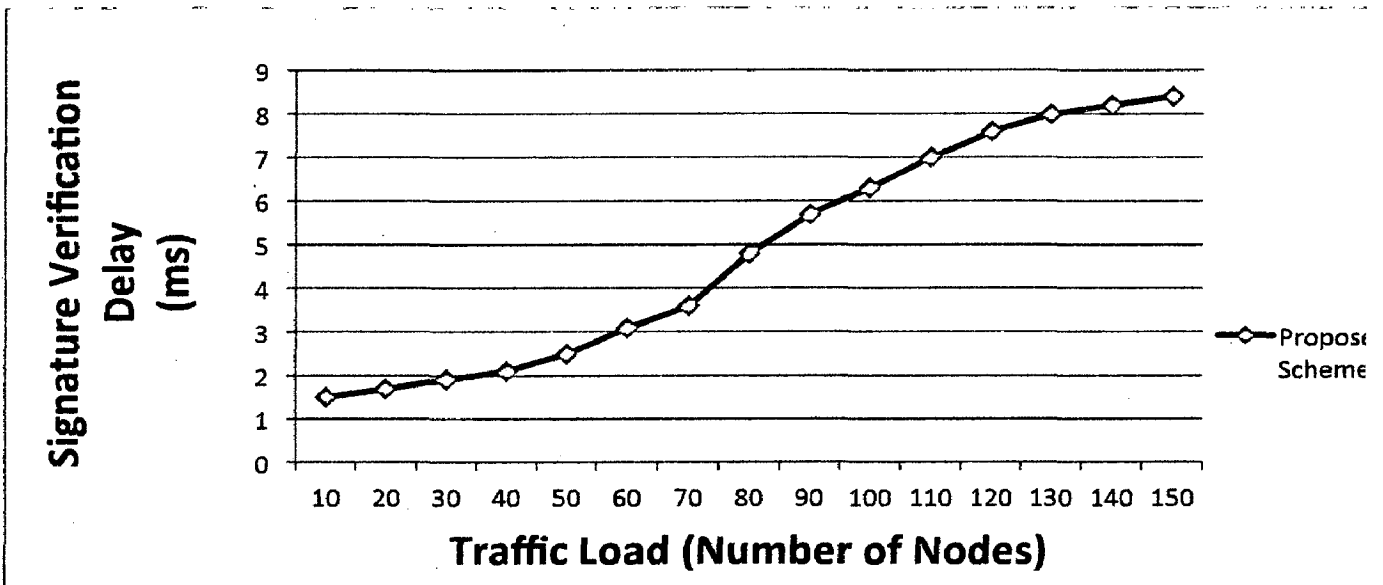


Figure 5.5 : Impact of Traffic Load on Signature Verification Delay

It is shown that the signature verification delay increases with increasing traffic load. As shown, the increase in signature verification delay saturates as the traffic load reaches around 150 because at this load, the receiver's queue is mostly full, hence nearly same time taken to process packets in the queue.

# CHAPTER 6

## CONCLUSION AND FUTURE WORK

---

Vehicular Ad hoc Networks (VANETs) are one of the most promising applications of Ad-hoc networking technology. VANETs are not only suitable for commercial and entertainment applications but also for safety and traffic management. However, very few studies have been reported on security in VANETs and to ensure the security and conditional privacy in service-oriented VANETs still represents a challenging issue.

In this dissertation, a secure conditional privacy scheme based on digital signature schemes and suitable for position based routing has been proposed for IVC applications. The central notion of the scheme is that each vehicle is assigned a set of anonymous but unique certificates with the vehicle to certificate-set mapping stored in a vehicle database with access to that database restricted to authorities only. This scheme satisfies the requirements of integrity, authenticity, non-repudiation and privacy through use of anonymous certificates, and traceability can be achieved by authorities by accessing vehicle database. Extensive simulation has been conducted on both city road and highway systems to demonstrate that the message delay and loss ratio can be kept low, even in the presence of a large computational latency due to the cryptographic operations. Performance comparisons and security analysis show that the proposed scheme is efficient and suitable for service-oriented vehicular ad hoc networks.

### 6.1 Suggestions for future work

Since this is an open area for research, the following issues may be addressed in future.

1. The scheme proposed in this dissertation employs a central database to store vehicle to certificate-set mapping. In future, the data can be distributed over several databases arranged in hierarchical manner.
2. The proposed scheme lacks the facility of membership revocation. In the case some certificates are compromised or a vehicle itself is compromised, then counterfeit messages can be introduced in the network. One solution can be the provision for releasing and

distributing Revocation Lists (RLs). These lists can contain the compromised certificates and can be distributed through RSUs.

3. The proposed scheme may fall short if the intruder follows victim's vehicle in an isolated environment with no other vehicle. In this case, the intruder can map the certificates to the victim. The solution can be to install a fresh set of certificates into victim's OBU and add the old certificate set into RLs.

# REFERENCES

---

- [1]. Leontiadis I., Mascolo C., "GeOpps: Geographical Opportunistic Routing for Vehicular Networks", *World of Wireless, Mobile and Multimedia Networks*, IEEE International Symposium, pp.1-6, June 2007.
- [2]. Fan Li, Yu Wang, "Routing in vehicular ad hoc networks: A survey", *Vehicular Technology Magazine*, IEEE , vol.2, no.2, pp.12-22, June 2007.
- [3]. Karp B. and Kung H. T., "GPSR: greedy perimeter stateless routing for wireless networks" in *Mobile Computing and Networking*, pages 243-254, 2000.
- [4]. Naumov V., Gross T.R., "Connectivity-Aware Routing (CAR) in Vehicular Ad-hoc Networks", 26th IEEE International Conference on Computer Communications. IEEE, pp.1919-1927, May 2007.
- [5]. Zhao J, Cao G., "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks", in *Proceedings of 25th IEEE International Conference on Computer Communications*, pp.1-12, April 2006.
- [6]. K. Plöb, T. Nowey and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks" in *Proceedings 1st International Conference on Reliable Security*, Vienna, Austria, pp. 374–381, April 2006.
- [7]. M. Raya and J. Hubaux, "The security of vehicular ad hoc networks" in *Proceedings 3rd ACM Workshop Security Ad Hoc Sensor Networks*, Alexandria, VA, pp. 11–21, November 2006.
- [8]. "National highway traffic safety administration, U.S. Department of Transportation, Vehicle Safety Communications Project—Final Rep.", Online available at: <http://www-nrd.nhtsa.dot.gov/pdf/nrd12/060419-0843/PDFTOC.htm>
- [9]. Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, Xuemin Shen; , "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", *Vehicular Technology*, IEEE Transactions on Vehicular Networks, vol.56, no.6, pp.3442-3456, November 2007.
- [10]. A. Aijaz, B. Bochow, D. Florian, A. Festag, M. Gerlach, R. Kroh, and L. Tim, "Attacks on inter vehicle communication systems—An analysis" in *Proceedings 3rd International Workshop Intelligent Transportation*, Hamburg, Germany, March 2006.



- [11]. Daza V., Domingo-Ferrer J, Sebe F, "Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks", *Vehicular Technology, IEEE Transactions on*, vol.58, no.4, pp.1876-1886, May 2009.
- [12]. S.Y. Wang, C.L. Chou, and C.C. Lin, "The GUI User Manual for the NCTUns 6.0 Network Simulator and Emulator".
- [13]. S.Y. Wang, C.L. Chou, C. C. Lin, and C.H. Huang, "The Protocol Developer Manual for the NCTUns 6.0 Network Simulator and Emulator".
- [14]. Kevin C. Lee, Uichin Lee, Mario Gerla, "Survey of Routing Protocols in Vehicular Ad Hoc Networks", *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, IGI Global, Oct, 2009.
- [15]. Yun-Wei Lin, Yuh-Shyan Chen, and Sing-Ling Lee, "Routing Protocols in Vehicular Ad Hoc Networks: A Survey and Future Perspectives", *Journal of Information Science and Engineering*, Vol. 26, No. 3, pp. 913-932, May 2010.
- [16]. Sandhaya Kohli, Bandanjot Kaur, Sabina Bindra, "A comparative study of Routing Protocols in VANET", in *Proceedings of ISCET*, 2010.
- [17]. Lochert C., Hartenstein H., Tian J., "A survey of routing protocols for vehicular ad hoc networks in city environments", *Intelligent Vehicles Symposium*, pp. 156-161, June 2007.
- [18]. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Comm. ACM*, vol. 21, pp. 120-126, 1978.
- [19]. Chung-Ming Huang, Yuh-Shyan Chen, "Application in vehicular ad hoc networks" in *Telematics Communication Technologies and Vehicular Networks: Wireless Architectures and Applications*, Hershey : IGI, pp.229-236, 2010.