Anonymous, Secure and Efficient Vehicular Communications

by

Xiaoting Sun

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2007

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

Xiaoting Sun

I understand that my thesis may be made electronically available to the public.

Xiaoting Sun

Abstract

Vehicular communication networking is a promising approach for facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. However, it is subject to various malicious abuses and security attacks which hinder it from practical implementation.

In this study, we propose a novel security protocol called GSIS based on group signature and identity-based signature schemes to meet the unique requirements of vehicular communication networks. The proposed protocol not only guarantees security and anonymity, but also provides easy traceability when the identity of the sender of a message has to be revealed by the authority. However, the cryptographic operations introduced in GSIS as well as the existing public key based message authentication protocols incur some computation and communication overhead which affect the system performance. Simulation results show that the GSIS security protocol is only applicable under light traffic conditions in terms of the message end to end delay and message loss ratio.

Both the GSIS protocol and the existing public key based security protocols have to sign and verify all the received messages with asymmetric algorithms. The PKI based approach also has to attach a public key certificate in each packet. Therefore, to enhance the system performance and mitigate the message overhead without compromising the security requirement, this study further proposes an enhanced TESLA based Secure Vehicular Communication (TSVC) protocol. In TSVC, the communication overhead can be significantly reduced due to the MAC tag attached in each packet and only a fast hash operation is required to verify each packet. Simulation results show that TSVC maintains acceptable message latency, using a much smaller packet size, and significantly reduces the message loss ratio as compared to GSIS and existing PKI based protocols, especially when the traffic is denser. We conclude that the proposed approach could serve as good candidate for future vehicular communication networks.

Acknowledgements

First, I would like to express my gratitude to my supervisor Prof. Pin-Han Ho for his research enthusiasm and inspiration, as well as the considerate encouragement and support concerning various decisions I made during these years. He helped me to set up the master's research topic and offered tremendous assistance on how to write papers. I appreciate my co-supervisor Prof. Ian Goldberg for his insightful and detailed comments about this thesis. I thank him for his efforts and time spent on the thesis modifications. His meticulous research attitude inspired me greatly.

I would especially like to acknowledge Prof. Raouf Boutaba, Prof. Sherman Shen, and Prof. Urs Hengartner for attending my thesis seminar and reading this thesis.

I would also like to thank to Xiaodong Lin, my academic brother, who helped me tremendously from start to finish. It was he who taught me how to run simulations in the Linux environment at the very beginning. He also provided many insightful ideas on how to improve the quality of my papers until they got published. His hard-working spirit, goal-oriented approach, and humorous personality were inspirational during my studies and will be in the future.

I also would like to say 'Thank you' to Ms. Margaret Towell who has helped to make the valuable three-month internship program possible.

Finally, I would like to show appreciation to Chenxi Zhang, Haojin Zhu, Chao Li, Leila Chinaei, Ahmed Ataullah, Rongxing Lu and all the other friends who helped me in all aspects of my study during the two years of my master's program and made my academic life fruitful and colorful.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

With the advancement of wireless communication technologies in recent years, there has been increasing interest in road-side vehicular communications which aim at improving driving safety and traffic management. By being equipped with communication devices, vehicles can communicate with each other as well as with the Road Side Units (RSUs) located in critical points of the road, such as intersections or construction sites. This self-organized network formed by connecting the vehicles and RSUs is called a Vehicular Ad-Hoc Network (VANET).

In a VANET, On Board Units (OBUs) (the communication devices in the vehicles) frequently broadcast routine traffic related messages with the information of position, current time, direction, speed, acceleration/deceleration, traffic events, etc. [DoT2006]. In addition, emergency messages are generated and sent by vehicles in case of emergency events such as sharp braking, traffic jams, or accidents. RSUs are also able to broadcast traffic related messages, such as 'maximum curve turning speed' or 'road construction ahead' notifications. Routine traffic related messages are one-hop broadcast without message relay, while emergency messages are transmitted through a multi-hop path, where the receiver of the messages continues broadcasting the message to the vehicles which follow. The VANET enables vehicles to communicate with each other. By frequently broadcasting and receiving traffic related messages, drivers are expected to get a better awareness of their driving environment. Early action can be taken to respond to an abnormal situation to avoid any possible damage or to follow a better route by circumventing a traffic bottleneck. For example, if drivers can receive an 'emergency braking' message from the vehicles several cars ahead, or a message such as 'change lane notification' from the cars in the neighboring lanes, they can take early action to slow down to avoid collisions. In addition, with a VANET connected with the backbone Internet, passengers sitting in the cars can go online to enjoy various entertainment-related Internet services with their laptops.

Tremendous attention from both industry and academia has been absorbed to this newly generated and promising network scenario. Doubtlessly, the creation of the VANET is a great advantage to traffic management, road-side safety related applications, and passengers' entertainment experience. Nevertheless, any malicious behavior of users, such as modification and replay attacks with respect to the disseminated traffic related messages, could be fatal to the other users. Furthermore, user related privacy information such as driver's name, license plate, speed, position, model and traveling route

has to be well-protected, which means the users should be kept anonymous when their vehicles are providing traffic related information. On the other hand, in the case of a dispute such as a crime/car accident scene investigation, the authorities should be able to trace and reveal the identities of the message senders to help expose the reason of the accident or look for witnesses (this co-existing anonymity and identity traceability is called conditional anonymity [RH2005]). Therefore, a suite of carefully designed security mechanisms, which are critical to its overall success, should be developed for achieving security and preserving conditional anonymity in VANETs,

This study mainly tackles the problems of security assurance and conditional anonymity in VANETs. We introduce a novel security and anonymity preserving protocol named GSIS, by integrating the techniques of group signature and identity-based signature algorithms. Unlike the previous studies, we divide the security problems into two categories: the communications between OBUs and OBUs, as well as between OBUs and RSUs, due to their different security requirements. In the first category, group signatures are used to secure the communication between OBUs and OBUs, where messages can be securely and anonymously signed by the senders, and meanwhile, the identities of the senders can be recovered by the authorities. On the other hand, identity-based cryptography is used to authenticate the messages sent by RSUs, within which the signature overhead can be reduced. Further, the efforts of deploying a public key infrastructure system can be totally avoided because the identity of a user is simply taken as its public key in identity-based cryptography. However, experiment and simulation results show that the GSIS protocol itself incurs a high message loss ratio especially when the traffic becomes denser.

The study then proposes an enhanced security scheme named TSVC (TESLA-based Secure Vehicular Communications) to improve the performance and the operating efficiency of the original GSIS and PKI based security protocols further without affecting the fundamental security and conditional anonymity requirements in VANETs. The proposed TSVC scheme can be applied to both the reported PKI based security schemes and the GSIS security protocol. Informed by the TESLA mechanism (Timed Efficient Stream Loss-tolerant Authentication) [PCTS2002], the new TSVC protocol only needs to do symmetric MAC operations at the receiver side, which is sufficient to authenticate the source of the message, instead of performing any asymmetric verification. Also since only a short MAC tag is attached at each message, the extra message length and the bandwidth overhead due to the security mechanism can be reduced significantly. Moreover, TSVC is much

different from any of the other security schemes in the resultant message loss ratio, which is found to be almost independent of the traffic density.

Extensive simulations were conducted which demonstrated that the new TSVC protocols significantly reduce the message loss ratio and maintain acceptable message latency, as compared to existing PKI based security protocols as well as the GSIS protocol. The performance enhancement is more obvious when traffic becomes denser.

Considering the future convergence of Internet and vehicular networks, this study also briefly introduces a practical three-layer network architecture based on the standard of IEEE 802.16e mesh mode [IEEE802.16e-2005] for providing Internet access to vehicles for broader and more versatile application scenarios.

The rest of this thesis is organized as follows: Related works and some preliminary and background knowledge as well as the network architecture are given in the later part of this chapter. In Chapter 2, the detailed GSIS protocol is presented including the simulation result. In Chapter 3, the enhanced version of the security protocol called TSVC is described followed by performance evaluations from the simulation result. Finally, the study is concluded in Chapter 4.

1.1 Related Work

Currently, the IEEE 802.11p task group is working on the DSRC (Dedicated Short Range Communications) [DoT_DSRC] standard which enhances the 802.11 protocols to support wireless data communications between vehicles and the road-side infrastructure [USDoT2006]. Extensive studies have been reported for inter-vehicle communications (IVC). However, most of them have focused on either a specific application scenario, feasibility, MAC layer performance analysis, or various routing solutions [TC2003, LH2004, NAG2004, K2005, YASM2005]. Some efforts have been made to improve security and anonymity [RH2005, PNM2006, ABD2006, DoT2006, RH2007, RPH2006, PKHK2006, IEEE1609.2-2006, SURH2007, FRF2007, GBW2007, PP2005].

The studies in [PNM2006, ABD2006] discussed general security issues such as attack models, security requirements and properties of IVC systems instead of providing a solution to ensure these requirements. Most of the current research [RH2005, RH2007, RPH2006, SURH2007] dealing with security and anonymity issues for VANETs propose to use Public Key Infrastructure (PKI) based security schemes. Vehicles are installed with a large number of anonymous certificates (43,800 certificates [RH2007]) and randomly select one of them at a time to sign each message in order to

meet the driver's privacy requirement. Also, a unique electronic identity is used to verify the identities of vehicle owners by the police in case of disputes.

The Vehicle Safety Communications (VSC) project group, part of the Department of Transportation in the United States, evaluated the feasibility of using the DSRC standard to support safety related applications [USDoT2006]. In [DoT2006], the VSC group also proposes to use a list of short-lived anonymous certificates to preserve the privacy of drivers; the certificates are discarded after being used. The scheme provides a higher security level than [RH2007] because the certificates are blindly signed by the Certificate Authority (CA) in order to deal with the 'insider' attack. A linkage marker is used for the escrow authorities to connect the blindly-signed anonymous certificates with a single vehicle.

The trial-use IEEE standard [IEEE1609.2-2006] for secure vehicle communications was released in July 2006. It provides detailed documentation including the format of the security messages and the choice of the cryptosystem. [IEEE1609.2-2006] adopts the VSC group's principal idea which uses anonymous public keys to sign and verify messages and use short-lived anonymous certificates to automatically revoke keys.

One disadvantage of the above schemes is the communication cost incurred by the certificates which have to be added to each message. (Each anonymous certificate has a short life time such as several minutes. Even if the certificate does not have to be added to each message since it could be cached by the receiver for later public key authentication sending from the same source, considering the dynamic changing neighbors of each message sender, whenever a new vehicle joins the group, the certificate has to be added to the message.)

In addition, all compromised or expired vehicles have to be revoked, as do all of the certificates owned by those revoked vehicles. The revocation is done by distributing CRLs (Certificate Revocation Lists). The CRL size is huge and is not efficient to transfer over the Internet. To overcome this high storage cost of the CRL, Raya, et al. in [RJPAH2006] proposed to use a tamper-proof device to assist the membership revocation. If a node has to be revoked, the CA sends a revocation message to the node. Once the node receives the revocation message, its tamper-proof device automatically erases all the anonymous public keys and stops signing messages. Therefore, the huge CRL does not have to be distributed over the Internet. [RJPAH2006] also presents a distributed revocation protocol to locally and temporally revoke the attacker once it is detected to have sent fake messages.

Another drawback of the above schemes is that they violate the location privacy requirement and are subject to a movement tracking attack. The movement path of any vehicle can easily be traced by malicious global message observers, even if the public keys do not contain the real ID information and are updated frequently. This is because each public key has a life time of several minutes [RH2007] and different vehicles update their public keys at different times. Therefore, the public key which changes at a particular time *t* is sure to be from the same source who uses a different public key before the moment *t*, because public keys used by other vehicles remain the same before and after *t*. In this way, messages sent by the same vehicle can be connected and thus the whole movement of a vehicle can be traced. To cope with this location privacy issue, Freudiger et al. in [FRF2007] employed the concept of a Mix-Zone. All vehicles within the mix zone will share a secret key initiated by the RSU. All traffic messages are encrypted by this shared secret key. Public keys are changed when vehicles go out of the mix zone. The location information is therefore protected and cannot be observed by external adversaries.

[SURH2007] proposed a protocol to secure the report of emergency events such as a crash. It presents a new security architecture from which vehicles can update their anonymous cryptographic credentials while they are on the go with the assistance of the Roadside Access Point (RAP). Their scheme also supports a decentralized architecture when providing conditionally anonymous inter-vehicle communications.

Unlike those asymmetric public key based security schemes, [CJW2005] and [XSSSZ2007] have proposed using symmetric key based ideas to secure the communications between vehicles and the roadside infrastructures used to gain Internet access. However, the former scheme which uses short-lived pseudonyms to do authentication severely violates the privacy of the user's route. Even though the identities are hidden, the whole traveling route can be tracked by a sequence of the collaborated roadside infrastructures. Also, to check the validity of the handles of the vehicles, the roadside infrastructure has to contact the ombudsman every time a vehicle is associating with it, which creates a huge communication latency. The latter scheme uses a randomly selected key set drawn from a local key pool to do message authentication. The identity privacy and traceability highly depend on the property that there is a high probability that two vehicles might share one of the keys used to do the authentication, but there is a low probability that two vehicles share all of the keys used to do authentication. Therefore it relies highly on the size of the each key pool. Also, there are heavy

storage costs for each roadside infrastructure. These disadvantages make them not applicable for real world deployment.

This study first proposes a novel security protocol from a different point of view. It is based on group signature and identity based signature schemes which not only meets the security and conditional anonymity requirements for the VANET, but also simplifies the certificate management, reduces the size of the CRL and the storage cost of the anonymous certificate list on the authority's server side. Moreover, it avoids the efforts of deploying a public key infrastructure system for the road-side units. Applying group signature schemes to VANETs was first mentioned in [PP2005] in a paragraph. No details were given in this paper. In addition, Guo et al. in [GBW2007] also proposed to use group signature schemes to preserve the security and privacy for VANETs. This work was published during the time when this thesis was being written.

1.2 Preliminaries and Background Knowledge

1.2.1 Attack Model

There are several possible attacks on VANETs:

1. Message integrity attack: The adversary may modify the contents of the messages sent by others to meet specific purposes.
2. Fake Messages: The adversary may send messages whose contents do not correspond to the real world traffic situation. For example, one may send a fake traffic jam message to the others on the road so that it can manipulate to get a better traffic condition.
3. Message replay attack: The adversary replays the messages sent some time before in order to disturb the traffic.
4. Impersonation attack: The adversary may pretend to be another vehicle or even an RSU to send false messages to fool others.
5. Denial of service (DoS) attack: The adversary sends irrelevant messages to take up the channel and consume the computational resources of other nodes.
6. Movement tracking: In this case, the adversary intercepts a significant amount of messages in a certain region, and traces a vehicle in terms of its physical position and moving patterns simply through information analysis.

Since DoS attacks in wireless communication networks have been extensively investigated in the past, [LY2006, M2005], in this study we will focus on non-DoS related security and privacy issues.

1.2.2 Security Requirements

In order to mitigate the potential threats in the above attack models, a well-developed security mechanism should meet the following requirements:

1. Message Integrity and Source Authentication: All messages should be delivered unaltered and the origin of the messages should be authenticated to guard against impersonation attack.
2. Message Authenticity: Messages should reflect the real situation instead of being forged maliciously.
3. Anonymous Vehicle Authentication: The identities of vehicles should be hidden to normal message receivers during the authentication process to protect the senders' private information, such as position, plate number, and movement route.
4. Avoid Movement Tracking: The movement paths of vehicles should not be tracked by message observers.
5. RSU ID Exposure: Roadside infrastructures have no anonymity issue. Instead, they should evidently present their identities, including the geographical location, what kind of equipment it is, what type of services it is authorized to provide, etc.
6. Vehicle ID Traceability: The law authority should be able to determine the real identities of the message senders in the event of a dispute.
7. Efficiency: The security protocol should be efficient with small communication overhead and acceptable processing latency.
8. Robustness: The network should be able to function well even under a denial of service attack.

As will be shown later, the protocols in this study satisfy the security requirements 1, 3, 5, 6, and 7.

1.2.3 Bilinear Pairing

The concept of group signatures was first proposed by Chaum and van Heyst [CvH1991] in Eurocrypt 1991. The main feature of a group signature scheme is that it provides anonymity of the signers. The verifiers can only judge that the signer belongs to a particular group without knowing who the signer is in the group. However, in exceptional situations, the group manager is able to reveal the unique identity of the signature's originator.

We first review the concept of bilinear pairing which is the fundamental technique of the proposed protocol. Bilinear pairing has had tremendous interest and attention from the security community since the technique has been identified to be able to solve some problems that were previously thought unsolvable, such as an id-based signature scheme [BF2001]. Another advantage is that pairing-based schemes can save communication bandwidth compared to traditional schemes such as RSA and ElGamal due to a smaller signature overhead.

Definition 1, Admissible bilinear map [BF2001]: Let $(G_1,\times)$, $(G_2,\times)$ and $(G_T,\times)$ be three groups of the same prime order p, and P_1,P_2 be generators of G_1 and G_2 ,respectively. An admissible bilinear map is a map $\hat{e}: G_1 \times G_2 \to G_T$ satisfying the following properties:

Bilinearity: $\forall (U,V) \in G_1 \times G_2$ and $\forall a,b \in Z_p$, $\hat{e}(U^a,V^b) = \hat{e}(U,V)^{ab}$;

Non-degeneracy: $\hat{e}(P_1,P_2) \neq 1_{G_T}$;

Computability: there exists an efficient algorithm to compute $\hat{e}(U,V)$, for all $(U,V) \in G_1 \times G_2$.

Definition 2, Bilinear parameter generator [BF2001]: A bilinear parameter generator *gen* is a probabilistic algorithm that takes a security parameter 1^k as input and outputs a 7-tuple $(p,P_1,G_1,P_2,G_2,G_T,\hat{e})$ in polynomial time satisfying the following conditions: p is a prime with $2^k < p < 2^{k+1}$, the groups G_1, G_2 and G_T are all of order p, P_1,P_2 generate G_1 and G_2, respectively, and $\hat{e}: G_1 \times G_2 \to G_T$ is an admissible bilinear map.

Next we present the underlying assumptions which are the basis of the proposed security protocol:

Let G_1, G_2 be cyclic groups of prime order p, where possibly $G_1 = G_2$.

1. $q-$Strong Diffie-Hellman problem (q-SDH) [BBS2004].

Let g_1, g_2 be generators of G_1 and G_2. The q-SDH problem in (G_1, G_2) is defined as follows: given a $(q+2)$ tuple $(g_1, g_2, g_2^{\gamma}, ..., g_2^{(\gamma^q)})$ as input, output a pair $(g_1^{1/(\gamma+x)}, x)$ where $x \in Z_p^*$. An algorithm A is said to have advantage ξ if

$\Pr[(g_1, g_2, g_2^{\gamma}, ..., g_2^{(\gamma^q)}) \xrightarrow{A} (g_1^{1/(\gamma+x)}, x)] \geq \xi$, where $x \in Z_p^*$ and γ is a random element of Z_p^*.

The $(q, t, \xi) - SDH$ assumption holds in (G_1, G_2) if no t-time algorithm has advantage at least ξ in solving the q-SDH problem in (G_1, G_2).

2. Decision Linear problem in G_1 [BBS2004].

Let g_1, u, v, h be generators of G_1. The decision linear problem is that given $u, v, h, u^a, v^b, h^c \in G_1$ as input, to output *yes* if $a + b = c$ and *no* otherwise.

The advantage of an algorithm A is defined as

$$Adv Linear_A \overset{def}{=} |\Pr[A(u, v, h, u^a, v^b, h^{a+b}) = yes : u, v, h \xleftarrow{R} G_1, a, b \xleftarrow{R} Z_p] - \Pr[A(u, v, h, u^a, v^b, \eta) = yes : u, v, h, \eta \xleftarrow{R} G_1, a, b \xleftarrow{R} Z_p]|$$

An algorithm A (t, ξ)-decides Decision Linear in G_1 if A runs in time at most t, and $Adv Linear_A$ is at least ξ.

The (t, ξ)-Decision Linear Assumption (LA) holds in G_1 if no t-time algorithm has advantage at least ξ in solving the Decision Linear problem in G_1.

3. q – Bilinear Diffie Hellman Inversion problem (q-BDHI) [BLMQ2005]

Let (G_1, G_2, G_T) be bilinear map groups of order p, with generators $g_1 \in G_1$ and $g_2 \in G_2$. The q-BDHI problem in (G_1, G_2, G_T) consists in, given $(g_1, g_2, g_2^{x}, g_2^{(x^2)}, ..., g_2^{(x^q)})$, computing $\hat{e}(g_1, g_2)^{1/x} \in G_T$, where x is a random element of Z_p^*.

An algorithm A is said to have advantage ξ if

$\Pr[(g_1, g_2, g_2^{x}, ..., g_2^{(x^q)}) \xrightarrow{A} \hat{e}(g_1, g_2)^{1/x}] \geq \xi$, where x is a random element of Z_p^*.

The $(q,t,\xi)-BDHI$ assumption holds in (G_1, G_2) if no t-time algorithm has advantage at least ξ in solving the q-BDHI problem in (G_1, G_2).

1.3 Network Architecture

An inter-vehicular communication network is used to exchange traffic-related messages to enhance road safety and help manage traffic. In order to provide infotainment for passengers, vehicles are expected to have Internet access. In addition, some safety-related applications also depend on Internet access such as certificate, CRL, or other keying material updating, broad-view traffic monitoring in the central office, automatic emergency reporting, or the retrieval of a stolen car.

In this section, we introduce a three-layer network architecture based on WiMax [IEEE802.16e-2005] as shown in Figure 1-1, in which broadband wireless Internet access is supported for both vehicles' safety related applications and general mobile users' entertainment related applications.

The top layer is composed of WiMax base stations, which are interconnected either through peer-to-peer wireless communication or through wired Internet connections.

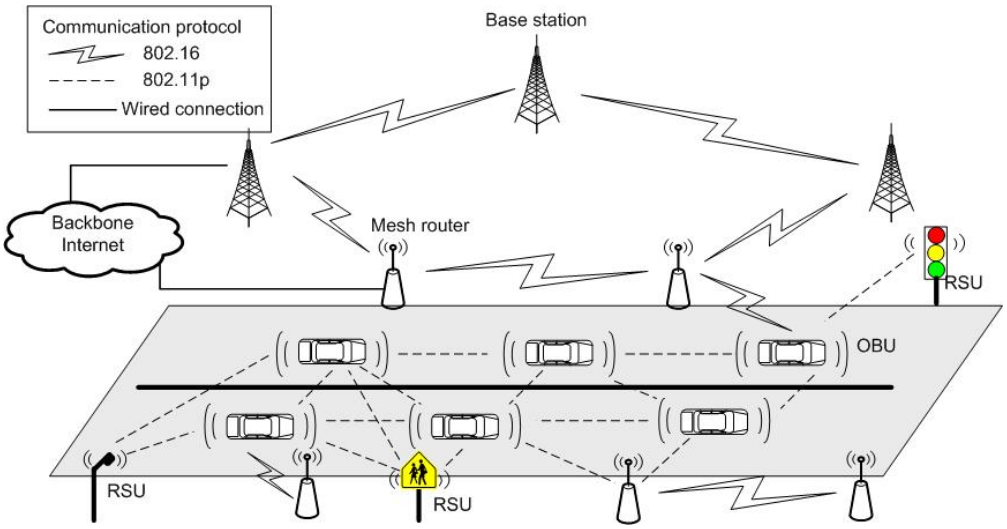

Figure 1-1. Proposed roadside vehicle network architecture

The second layer is composed of roadside WiMax mesh routers, which form a wireless multi-hop mesh network (mesh mode in WiMax) aiming to extend the wireless coverage and increase the network robustness and throughput. Some of these nodes are connected with the Internet either with wired backhaul or wireless connections with WiMax base stations.

The third layer includes vehicles, user devices and roadside units (RSU), which form an ad hoc network based on the IEEE 802.11p protocol. Note that an RSU and a mesh router can be integrated into a single physical device. The communication between mesh routers and between mesh routers and WiMax base stations adopts 802.16 protocols. For the passengers sitting inside of the vehicles, they can either connect with the Wi-Fi access point installed on top of their vehicle with 802.11g or they can communicate with the road-side mesh routers directly if the users' devices support 802.16 standards.

By communicating with the roadside mesh routers, vehicles and passengers can gain access to the Internet for a short moment when passing through any of the roadside mesh routers. Thus, the second layer mesh routers should be able to perform fast handoff in order to support basic Internet services such as e-mail and TCP applications. Note that the handoff process is expected to be predictive when the moving pattern and speed of the vehicle are given. In addition, the roadside mesh routers should work as gateways which also support the 802.11p protocol which transform the safety messages broadcasted by the vehicles into IP packets. With the second layer, the workload of the vehicles is reduced. Otherwise, the vehicles need to send multiple copies of safety messages in different formats: one to the other vehicles with 802.11p, and one to the base stations with 802.16e.

There are many security issues in this network architecture, such as the fast and private handoff process of mesh routers, the secure routing problems in the VANET and the mutual authentication between the mesh routers and the base stations; however, in this paper, we mainly discuss the secure communication issues in the third layer of this network architecture, communication between vehicles and roadside units (RSU).

Chapter 2
GSIS: A Secure and Anonymous Vehicular Communication Protocol

2.1 Overview of the GSIS Protocol

2.1.1 System Formulation

First, we assume there is no energy limit for vehicles and the vehicle's communication device is actively powered for any computation and communication task. Furthermore, the vehicles are equipped with reliable positioning system like GPS and they can get reliable and accurate time information, for example through a central satellite. Finally, we assume the highest security scenario in which adversaries are able to intercept, modify, retransmit and delete any message they desire in a VANET.

In our protocol, routine messages from the opposite direction of the road are ignored, while emergency messages from the opposite side will be processed.

In IVC applications, it is not necessary to achieve message confidentiality since everybody has the right to know the content of the traffic related messages. Thus, we choose to use digital signatures to sign every message sent by OBUs and RSUs. In this case, any receiver can verify the received messages and make certain of the integrity and authenticity of the messages with the non-repudiation property.

We divide our security design into two categories: communications between OBUs as well as between RSUs and OBUs, and consider the security solutions separately due to their respective requirements. The two categories are discussed in the following two subsections.

2.1.2 Communications between OBUs

The main challenge of the communications between OBUs lies in the contradiction between the design requirements of vehicle anonymity and identity traceability. Traditional public key encryption schemes are not suitable for signing the safety messages because identity information is included in the public key certificates. One solution is to use a list of anonymous certificates which do not contain

the identification information [RH2005]. All these anonymous certificates and the relationship with their owners are kept in the central Transportation Regulation Center (TRC) who could trace the real ID of the sender in their huge database. This approach can achieve conditional anonymity in a straightforward manner but at the expense of the high storage cost for a global certificate list for the authorities.

Therefore, we propose a security protocol by using a group signature scheme [CvH1991] to sign the messages sent by vehicles. As we mentioned, the main feature of a group signature scheme is that it provides for anonymity of the signers. The verifiers can judge whether the signer belongs to a group without knowing who the signer is in the group. However, in exceptional situations, the group manager is able to reveal the unique identity of the signature's originator. Therefore, the group signature technique provides a better way to meet the anonymity and traceability requirements. The group signature technique also reduces the workload of the public key verification and certificate path verification operations. In addition, the group signature scheme can satisfy other basic security requirements such as message integrity and source authentication.

A secure group signature has the following desirable properties [ACJT2000, W2004]:

1. Correctness: Signatures produced by a group member must be accepted by the verifier.
2. Unforgeability: Only a member in the group can sign messages on behalf of the group.
3. Anonymity: Given a valid signature, identifying the actual signer is computationally hard for normal members other than the group manager.
4. Unlinkability: Deciding whether two different valid signatures were computed by the same group member is computationally hard.
5. No Framing: Even if a subset of group members and group managers collude, they cannot sign on behalf of non-involved group members.
6. Traceability: The group manager is able to open a valid signature and identify the actual signer.

In addition to the basic properties mentioned above, some other features are also preferred in IVC application, which are listed as follows.

1. Role Separation: In the real world, it is preferred if the role of the group manager can be divided into a membership manager and a tracing manager. The membership manager

could be the TRC in charge of assigning private keys and group public keys to the vehicles, whereas the tracing mangers are law authorities in charge of revealing the real IDs of the message senders.

2. Group Membership Revocation: It is indispensable in the IVC system to have the ability to selectively revoke the group memberships of the compromised vehicles either through updating keys or releasing Certificate Revocation Lists (CRLs).

3. High Efficiency: The computational cost and the length of the signatures should be small in order to meet the stringent communication requirement in the IVC system.

Dozens of group signature schemes have been proposed since 1991. However, the security of some proposed group signature schemes are susceptible to attack. For instance, many ID-based group signature schemes, like those in [W2004, P2002, H2004], cannot meet the unlinkability requirement. In addition, some schemes, like those in [ZWW2003, W2004], are proven to be forgeable and traceable. Also, most of the reported group signature schemes either have too long a signature overhead or are not-revocable, or the roles of the group manager are indivisible. Thus, after thorough evaluation, we choose the Short Group Signature scheme that is proposed by Boneh et al. [BBS2004] which is considered to suit IVC applications best.

2.1.3 Communications between RSU and OBU

The main difference with respect to the security requirements between RSUs and OBUs is that RSUs do not need anonymity. Therefore, we propose to use the identity string of each RSU as the public key to sign the messages. With the ID-based signature scheme, the workload caused by the certificate management process can be significantly reduced, and the public key updating and revocation operation can be largely simplified. Among all the known ID-based signature schemes, the provably-secure ID-based signature scheme given by Barreto et al [BLMQ2005] is adopted in this study since the length of the signature is reduced due to bilinear pairing. Barreto's scheme is also among the most efficient ones regarding the verification algorithm which needs only 1 pairing computation.

2.1.4 System Notations

For ease of presentation, the notations used to describe the security protocol throughout the paper are listed as follows:

Table 2-1. Notations

Notations	Descriptions
TRC	Transportation Regulation Center
OBU	On Board Unit
RSU	Road Side Unit
IVC	inter-vehicular Communications
MM	Membership Manager
TM	Tracing Manager
gpk	Group Public Key
$gsk[i]$	Vehicle $i's$ private key
$gmsk_t$	TM's private key
$gmsk_m$	MM's private key
$\gamma \overset{R}{\leftarrow} Z$	Randomly select a number γ from set Z

2.2 Proposed Security Protocol between OBUs

2.2.1 Message Format

The packet format of the safety messages sent by OBU is defined as follows:

Table 2-2. Packet format for OBU messages

Group ID	Payload	Signature
4 bytes	100 bytes	184 bytes

Vehicles will be divided into several groups as will be discussed in section 2.4. Group ID is thus used to identify which group the vehicle belongs to. The message payload part should include position, current time, direction, speed, acceleration/deceleration, traffic events, etc., as well as the timestamp of when the message is generated. According to [DoT2006], the payload of a message is around 100 bytes. The timestamp is used to ensure that the message is freshly generated instead of a duplicate of a previous one. The timestamp is 8 bytes long, supporting resolution to milliseconds. If the vehicles are synchronized to within one millisecond, by a central satellite for example, then messages should be ignored if they arrive α time late, where α is the maximum message transmission time between vehicles. The last field is the signature of the OBU on the first two parts. The length of the signature will be discussed in the following paragraphs.

2.2.2 Security Protocol for OBU and OBU Communication

The security protocol is an elaboration of the short group signature scheme [BBS2004]. We divide the role of the group manager into MM and TM to better suit the real-world management architecture. MMs can be conceived as real-world Traffic Regulation Centers who are only responsible for assigning keying materials to vehicles during vehicle registration time. TMs are law authorities who are only responsible for revealing the identities of message senders. The protocol contains the following six phases. We will show how to incorporate the group signature scheme to the vehicular communications field.

2.2.2.1 System setup

The law authority who acts as TM first generates two multiplicative cyclic groups G_1 and G_2 with generators g_1 and g_2 respectively of the same prime order p. Let φ be a computable isomorphism from G_2 to G_1, with $\varphi(g_2) = g_1$; and $\hat{e}$ be a computable bilinear map, $\hat{e}: G_1 \times G_2 \to G_T$ with the following properties:

Bilinearity: $\forall (u,v) \in G_1 \times G_2$ and $\forall a,b \in Z_q$, $\hat{e}(u^a, v^b) = \hat{e}(u,v)^{ab}$;

Non-degeneracy: $\hat{e}(g_1, g_2) = g \neq 1_{G_T}$;

For security and efficiency's consideration, we recommend choosing the MNT curve [SB2006] with embedding degree k=6 and 163-bit prime order p.

The TM selects $h \overset{R}{\leftarrow} G_1 \setminus \{1_{G_1}\}$, $h_0 \overset{R}{\leftarrow} G_2 \setminus \{1_{G_2}\}$ and $\xi_1, \xi_2 \overset{R}{\leftarrow} Z_p^*$. It then sets $u, v \in G_1$ s.t. $u^{\xi_1} = v^{\xi_2} = h$ and sets $h_1, h_2 \in G_2$ such that $h_1 = h_0^{\xi_1}$, $h_2 = h_0^{\xi_2}$. Finally, TM keeps its private key as $gmsk_t = (\xi_1, \xi_2)$ and sends the system parameters

$$(u, v, h, h_0, h_1, h_2, G_1, G_2, G_T, g_1, g_2, g, p, \varphi, \hat{e})$$

to the TRC which works as the MM.

In the original short group signature scheme, TM randomly selects $\gamma \overset{R}{\leftarrow} Z_p^*$ and sets $w = P_{pub} = g_2^{\gamma}$ as a system parameter. Here, in our protocol, it is the MM who randomly chooses $\gamma \overset{R}{\leftarrow} Z_p^*$ and sets $w = P_{pub} = g_2^{\gamma}$, but not the TM. The private key for MM is $gmsk_m = (\gamma)$. MM also chooses a secure

cryptographic hash function $H:\{0,1\}^* \times G_1^5 \times G_T \times G_1^2 \to Z_p^*$. Finally, MM publishes the system parameters *param* and the group public key *gpk* as follows:

$$param = (u, v, h, h_0, h_1, h_2, G_1, G_2, G_T, g_1, g_2, g, p, \varphi, \hat{e}, H)$$

$$gpk = (g_1, g_2, g, w)$$

We separate the *gpk* from *param* because every time a node is revoked, *gpk* is updated while *param* remains the same. The revocation scheme can be found in section 2.2.2.6.

So far the system has been set up.

2.2.2.2 Membership registration

During the vehicle registration process, the MM generates a tuple (A_i, x_i) for each vehicle *i* as its private key *gsk*[*i*] using MM's secret key γ. This is done by the following procedure: MM first computes $x_i \overset{R}{\leftarrow} Z_p^*$, and then sets $A_i \leftarrow g_1^{1/(\gamma + x_i)}$. In the end, MM stores the information (A_i, x_i, ID_i) into its record, which completes the membership registration. The (A_i, x_i, ID_i) database is shared with TM. Note that only MM has the secret key γ, therefore, only MM but not TM, can assign private keys to vehicles. (A_i, x_i, ID_i) can come with the signature signed by MM with any public key based scheme in order to prevent TM from choosing its own γ and registering vehicles by itself illegally. With the signature signed by TM, vehicles can prove that their private keys are indeed from the MM later when necessary.

2.2.2.3 Signing

Given a safety message M , the vehicle signs the message before sending it out. With the group public key *gpk* , and the private key pair (A_i, x_i) , the signing procedure is composed of the following steps:

Select the exponents $\alpha, \beta \overset{R}{\leftarrow} Z_p^*$.

Compute an encryption of A_i , and (T_1, T_2, T_3) , where $T_1 \leftarrow u^{\alpha}$, $T_2 \leftarrow v^{\beta}$, $T_3 \leftarrow A_i h^{(\alpha+\beta)}$.

Compute $\delta_1 \leftarrow x_i \alpha$ and $\delta_2 \leftarrow x_i \beta$.

Randomly pick up blinding values $r_\alpha, r_\beta, r_{x_i}, r_{\delta_1}$, and r_{δ_2} from Z_p^*.

Compute R_1, R_2, R_3, R_4, R_5 as below:

$$R_1 \leftarrow u^{r_\alpha}$$

$$R_2 \leftarrow v^{r_\beta}$$

$$R_3 \leftarrow \hat{e}(T_3, g_2)^{r_{x_i}} \cdot \hat{e}(h, w)^{-r_\alpha - r_\beta} \cdot \hat{e}(h, g_2)^{-r_{\delta_1} - r_{\delta_2}}$$

$$R_4 \leftarrow T_1^{r_{x_i}} \cdot u^{-r_{\delta_1}}$$

$$R_5 \leftarrow T_2^{r_{x_i}} \cdot v^{-r_{\delta_2}} .$$

Obtain the challenge *c* using the above values and the *M*,

$$c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_p^* .$$

Compute $s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2}$, where:

$$s_\alpha = r_\alpha + c\alpha ,$$

$$s_\beta = r_\beta + c\beta ,$$

$$s_{x_i} = r_{x_i} + cx_i ,$$

$$s_{\delta_1} = r_{\delta_1} + c\delta_1 ,$$

$$s_{\delta_2} = r_{\delta_2} + c\delta_2$$

Finally, combine the above values to form the message signature σ

$$\sigma \leftarrow (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_{x_i}, s_{\delta_1}, s_{\delta_2})$$

Format the message according to Table 2-2 and send it out.

2.2.2.4 Verification

Once receiving a message, the receiver first checks if the time information in the message payload is within the allowable time window. If not, the message is ignored; otherwise the receiving vehicles will perform signature verification by first reconstructing ($\tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5$) and then re-computing the challenge $\tilde{c}$ according to the following formulae:

$$\tilde{R}_1 \leftarrow u^{s_\alpha} / T_1^c ,$$

$$\tilde{R}_2 \leftarrow u^{s_\beta} / T_2^c ,$$

$$\tilde{R}_3 \leftarrow \tilde{e}(T_3, g_2)^{s_{x_i}} \cdot \tilde{e}(h, w)^{-s_\alpha - s_\beta} \cdot \tilde{e}(h, g_2)^{-s_{\delta_1} - s_{\delta_2}} \cdot (\tilde{e}(T_3, w) / \tilde{e}(g_1, g_2))^c$$

$$\tilde{R}_4 \leftarrow T_1^{s_{x_i}} / u^{s_{\delta_1}} ,$$

$$\tilde{R}_5 \leftarrow T_2^{s_{x_i}} / v^{s_{\delta_2}}$$

Then, $\tilde{c}$ is re-computed from

$$\tilde{c} = H(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5).$$

The receiver finally checks to see if this value is the same as the c in the signature σ. If so, the receiver considers the message to be valid and unaltered from a trusted group member. If not, the receiver neglects the message.

2.2.2.5 Membership tracing

A membership tracing operation is performed when solving a dispute, where the real identity of the signature generator is desired. The TM first checks the validity of the signature, and then computes A_i as:

$$A_i \leftarrow T_3 / (T_1^{\xi_1} \cdot T_2^{\xi_2}) .$$

Once the authority has revealed the element A_i from the TM, it can look up the record (A_i, x_i, ID_i) which is shared with MM to find the corresponding identity ID_i. Note that only TM has the secret information of $gmsk_t = (\xi_1, \xi_2)$, therefore, only TM but not MM, can reveal vehicles' private keys and their real world identities.

2.2.2.6 Membership revocation

Once a vehicle is found to be compromised and its private keys and identities are identified by the law authority, this vehicle should be excluded from the system. Currently there are two approaches of revoking the compromised nodes. One is through group public key and private key updating to all un-revoked vehicles. Given the released private key pairs of the revoked vehicles in a Revocation List (RL), un-revoked nodes can locally update their private key pair $gsk[i]$ and the group public key gpk, whereas those revoked nodes cannot update their keying materials [BBS2004]. This scheme may introduce significant overhead since each vehicle has to change the public and private keys from time to time when there is a member get revoked. The other revoking mechanism is similar to the traditional CRL-based revocation scheme, called Verifier-Local Revocation (VLR) [BS2004], by

which only verifiers are involved in the revocation check up operation. The VLR scheme is efficient when the number of the revoked vehicles is small. However, since the signature verification time grows linearly with the number of revoked vehicles, the vehicle revocation verification procedure becomes particularly time-consuming and inefficient when a large number of revoked vehicles exist in the revocation list.

Based on the above concerns, we propose a hybrid membership revocation mechanism in order to achieve a graceful tradeoff which is a combination of the VLR scheme [BS2004] and the keying material updating scheme [BBS2004].

The basic idea of the proposed mechanism is that when the number of revoked vehicles in the RL is less than a pre-defined threshold value Tr, the VLR mechanism is adopted; otherwise, the first approach through updating the corresponding public keys and private key pairs is employed. In real world deployment, the threshold value Tr can be decided by a combination of several factors such as how often a node is revoked in real situations and how efficient the revocation verification algorithm is implemented by the hardware. The proposed revocation mechanism is further described as follows:

Case 1:

When $|RL| < Tr$, the MM publishes the Revocation List $RL = \{A_1, A_2, ...A_b\}$, where $b < Tr$. For a given group signature σ, the receiver first executes the signature verification operation, and then executes the revocation check, which is shown in Table 2-3.

Table 2-3. Revocation Verification Algorithm

Revocation Verification Algorithm:
Input: ($param, RL, \sigma$)
Output: *valid* or *invalid*
for $i \leftarrow 1$ to $|RL|$ do
  get one A_i from RL do
    if $\hat{e}(T_3 / A_i, h_0) = \hat{e}(T_1, h_1) \cdot \hat{e}(T_2, h_2)$, then
      return *invalid*
    end
end
return *valid*

$param = (u, v, h, h_0, h_1, h_2, G_1, G_2, G_T, g_1, g_2, g, p, \varphi, \hat{e}, H)$. If the returned value is *valid*, the signer of the group σ has not been revoked. However, if the returned value is *invalid*, then there exists some A_i being encoded in T_1, T_2, T_3, which can be checked by $\hat{e}(T_3 / A_i, h_0) = \hat{e}(T_1, h_1)\hat{e}(T_2, h_2)$ since

$$\begin{aligned}
& \hat{e}(T_3 / A_i, h_0) \\
= \ & \hat{e}(A_i h^{\alpha+\beta} / A_i, h_0) \\
= \ & \hat{e}(h^{\alpha+\beta}, h_0) = \hat{e}(h^{\alpha}, h_0)\hat{e}(h^{\beta}, h_0) \\
= \ & \hat{e}(u^{\alpha\xi_1}, h_0)\hat{e}(v^{\beta\xi_2}, h_0) \\
= \ & \hat{e}(u^{\alpha}, h_0^{\xi_1})\hat{e}(v^{\beta}, h_0^{\xi_2}) \\
= \ & \hat{e}(T_1, h_1)\hat{e}(T_2, h_2)
\end{aligned}$$

Case 2:

When $|RL| \geq Tr$, the MM sends all signers and verifiers in the system the revocation list which is represented as $RL = \{(A_1^*, x_1), ..., (A_b^*, x_b)\}$, where $b \geq Tr$. For each pair (A_i^*, x_i), $A_i^* \leftarrow g_2^{1/(\gamma + x_i)} \in G_2$. After receiving the revocation list RL, the group public key *gpk* and the new private keys can be easily updated by the non-revoked users [BBS2004].

Given the group public key $gpk = (g_1, g_2, g, w)$ and a revoked private key $(A_1^*, x_1) \in RL$, the new group public key can be constructed as

$$gpk_{new} = (\bar{g}_1, \bar{g}_2, \bar{g}, \bar{w})$$

where $\bar{g}_1 = \varphi(A_1^*)$, $\bar{g}_2 = A_1^*$, $\bar{g} = \hat{e}(\bar{g}_1, \bar{g}_2)$ and $\bar{w} = g_2 \cdot (A_1^*)^{-x_1}$.

Given a revoked private key $(A_1^*, x_1) \in RL$, the new private key for an unrevoked vehicle *i* can be constructed as $(\bar{A}_i, x_i)$, where $\bar{A}_i = \varphi(A_1^*)^{1/(x_i - x_1)} / A_i^{1/(x_i - x_1)}$.

The proofs of these two results can be found in [BBS2004]. Note that all keys in the RL can also be updated at once rather than updated one by one.

Synchronizing the key update for all the group members is difficult. If some cars have updated their keys, while some haven't, then those who don't have new keys cannot verify the messages signed by the new keys. Similarly, the message might be rejected if the sender doesn't have the latest keys. One possible solution is to add a version number to the group public keys and the message format and allow receivers to accept messages signed with the keys several (such as 2) versions

behind. Once a newer version of the group public key is found from other senders, the receiver will try to update its own group key as soon as possible. Note that this approach might reduce the security level since this extends the life time of the revoked malicious users, because they can still use their old group public keys to sign the messages for some time.

2.2.3 Message Length

The length of the OBU message can be expressed as:

$$L_{msg\_OBU} = L_{groupID} + L_{payload} + L_{sig} .$$

Since p is a 163-bit prime and the elements of G_1 are 164 bits long, $L_{sig} = 3 \times 164 + 6 \times 163 = 1470$ bits = 184 bytes. Thus L_{msg_OBU} = 4 + 100 + 184 = 288 bytes.

2.2.4 Analysis of the Membership Revocation and Tracing Efficiency

The efficiency of the membership revocation and tracing schemes is a key requirement to the success of any vehicular application since users are exposed to serious risks if malicious users conduct dangerous activity or adversaries impersonate a compromised yet legitimate group member. These behaviors have been seen to be common in our daily life. Thus, we need to improve the performance of membership revocation and tracing schemes as much as possible. In this subsection, we evaluate the efficiency of membership revocation and tracing schemes in the proposed protocol.

When a vehicle is compromised, the certificates that the vehicle owns need to be revoked in order to prevent the potential threats from happening. In [RH2005], a total of 43,800 anonymous certificates have to be put in the CRL once the vehicle is discovered compromised. The storage cost of the CRL is $43{,}800KB$ [1] per vehicle revoked. In our proposed membership revocation scheme, when the number of revoked nodes is less than a threshold Tr, an A_i that is 164 bits long is put in the revocation list for each revoked vehicle. When the number of revoked nodes is greater than Tr, a pair (A_i^*, x_i) needs to be put in the CRL when a vehicle is discovered compromised. Since the length of the element in G_2 is 490 bits long, the storage cost of the CRL in this case is 653 (which is 490+163) bits per vehicle. Therefore, we can see the size of the CRL is reduced, as compared with [RH2005]. The larger the number of revoked vehicle certificates in the CRL the more storage the proposed

[1] The size of a X.509 public key certificate is about 1KB [AF1999].

membership revocation scheme can save. This is extremely important since the CRL should be distributed to each OBU and RSU in order to avoid contacting a centralized CRL authority center. A reduction of the storage cost is also a reduction in bandwidth, which alleviates the transmission burden.

As discussed in Section 1.1, Raya, et al. in [RJPAH2006] proposed a way to reduce the storage cost of CRL by using a tamper-proof device to erase the stored anonymous certificates and stop signing messages automatically. This technique can be applied to our group signature based scheme as well. In this case, the distribution of CRL over the Internet can be saved for both schemes. However, once a node is discovered to be an attacker and needs to be revoked later, how to find where the attacker is and how to send the revoke message to the attacker is an open problem. In addition, if the attacker cuts the communication channel with the party who is responsible for releasing revoking messages, the attacker will not receive the revoke message and then can successfully refuse to revoke himself.

Furthermore, for identity tracing in exceptional cases, in [RH2005] the authority has to keep all the anonymous certificates for each vehicle in the administrative region, which results in a high storage cost of $43{,}800KB \times n$, where n is the total number of vehicles (probably millions of cars) in the system. The proposed membership tracing scheme in this study needs to maintain a table containing A_i^*, x_i and the corresponding real identity for each vehicle. Each entry in this table is 789 bits long if the identity of the vehicle is 136 bits (the VIN of a vehicle is a 17 character number made up of both alpha and numeric characters). Thus, the storage cost for the proposed scheme is $789 \times n$ *bits*, which is a considerable storage saving.

[RH2005] indeed provides a work around to reduce its high storage cost. It is mentioned in the paper that a master key can be used to generate all the anonymous keys. However, the paper did not discuss how the anonymous keys can be derived and whether the anonymous keys can be matched to the master key in an efficient way. Therefore, for the identity tracing process, the authority has to go through the whole master key set sequentially and regenerate the corresponding anonymous keys. In this way, this workaround has a less efficient searching process compared with the original anonymous key based tracing process even if the storage cost is reduced. Considering the high frequency of accidents happening everyday, it is important to maintain a low identity tracing overhead. We, therefore, have compared our storage cost with the storage cost of the approach discussed in the main part of [RH2005].

2.3 Proposed Protocol between OBUs and RSUs

2.3.1 Message Format

We define the packet format of the safety messages sent by RSUs as follows:

Table 2-4. Packet format for RSU messages

Type ID	Payload	Signature	ID String
2 bytes	100 bytes	41 bytes	40 byes

Type ID represents the type of message that is being sent. The first two parts are signed by RSU which become the 'Signature' part. The 'ID string' is a 40-byte-long string which works as the public key of the message sender. It must include the following information: the name of the road side device; the authorized geographical region to operate; the authorized message types such as 'maximum curve turning speed notification' or 'road under construction notification'. Again, the payload part includes an 8 byte timestamp information with a resolution of milliseconds that is used to deal with message replay attacks as briefly discussed in section 2.2.1. The size of the signature will be discussed later.

2.3.2 Security Protocol for RSU and OBU Communication

The proposed protocol contains the following phases, which can also be found in [BLMQ2005]. The parameters used below such as $G_1, G_2, G_T, \gamma, g, p, P_{pub}$ are the same as the ones used in the protocol for OBU to OBU communication.

2.3.2.1 Private key generation

There is a unique identity string assigned for each RSU according to its properties. The MM chooses two hash functions $H_1 : \{0,1\}^* \times G_1 \rightarrow Z_p^*$, and $H_2 : \{0,1\}^* \rightarrow Z_p^*$. The MM then computes the private key S_{ID_i} for each RSU as

$$S_{ID_i} \leftarrow g_1^{1/(\gamma + H_2(ID_i))}$$

and sends it to the RSU through a secure communication channel. H_1, H_2 are system parameters open to all the vehicles.

2.3.2.2 Signing

Before sending each safety message, RSU signs the message M with the procedure described below:

Pick a random value $x \overset{R}{\leftarrow} Z_p^*$.

Compute $r \leftarrow g^x \in G_T$.

Set $h_\sigma \leftarrow H_1(M, r) \in Z_p^*$.

Compute $S_\sigma \leftarrow S_{ID_i}^{x+h_\sigma} \in G_1$.

The signature σ is then the pair $(h_\sigma, S_\sigma) \in Z_p^* \times G_1$. Finally, formulate the message according to Table 2-4 and send it out.

2.3.2.3 Verification

Any vehicle receiving a message from a RSU will first guarantee that the senders are working under the authorized domain. The vehicle compares the physical location of the message sender with the location information in the RSU's identity string. Then, the vehicle compares the type ID in the received message with the properties stated in the identity string to see if this type of message is authenticated for this unit. For example, if the RSU designed for the curve speed warning is nonetheless sending a message like 'sharp turn ahead'. The vehicle should also check the timestamp of the message to make sure the message is freshly generated and is not a duplicate of a previously received message. If the message comes late, which is after the allowed time range, the message is ignored. Finally, the vehicle checks the validity of the message signature by computing

$$\tilde{h}_\sigma = H_1(M, \hat{e}(S_\sigma, g_2^{H_2(ID_i)} \cdot P_{pub}) g^{-h_\sigma})$$

to see if $\tilde{h}_\sigma = h_\sigma$, where h_σ is from the signature σ. If the equation holds, the vehicle accepts the message; otherwise, the vehicle drops it.

2.3.2.4 Membership revocation

Once an RSU is discovered compromised by the management authority, it should be revoked from the system. This could be done by the revocation scheme that is proposed in [BF2001]. The basic idea is that there is a 'current date' information in the RSU's public key. Normal RSUs will get a fresh

private key every day from the trusted authority. The revocation of an RSU is done simply by stopping issuing new private keys for it. The downside of the revocation scheme is that the revocation cannot be done in a real-time manner. To achieve real-time revocation, the public keys of revoked RSUs can always be put in the CRL. The receivers can check whether a certain RSU has been revoked or not by comparing its ID string with the ones in the CRL.

2.3.3 Message Length

The length of an RSU message can be calculated as:

$$L_{msg\_RSU} = L_{typeID} + L_{payload} + L_{sig} + L_{ID}$$

where the order p is 163 bits long and elements of G_1 are 164 bits long; thus the size of the signature σ is 41 bytes long. Finally, L_{msg_RSU} = 2 + 100 + 41 + 40 = 183 bytes.

2.3.4 Security Analysis

Using the provably secure ID-based signature scheme in [BLMQ2005] allows the RSU to sign an arbitrary number of messages by guaranteeing unforgeability, authentication, data integrity, and non-repudiation. We refer to [BLMQ2005] for more comprehensive security analysis of these security requirements. In this section, we analyze the proposed protocol in the aspects of (1) RSU replication attack prevention, and (2) replay attack prevention.

Prevention of RSU replication attack: The message from an RSU has an “ID” field which keeps the RSU's original physical location as well as the type of the 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 string. If the distance is farther than RSU's transmission range, the OBU ignores the message. Therefore by this means, the vehicles outside the original coverage range of the RSU can discover the replication attack. If the RSU is relocated by the malicious user in a place which is within the coverage range of the original legitimate RSU, the proposed scheme cannot detect such behavior. Therefore, a physical position detection device is needed to estimate the accuracy of the location information to assist guarding against this type of replica attack. This device may use a combination of GPS, differential correction, dead reckoning and other techniques as appropriate [IEEE1609.2-2006]. To verify the message, the OBU also needs to compare the type ID in the

received message with the corresponding property part specified in the ID string of the RSU. If the type ID cannot match the property, the message will be ignored.

Prevention of replay attack: With a replay attack, an adversary replays the intercepted message from an RSU in order to impersonate a legitimate RSU. It cannot work in the proposed protocol because of the time stamp check in the verification procedure.

2.3.5 Analysis of the Communication Overhead

By using an ID based signature scheme, the additional cryptographic load for a signed message is a result of the signature of the message and the public ID string, which is 41 + 40 = 81 bytes. For traditional PKI based signature schemes, the additional load is a result of the length of the public key certificate and the signature of the message. Among existing digital signature schemes such as RSA, DSA [USDoC], ECDSA [ANSI X9.62-2005], and BLS [BLS2001], the most appropriate candidate for the VANET application in terms of the packet overhead and the verification time is ECDSA. The minimum additional space caused by the use of 224-bit ECDSA is 181 bytes for each message, including the digital signature (which is 56 bytes [IEEE1609.2-2006]), and the public key certificate (which is 125 bytes [IEEE1609.2-2006]). Therefore, we can see there is an improvement on the communication overhead by deploying ID based signature schemes.

2.4 Group Division

It is desirable to divide the vehicles around the world into several groups for ease of management. There are many possible ways to do this. First, it is natural to divide groups according to places of registration. For example, all vehicles registered in Ontario, Canada could belong to the same group. They share the same group public key and their private keys are issued by the local transportation regulation centers in Ontario. The vehicles have to store the public key information of other provinces as well in order to verify the messages sent by the vehicles coming from other provinces.

Another possible division is manufacturer based. The vehicles produced by each manufacturer belong to the same group. Similarly, vehicles within communication range may come from different groups. Therefore, every vehicle is also installed with the group public keys of other manufacturers.

These two division methods are easy to understand and implement. However, one drawback is whenever the group public keys are updated, all vehicles around the world should be notified to update their local information of the updated group public keys.

To solve this problem, it is possible to divide the vehicles according to their current geographic region. For example, all the vehicles driving in Ontario, Canada belong to the same group. Then the revocation only needs to be done within a single group domain without affecting groups in other provinces. Each vehicle only has to store one public key, namely the one being used in this province. In this division, cars traveling across the border of a geographic group (such as the border of provinces or countries) need to update their group public key and private key information. This could be done by setting an RSU at the border. The RSU and the new coming vehicles establish a secure communication channel by using an existing mutual authentication and key agreement protocol such as Diffie-Hellman key exchange protocol secured by ID-based signature scheme and the group signature scheme. The RSU then could send the new keying materials to the new comer encrypted by the shared secret key.

2.5 Performance Evaluation

We conducted simulations using the ns-2 simulator [USC] to evaluate the performance and feasibility of the proposed GSIS security protocol. We use 802.11a to approximate the 802.11p protocol as was done in [RH2005]. In order to fully estimate the real-world road environment and vehicular traffic, two road scenarios are simulated. For the city environment, we use the mobility model generation tool developed by [SJ2004] which is specialized to generate realistic traffic scenario files for the ns-2 platform. This tool makes use of the publicly available TIGER (Topologically Integrated Geographic Encoding and Referencing) database from the U.S. Census Bureau, giving detailed street maps of the entire United States. The map we are using is shown below in Figure 2-1 which corresponds to the Afton Oaks area, Houston, TX. Vehicles are first scattered randomly on one intersection of the roads and repeatedly move towards another randomly selected intersection along the path constrained by the map. Vehicles are driving with a random speed with fluctuation range of 5 miles/hr according to the road speed limit that ranges from 35-75 miles/hr. The second road scenario we are simulating is a straight bi-directional six lane highway, where vehicles are driving with their speed within the range of 100 ± 10 km/hr. (Because routine safety messages from the opposite driving direction are ignored in our scheme, the actual scenario we simulated was a three-lane highway with a single driving direction. In a real world deployment, vehicles can distinguish those on the opposite of the road from the ‘direction’ information incorporated in safety messages.) RSUs are located every 500 meters along the road side sending messages every 300 ms. The simulation time is 30 s. (We have tested

longer simulation times such as 100 s. They return similar results to those of 30 s; we thus choose 30 s as the simulation time.)

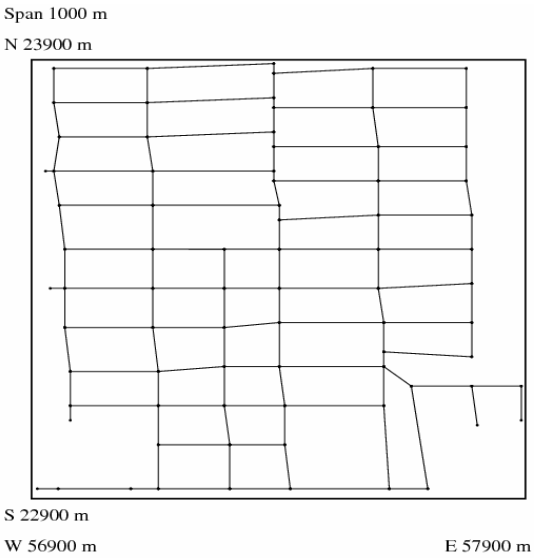

Figure 2-1. City map with span of 1000m

Other simulation parameters are listed in Table 2-5. Pause time is a special parameter in the ns-2 simulator that gives the waiting interval between the times when vehicles reach one destination and when they head for another destination. Buffer size is the length of the queue for vehicles to store incoming messages. The message loss ratio is related to the distribution of the arriving messages, the message arrival rate, the message processing time and the length of the queue. If we approximate message arrivals as being uniformly spaced, and note that the message processing time is usually higher than the message inter-arrival time, we see that the message loss ratio is independent of the length of the queue. Therefore, in our simulation we set the length of the queue to be 2 instead of a larger value in order to reduce the time each message waits in the queue. The cryptographic signing and verification delays are estimated based on the numbers provided by [S2007] with a 3 GHz Pentium IV system. All possible cryptographic time intervals are represented as equal time delays in the simulation.

Table 2-5. Simulation configurations

City simulation area	1000 m x 1000 m
Highway simulation area	2500 m x 30 m
Communication range	300 m
Message interval	300 ms
Simulation time	100 s
Channel bandwidth	6 Mb/s
Wireless communication protocol	802.11a
Pause time	0 s
Buffer size	2
Group Signature verification delay[2]	11 ms
Group Signature signing delay[2]	negligible
IBE verification delay[2]	5.7 ms
IBE signing delay[2]	0.6 ms

The performance metrics taken in the simulation are the average Message Delay (MD) and average Message Loss Ratio (MLR), and are expressed as follows:

$$avgMD = \frac{1}{N_D}\sum_{n\in D}\frac{1}{M_{sent\_n}\cdot K_n}\sum_{m=1}^{M_{sent\_n}}\sum_{k=1}^{K_n}(T_{sign}^{n\_m} + T_{transmission}^{n\_m\_k} + T_{verify}^{n\_m\_k}(L_{n\_m\_k}+1))$$

where D is the sampled simulation area in which the node's communication range has full coverage. N_D is the number of nodes in D; M_{sent_n} is the number of messages sent by node n; K_n is the number of adjacent vehicles within n's communication range; $T_{sign}^{n\_m}$ is the time used for n to sign message m; n_m_k represents the message m which is sent by n and received by k; $L_{n\_m\_k}$ is the length of the queue in k when message m sent by n arrives. So, we can see the metric of MD here is composed of all the periods from the moment that the data message is formed at the sender's side in the application layer to the moment that the receiving vehicle has the opportunity to react to the received data.

[2] As in [BBS2004], the verification process of the group signature includes 1 non-preprocessable pairing plus 4 non-preprocessable multi-exponentiations in G_1, plus 1 preprocessable multi-exponentiation in G_2, and 1 non-preprocessable multi-exponentiation in G_T. The signing process includes 8 precomputable exponentiations and therefore the time is neglected. The IBE verification contains 1 preprocessable pairing, and 1 non-preprocessable exponentiation in G_T based on the fact that the vehicle will receive many messages from one RSU. The IBE signing process contains 1 non-preprocessable exponentiation in G_1. The preprocessable multi-exponentiation in G_2 and the non-preprocessable multi-exponentiation in G_1 are estimated to be twice the time for 1 non-preprocessable multi-exponentiation in G_1. From [S2007], the time to do 1 non-preprocessable pairing is 6.2 ms and 4.5 ms for 1 preprocessable pairing. The time to do 1 point multiplication is 0.6 ms. The pairing in [S2007] is based on a 160-bit MNT curve with k=6.

$$avgMLR = \frac{1}{N_D}\sum_{n=1}^{N_D}\frac{M^n_{consumed}}{M^n_{arrived}}$$

where $M^n_{consumed}$ represents the number of messages consumed by node n in the application layer; $M^n_{arrived}$ represents the number of messages that are received by node n in the MAC layer. Here we only consider the message loss caused by delays due to the security protocol rather than the wireless transmission channel such as MAC layer contention. Note that the message will be lost and will not be consumed if the queue is full when the message arrival rate is higher than the message verification rate.

Two sets of experiments are conducted respectively to analyze the impacts of having different traffic loads and cryptographic algorithm processing speeds.

2.5.1 Impact of Traffic load

The vehicle density on the road is the major impact on system performance since it is related to the total number of messages received by each vehicle. Previous studies consider the effect brought by the actual vehicle density on the road such as $nodes/km$ or $nodes/km^2$. However they did not consider the varying relationship between the communication range and the actual vehicle density. According to [USDoT2006], the denser the traffic is, the shorter the communication range (or a smaller radiation power) should be to achieve an acceptable packet loss ratio. Therefore, the number of messages received by a certain vehicle within its communication range should be taken into account, when considering the impact on the system performance. Thus, this study takes the average number of neighboring vehicles within the communication range of each vehicle as the traffic load instead of the number of vehicles within one kilometer. Simulation results are shown in Figure 2-2 and Figure 2-3.

It can be seen that with the increase of traffic load (i.e., the number of vehicles within the communication range), MD is increasing but is smaller than the maximum allowable message end-to-end transmission latency which is 100 ms, as defined in [USDoT2006]. However, MLR increases dramatically when the traffic load is increasing. It is notable that a large number of messages are lost. This is because with the increase of the traffic load, the message arrival rate will be higher than the message consumption rate, which makes the receiver's buffer fill.

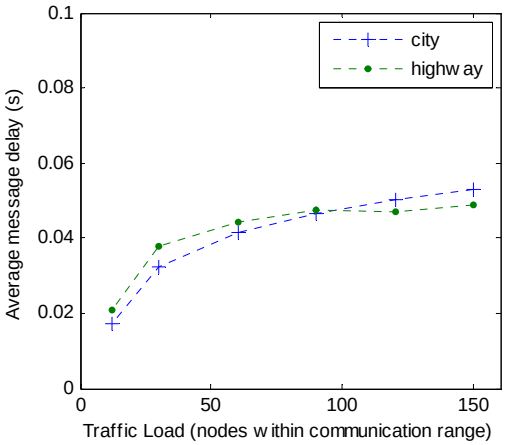

Figure 2-2. Impact of traffic load on the message end-to-end delay

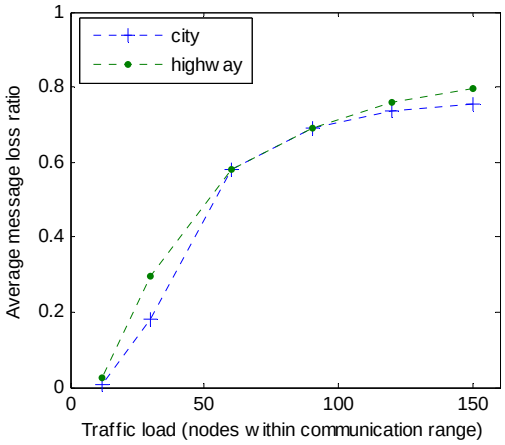

Figure 2-3. Impact of traffic load on the message loss ratio

2.5.2 Impact of Cryptographic Signature Verification Delay

Another important factor that determines the performance of a security protocol is its cryptographic efficiency. However, cryptographic algorithm processing speed is a non-determinate issue which depends highly on the level of the hardware. A quicker processor can achieve much higher processing speed. The group signature verification delay is estimated to be 11 ms in this study. Therefore, in this set of experiments, the group signature verification delay, which is the most important element in our security protocol, is varied from 1 ms to 13 ms. Since group signature verification delay is the bottleneck of all cryptographic operations, other cryptographic processing times are kept the same in

this set of experiments. Normal traffic load in the city and highway environment is simulated, where there are around 60 vehicles within communication range. Simulation results are shown in Figure 2-4 and Figure 2-5.

It can be seen that MD and MLR increase when the cryptographic operation cost becomes larger. Also, the MLR is significantly increased after the signature verification latency reaches a certain value when the incoming messages can not be verified since the message arrival rate is higher than the message verification rate. As shown in Figure 2-5, the MLR has reached 69% when the verification time is 13 ms even in normal traffic load. Reasonable performance can be achieved when the verification delay is below 3 ms.

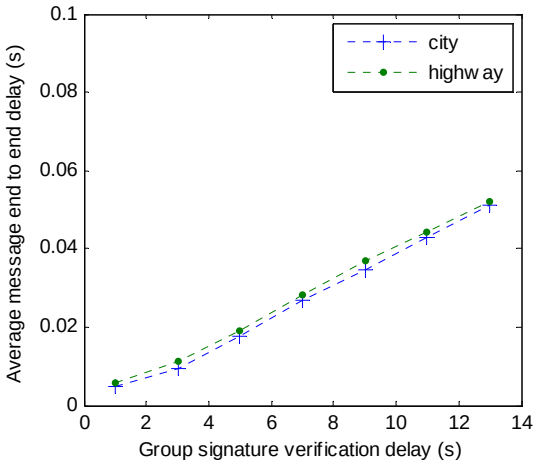

Figure 2-4. Impact of the signature verification latency on message end to end delay

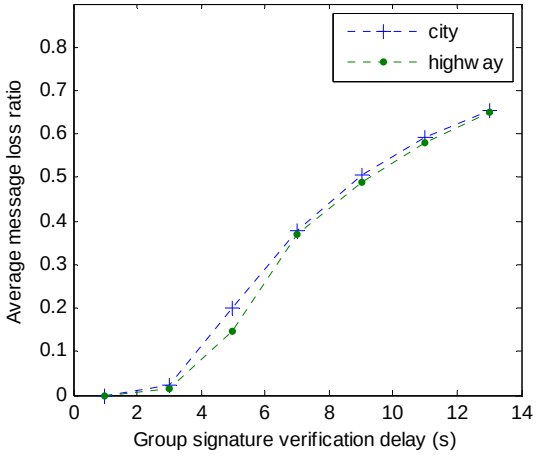

Figure 2-5. Impact of the signature verification latency on message loss ratio

In summary, the simulation results show that the proposed GSIS scheme can only meet the communication requirements under the condition that vehicles are equipped with fast computational devices and under a light traffic load scenario. Hardware implementation of the group signature is desired to achieve acceptable performances under all kinds of traffic loads, since the group signature verification time can, therefore, be reduced dramatically.

The GSIS scheme meets the following security requirements. It guarantees the message integrity. It provides anonymous vehicle authentication, while at the same time enables vehicles' identity tracing in exceptional cases. It deals with message replay attack. The GSIS scheme does not cover the message authenticity requirement because it does include a mechanism to detect the node sending valid but fake messages.

In addition, by observing contents of the traffic messages such as the position information, two messages can still be linked together by global observers based on the high frequency of sending messages. This is because the position of the vehicles won't change too much in 300 ms. This problem happens to PKI based security protocol as well. How to prevent this type of attack is left for future work.

In the next Chapter, an enhanced protocol called TSVC is proposed to improve the system performance in terms of the message end to end delay, and especially the message loss ratio, without influencing the security requirements. TSVC can also be applied to enhance the performance of the traditional PKI-based security protocols.

Chapter 3
Performance Enhancement for Secure Vehicular Communications

The studies on security and anonymity between OBUs and OBUs in VANETs can mainly be divided into two categories. The first is by way of the traditional PKI-based security architectures [RH2005, DoT2006], while the other is a group signature based security scheme as in the GSIS protocol. In both of these schemes, each message needs to be signed by the sender before it is sent, and the receiver needs to verify the message when it is received. According to DSRC [DoT_DSRC], a vehicle sends each message within a time interval of 100 ms to 300 ms. Generating a signature every 100 ms is not a problem for current hardware techniques. However, in the case that 50-120 cars are within the communication range, the receiver needs to verify around 500-1200 messages per second, which will lead to high computation burden to the receivers consuming these messages. Signing and verifying each message can certainly achieve secure communication; however, the corresponding cryptographic operations incur some computational overhead which makes them not scalable to the traffic density. Therefore, the verification algorithms are required to be very fast, such that the incoming messages can be processed with limited message loss. Otherwise, a large number of messages will be lost and sent in vain, as shown from the simulation result in section 2.5. Furthermore, in the traditional PKI-based security architecture, each packet must contain the public key of the sender and the corresponding certificate. The security overhead is usually longer than the message content and takes up a significant portion of the packet size.

In addition to achieving the satisfied security level and anonymity requirements, the design of a security protocol in VANETs must take certain issues into consideration, such as the signature overhead of each packet, packet sending rate, and the requirements for packet loss rate and message latency [DoT2006]. These issues are critical and must be well addressed before the developed scheme can be applied to practical vehicular communications.

To consider all the design requirements mentioned above without compromising the security and anonymity level, this chapter introduces a new enhanced security scheme, called TSVC (TESLA based Secure Vehicular Communication) protocol. Informed by the TESLA (Timed Efficient Stream Loss-tolerant Authentication) mechanism [PCTS2002], with the exception of the first message received from a certain OBU, the proposed protocol needs to do only symmetric MAC operations at the receiver, which is sufficient to authenticate the source of the message, instead of performing any

asymmetric verification whenever a message is received. The proposed TSVC scheme can be applied to both the reported PKI based security schemes as well as the GSIS security protocol. Similar to TESLA, in TSVC, only a short MAC tag is attached to each message. The extra message length and the bandwidth overhead due to the security mechanism can be reduced. Moreover, the enhanced protocol reduces the message loss ratio, which is almost independent of the traffic density.

We will show by extensive simulation that the proposed TSVC protocol significantly reduces message loss ratio compared to the existing PKI based security protocols as well as the GSIS protocol, especially when the traffic is becoming denser, while maintaining acceptable message latency. The TSVC scheme is feasible due to the unique features of VANETs, such as a fixed message release interval, and temporally stable geographical groups, which will be discussed later.

3.1 Related work

One work in the literature has aimed to reduce the overhead of the security protocol in a VANET, which is the aggregate signature based scheme [RAH2006]. In [RAH2006], the authors proposed a secure traffic aggregation scheme to minimize the communication overhead and initiate a tradeoff between security and efficiency. First, the map or the geographic region is dissected into predetermined small cells (such as every 400 meters along the road), each of which determines a dynamic vehicle group. A unique group leader is automatically elected as the one who is the closest to the geographic center of the cell. The dissemination of messages is delegated to each group leader who performs message aggregation for all the vehicles in the group and forwards the message to the neighbor groups. Although this scheme may yield low communication overhead, the vehicle closest to the center of a cell could change frequently, leading to a frequent update of the group leader of a cell (e.g. once every few seconds). The update of the group leader consumes all the effort such as the negotiation and reselection of the leader, and the aggregation of new signatures. Therefore, the approach leaves some space to be improved in terms of its efficiency and practical applicability.

Similar to [RAH2006], TSVC aims to reduce the overhead incurred in the security protocol without compromising the security performance. However, we approach the problem from a totally different angle. TSVC follows a more natural and dynamic approach to group the vehicles on the road; moreover, a group leader is not required, which largely reduces the resultant computation overhead in negotiating for a new group leader, identifying group members, or realizing the roles as relay nodes.

3.2 Preliminaries

Before the proposed security scheme is presented, some preliminaries throughout the protocol are introduced here.

3.2.1 One Way Hash Chain

One way hash chains were first proposed by Lamport in 1981 [L1981] for secure password authentication, and quickly became an important cryptographic primitive in many other applications, such as micropayment systems [RS1996], secure data forwarding in wireless ad hoc networks [HAKL2005], and stream data authentication [GM2001]

A one way hash chain is a repeated application of a hash function $H(x)$ to a randomly selected seed S, where $H(x)$ has the property that given x, it is easy to compute $H(x)$ and given $H(x)$, it is computationally hard to compute x. A hash chain is denoted as $h_1, h_2, ..., h_n$, where $h_1 = H(h_2)$, $h_{i-1} = H(h_i)$, $h_n = S$. h_1 is called the *tip* or the *commitment* of the chain. A node serving as the source can apply the hash chain by revealing the chain elements in the opposite order: first h_1, then $h_2, ...,$ then h_n. h_1 is usually signed using a normal signature scheme. By checking that $h_i = H^{j-i}(h_j)$, where $i < j$, the receiver can determine that h_j is indeed an element in the chain sent by the same source as h_1.

3.2.2 TESLA authentication scheme

TESLA was first proposed by A. Perrig et al. [PCTS2002], which is an efficient and message-loss tolerant protocol for broadcast authentication with low communication and computation overhead. It is widely used in the area of sensor networks [PSWCT2002]. With TESLA, the elements in a one way hash chain are used as cryptographic keys in the MAC operations. A sender sends the key disclosure schedule information to the receivers, which includes a time interval schedule to disclose one-way hash chain elements, a key disclosure delay, and a key commitment. This information, as well as the tip, is signed with any conventional digital signature scheme, such as RSA, or the ElGamal signature scheme. Then, for the following messages, the sender attaches a MAC tag to each message M_i. This MAC tag is derived using the next corresponding MAC key in the hash chain. Each key corresponds to a certain time interval. The key remains secret for the next (d – 1) intervals, where d is the key disclosure delay. Thus, the messages sent in interval j will disclose the keys for interval *(j*

– *d)*. So, the broadcast message M_i sent in interval *j* is encapsulated in packet P_i, which is expressed as $M_i \| MAC_{h_j}(M_i) \| h_{j-d}$, where h_j is the MAC key in interval *j*. Thus, message M_i can be authenticated after a time delay, once the key h_j is released in interval (*j* + *d)*. By checking the validity of the MAC tag of a message, one can make sure that the message originated from the same source as the previous message.

TESLA scheme requires only loose synchronization among the nodes. The disadvantage of TESLA is the delayed message authentication.

3.3 TSVC in a nutshell

We first assume that each vehicle is able to estimate the message transmission delay through the traffic density information. We also assume all the vehicles have synchronized clocks to millisecond accuracy, for example, through a central satellite. We divide the message authentication into two categories based on the message type: routine messages and emergency messages, where the former one obviously dominates the total traffic amount while the latter one is much less frequent.

The general idea of the proposed approach on performance enhancement for the routine traffic related messages is described as follows. Each sender generates a hash chain in advance. The elements of this chain are used as MAC keys. A signature is produced for the first message with a conventional public key signature scheme. For the following messages, on the other hand, the MAC tag of each message is computed with the corresponding key in the hash chain, which is disclosed after a short delay. Messages can be authenticated when the MAC keys are released. Based on the expected transmission delay of each message along with the serial number of the key used in a hash chain and the pre-shared key release schedule information, the receiver can check whether or not the next hash key used to generate the MAC tag of the received message has been released. If so, the message should be discarded to prevent a message forgery attack.

Emergency messages such as ‘accident ahead’ or ‘emergency braking’ that are sent with a much lower frequency are processed in a higher priority. Therefore, emergency messages sending from both directions of the roads are signed and verified with normal signature schemes such as RSA, from which the best security assurance, a constant delay and low loss ratio can be achieved.

The detailed security protocol is given in the next section.

3.4 Proposed TSVC Protocol

3.4.1 Vehicle Group Formation

One of the unique features of VANETs is that the vehicles driving on the highway maintain a temporally stable relative distance with the neighboring vehicles. Since the communication range is typically 250 m-1000 m, and as we stated in section 2.1.1, routine traffic messages coming from the other direction of the road are not taken into consideration, this neighborhood relationship could last from several seconds to several minutes according to the driving speed of an individual car. By taking advantage of this property, we can group the cars according to their physical locations.

For a specific vehicle V , all the other vehicles that are within its one-hop communication range are defined as in the same group as v as shown in Figure 3-1. Vehicle N_1 , N_2 and V form a group centered by vehicle V . Obviously a car can belong to many different groups. The group relationship is dynamic and is updated when any other car comes into the communication range or any group member leaves the group. The majority of the group members remain stable for a relatively long time.

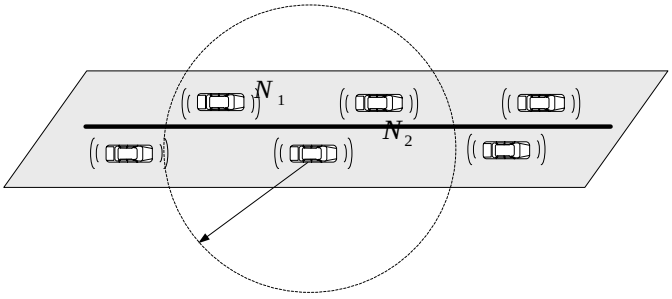

Figure 3-1. Dynamic virtual vehicle group formation

3.4.2 TSVC protocol

As mentioned above, the TSVC protocol can be applied to both of the two main streams of the existed security protocols. For ease of explanation, we first show how to combine the TSVC scheme with the anonymous PKI-based security schemes as discussed in [RH2005], which we call the TSVC-enhanced PKI-based security scheme. The combination of TSVC and GSIS will be discussed in section 3.5.4.

Let all the vehicles be installed with a list of anonymous public key pairs $< PK_i, SK_i >$ and the corresponding anonymous certificates $Cert_i$ in the vehicle registration phase or annual check-up time.

Each pair of keys has a short life time, e.g., a few minutes. Each vehicle has to generate a hash chain $h_1, h_2, ..., h_n$ initiated from a random seed *S*, where $h_n = S$, and $h_i = H^{j-i}(h_j)$ with $i < j$. Each element in the hash chain is used to generate one MAC code for each message. Hash keys will be released after a short delay δ which we call the key disclosure delay. For simplicity, we assume the number of messages each MAC key works on is 1; thus, each hash element will generate one MAC code for one message. Also, we set the time interval in the TESLA scheme as the packet release interval which means one packet, and its corresponding key, are transmitted during each time interval by each OBU.

The length of the hash chain can be predetermined according to the life time of each anonymous certificate and the message sending interval. Once the anonymous public key pairs are updated, a new chain is initiated and comes into use. Note that all the hash chains can be initialized in advance before going into function to reduce system operation delay. Let the routine safety messages to be sent by a vehicle be denoted as $M_1, M_2, ..., M_k$. Let messages be launched with a fixed interval of 300ms. The message authentication process is shown below in Figure 3-2, where P_i represents packet i.

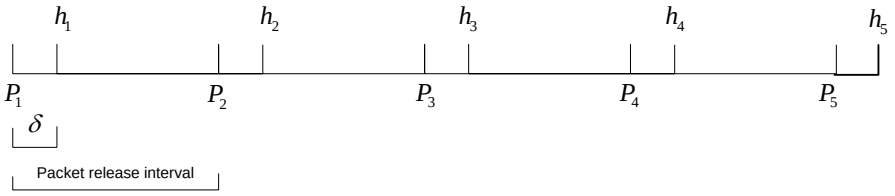

Figure 3-2. Relationship between a hash chain and the corresponding packets

There are two categories of packets in the TSVC scheme. The first category are the data packets which are used for sending data information while the second category are the key release packets (KRP), denoted as Kr_P_i, which are used for releasing the MAC keys. The messages are released every 100 ms ~ 300 ms. Considering the packet transmission time and the cryptographic delays, in order to meet the maximum allowed message latency that is 100 ms [USDoT2006], instead of combining the data and keys in the same packet, we divide them into two packets. Each KRP is disclosed a fixed time δ after the previous data packet is released.

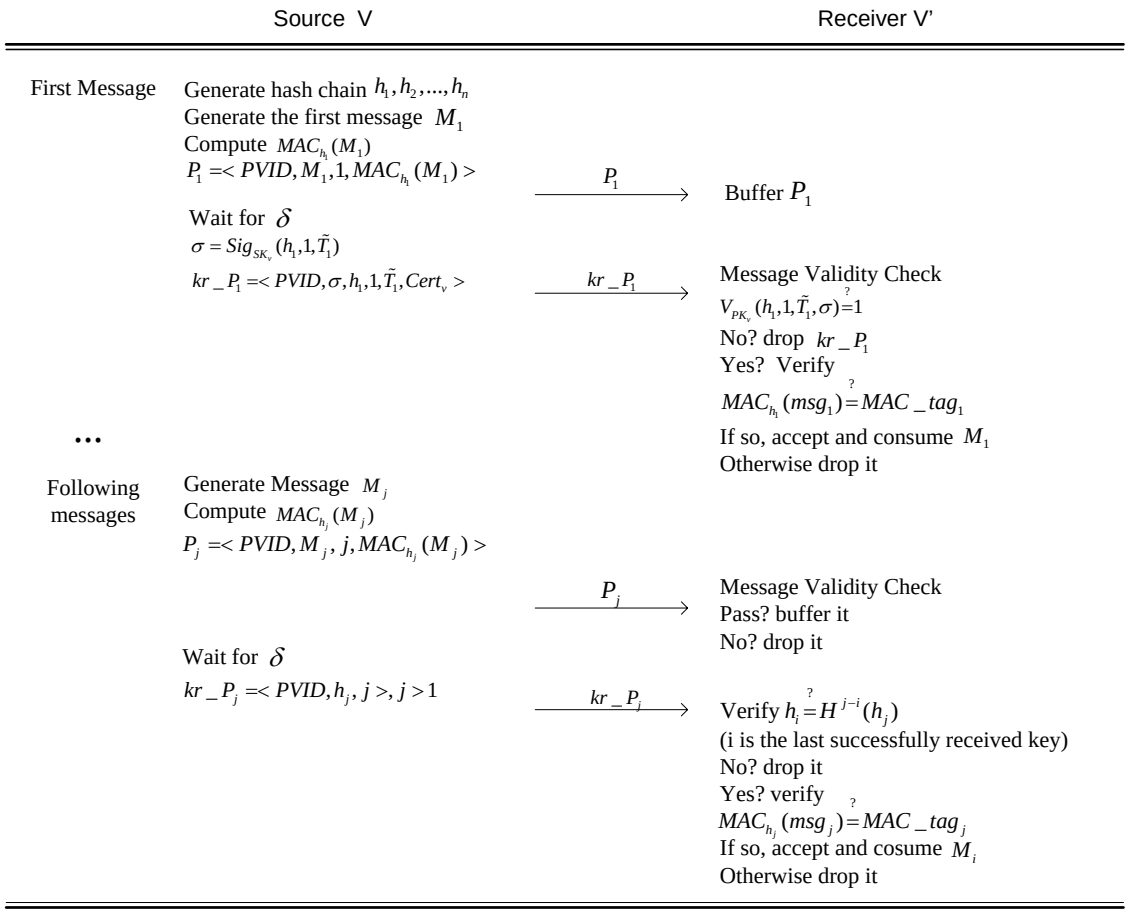

Figure 3-3. The diagram of the TSVC protocol

The proposed security protocol is illustrated in Figure 3-3. Each sender *v* generates the MAC tag of M_j using h_j as the MAC key. The resulting data packets have the following format:

$$P_j =< PVID, M_j, index, MAC_{h_j}(M_j) >,\ j \geq 1$$

where *PVID* is the pseudo ID of vehicle *v*, which is kept in accordance with the IDs that are being used in the current public key certificate $Cert_v$; M_j is safety message *j*; *index* is the ordered packet number: i.e. 1 in P_1. Note that the timestamp when the sender sends P_j is included in M_j. When the first packet is received from a certain vehicle, the receivers create an entry for source *v* in their local data base in the form of

$$ENTRY_v = (PVID,\ msg,\ packet\_index,\ MAC\_tag,\ hash\_key,\ lifetime)$$

to synchronize the later packets coming from the same source, where *lifetime* is the expiration time of a certain message that can be computed from the time stamp information in the message payload part. The receivers fill in the $PVID$, msg, $packet\_index$, MAC_tag, and the *lifetime* fields and leave the $hash\_key$ part blank. The receivers cannot verify the first data packet until they receive the first KRP.

After the first data packet is sent, the sender v prepares the first KRP by signing the tip of the hash chain h_1 using a traditional public key based signature scheme. The first key release packet is signed by the traditional PKI scheme and has the following format:

$$kr\_P_1 =< PVID, Sig_{SK_v}(h_1, index, \tilde{T}_1), h_1, index, \tilde{T}_1, Cert_v >$$

where h_1 is the key used to generate the MAC tag of the first message M_1, $Cert_v$ is the currently used anonymous certificate, *index* is the ordered number of the hash chain element: i.e. 1 in kr_P_1, and $\tilde{T}_1$ is the time when kr_P_1 is sent. $\tilde{T}_1$ is an 8-byte variable with a resolution of milliseconds. Given this time information of when this first hash key is released and the fixed key released delay, the receivers are able to know the release time of the following hash keys. kr_P_1 will be released δ time later than P_1.

Once kr_P_1 arrives, the receivers perform the following verification:

$$Ver_{PK_v}(h_1, index, \tilde{T}, Sig_{SK_v}(h_1, index, \tilde{T}_1)) \stackrel{?}{=} 1, \text{ where } index = 1$$

$$MAC_{h_1}(msg_1) \stackrel{?}{=} MAC\_tag_1$$

where msg_1 and MAC_tag_1 are the previously stored values.

If the above verification fails, the packet is dropped; otherwise, the receivers fill in the $hash\_key$ field in the corresponding entry and start consuming M_1.

The following KRPs have the following format:

$$kr\_P_j =< PVID, h_j, index = j >, j > 1$$

We can see that the following KRPs are not signed. Note that all the KRPs are released δ time later than the previous data packets.

When receiving data packet P_j, when j > 1, the receivers simply update the corresponding entry for vehicle v without trying to verify the messages. As soon as the next key release packet kr_P_j arrives, the receivers start to verify the previous data packet. Before doing that, the receivers will first find the corresponding entry for vehicle v and check the legitimacy of the hash chain, which is done by checking if $H(h_j) = h_{j-1}$, where h_{j-1} is the previously stored $hash\_key$ field in the entry. If the equation does not hold, the packet kr_P_j is dropped; otherwise, the receivers start to validate the data packet P_j by checking

$$MAC_{h_j}(msg_j) \stackrel{?}{=} MAC\_tag_j .$$

Again msg_j and MAC_tag_j are the previously stored values in the database. If the verification succeeds, M_j is accepted and consumed by the application layer, and the $ENTRY_v$ is updated by filling in the field $hash\_key$ with h_j; if the verification fails, P_j is dropped.

In summary, the proposed protocol can achieve the same guarantee for message integrity, anonymity, and authenticity as the traditional PKI based schemes do. In spite of the anonymity for the public receivers, the protocol can well maintain a conditional traceability property for authorities such as police, because all the accepted messages can be tied uniquely to an anonymous public key and the certificate of its sender. Thus, by checking this unique public key certificate, the authority can trace the unique real-world identity of the message sender as can be done in the traditional PKI based schemes.

3.4.3 Security requirement and Key Release Delay δ

The security requirement to prevent message forgery attacks for the proposed scheme is that the key release waiting time should be longer than the time for a message to travel from the source to all recipients. If any receiver r can receive the released key before the original data packet arrives at another receiver $\tilde{r}$, then receiver r, who holds the key, can forge a message by generating a valid MAC tag to this message and sending the tagged message to $\tilde{r}$. Note that this forged message can pass $\tilde{r}$'s verification. This situation can be avoided by choosing the key release delay δ properly. In the vehicular communications with IEEE 802.11p, since the longest transmission range is about 1000 m, δ should be slightly greater than the time for a message to travel for 1000 m in the wireless channel. In [DoT2006], the communication latency is identified as about 10 ms. In our scheme,

therefore, δ is set to be 70 ms, which is approximately several times the communication latency for the concern to achieve a higher level of security and at the same time to meet the requirement of the maximum allowable message latency. (This number is derived from the simulation results in section 3.6.2 where the biggest message end to end delay is measured 30 ms higher than the key release delay). This figure will be verified through simulation as presented in section 3.6.

Before performing a normal message authentication process as discussed above, the validity of the messages needs to be checked to see if the security requirement can be met. This means the receiver has to know which interval the data packet belongs to and whether the corresponding key has been released already. This can be derived from the pre-shared key-disclosure schedule information and the index of the hash key. If yes, the packet is dropped without trying to authenticate it. The receivers have no idea of the validity of the first data packet. When kr_P_1 arrives is checked valid, the receivers can trace back to see if P_1 was received δ time earlier than kr_P_1. If not, P_1 should be deleted immediately.

Note that due to the stringent time requirement of the real-time applications in VANETs, late or outdated messages should be dropped. Therefore, if a message arrives after the maximum allowable latency such as the human's maximum reaction time, this message should be dropped without putting it into the buffer.

3.5 Protocol Analysis

3.5.1 Group Membership Fluctuation

We have assumed that the neighborhood of each car is not fluctuating seriously, but memberships are occasionally subject to fluctuations. Once car *v* leaves the transmission range of *v'*, *v'* keeps the information record of *v* for a short while in order to avoid frequent update of the group members. When car *v* joins the group of *v'*, *v* needs to catch up with the previously released hash chain MAC keys sent by *v'*. This can be achieved by checking if a new routine safety message is coming from an unknown party. If a newcomer joins, *v'* needs to rebroadcast the authenticated tip of the hash chain kr_P_1, from which the newcomer *v* can verify the MAC key h_1. The source *v'* continues to send normal data and KRPs as usual. The new comer *v* will catch up with the new messages by applying the hash function multiple times until the first verified hash key is met. Note that given the time stamp information in kr_P_1 and the indexes of the following hash keys, the new comer is able to

compute the scheduling information of the following hash keys and therefore can verify their legitimacy to defend against message forgery attacks. After this process, the later communications between *v* and *v'* are identical to the normal protocols.

3.5.2 The Capability to Deal with Message Loss

Wireless communication channels are inherently lossy. Since TSVC is based on TESLA, which is packet-loss tolerant, our scheme is also packet-loss tolerant.

In the case that a data packet is lost, no further action will be taken.

On the other hand, if the KRP kr_P_i, ($i > 1$) is lost, the legitimacy of the previous message can still be verified upon receiving kr_P_j with $j > i$. The broken hash chain can be connected by applying the hash function $j - i$ times and checking if $H^{j-i}(h_j) = h_i$. If so, the newly arrived hash value h_j is acceptable. However, in the case where multiple continuous packets are lost such that the time to wait for the new key release packet is longer than the maximum tolerable message delay, M_i is neglected.

If kr_P_1 is lost, this means the receiver does not receive the signed tip of the hash chain. This is similar to the case when a new comer comes into the communication range in the middle of the hash chain. The receiver who has lost kr_P_1 will request for another signed tip from the source.

So in all cases, the subsequent messages can still be authenticated when new data packets and key release packets arrive. In a manner similar to that discussed in 3.5.1, the receivers are able to defend against message forgery attacks even if some of the messages are lost.

3.5.3 Bandwidth Efficiency

In this section, we would like to analyze the reduction of bandwidth consumption due to the decrease of the average packet size compared with regular public key based schemes.

As discussed in Section 2.3.5, ECDSA is adopted by [IEEE1609.2-2006]. The minimum additional space caused by the use of 224-bit ECDSA is 181 bytes for each message, including a 56-byte digital signature [IEEE1609.2-2006], and a 125-byte public key certificate [IEEE1609.2-2006]. Thus, the total length of a traditional signed packet with certificate is around 289 bytes including the message payload which is around 100 bytes [DoT2006], and *PVID* which is taken as 8 bytes in this study.

To evaluate the average packet size in our scheme, we assume that the KRPs are signed with the ECDSA scheme. Similarly, whenever a new group member is found in the communication range, the signed tip of the hash chain will be sent which is 219 bytes as computed below. Suppose the life time of an anonymous certificate is 10 minutes, routine traffic messages are sent every 300 ms, and a new group member will be encountered every 10 secs. The following comparisons can be made.

For the traditional PKI based scheme, the total information that needs to be transmitted in 10 minutes for each vehicle is:

$L_{P\_cert} \times Num_{Total}$ = 289*2000= 578,000 bytes

For the TSVC scheme, the length of a data packet is:

$$L_{p_j} = L_{PVID} + L_M + L_{index} + L_{MAC} = 8 + 100 + 2 + 20 = 130 \text{ bytes}, \quad j \geq 1$$

where *index* is taken as 2 bytes.

The length of a KRP is

$$L_{kr\_P_1} = L_{PVID} + L_h + L_{index} + L_T + L_\sigma + L_{Cert} = 8 + 20 + 2 + 8 + 56 + 125 = 219 \text{ bytes}$$

$$L_{kr\_p_j} = L_{PVID} + L_h + L_{index} = 8 + 20 + 2 = 30 \text{ bytes}, \ (j > 1)$$

Therefore, the total information that needs to be transmitted in 10 minutes for each vehicle in our scheme is:

$$\begin{aligned} & L_{kr\_P_1} \times Num_{Cert} + L_{P_j} \times Num_{Total} + L_{kr\_p_j (j>1)} \times Num_{Total} \\ = \ & 219 \times 60 + 130 \times 2000 + 30 \times 2000 \\ = \ & 333{,}140 \text{ bytes} \end{aligned}$$

which can be seen to have improved the bandwidth usage as compared to the traditional PKI based scheme.

3.5.4 Combination of TSVC and GSIS

TSVC can also be applied to the GSIS protocol with some tiny modifications. In the TSVC-enhanced PKI-based security scheme, the *PVID* part is incorporated in the vehicle's anonymous certificates. It comes into effect for several minutes and will be updated once the certificate expires. Based on this *PVID* information, we are able to chain the messages sent by the same source together using the hash key chain. In the case of the GSIS protocol, since the message signed by group signature scheme does

not contain any identity information of the source, we need to generate a list of pseudo IDs for each vehicle. These pseudo IDs are also short-lived with a lifetime of several minutes. For each vehicle, each hash key chain corresponds to one pseudo ID and will be reinitialized whenever a new pseudo ID takes effect. All the other parts of the enhanced GSIS protocol remain the same with the enhanced PKI-based protocol except that the first key release packet is now signed and verified by the group signature scheme as we discussed in section 2.2.2. Therefore, by changing the length of the signature to 184 bytes, removing the certificate, and following the computation in section 3.5.3, the total information that needs to be transmitted for TSVC-enhanced GSIS in 10 minutes for each vehicle is 333,320 bytes. This result is similar to that of the TSVC-enhanced PKI-based protocol.

Note that the anonymity of the traditional PKI based protocol is based on short-lived anonymous certificates and the TSVC protocol takes advantage of this by chaining the messages sent by the same source together in a short period. However, by artificially adding a short-lived PVID, the unlinkability or the anonymity of the TSVC-enhanced GSIS protocol is weakened as compared with the original GSIS protocol in which no two messages can be determined to have been sent from the same source. However, the new GSIS protocol can still maintain the same level of anonymity as the PKI based security protocols and is sufficient for real-world anonymity requirements. In addition, not only does the TSVC-enhanced GSIS improve the system performance in terms of computation efficiency as will be shown in section 3.6, it also retains all the other advantages over the PKI security scheme such as the low overhead of the membership identity management and low storage cost for CRLs.

3.6 Performance Evaluation

Again, simulation is conducted to measure the four discussed protocols: the traditional PKI based scheme, the GSIS protocol, and their corresponding TSVC-enhanced protocols. We used the ns-2 simulator with the same performance metrics and the same road scenarios as defined in section 2.4. In this part, we are interested in comparing the MD and MLR between the traditional PKI-based protocol and its TSVC enhanced version as well as between the GSIS protocol and its TSVC enhanced version. Some additional simulation configurations are shown in Table 3-1. The other parameters are the same as defined in section 2.4.

Table 3-1. Some simulation configurations

ECDSA signing delay[3]	2.92 ms
ECDSA verification delay[3]	3.87 ms
MAC generation & verification delay	0.5 ms

Before starting the experiment, a small simulation was run to test the time that is needed to transmit a packet over the wireless channel in the highway scenario. Because most of the delay is incurred by channel contention, the longest transmission time happens when the density of the traffic is the highest. So in this experiment, we simulate the most crowded traffic scenario in which the communication range is set as 300 m, and the inter-vehicular distance is set as 5 m. Here, the time we considered includes the period from when the packet is ready to be put in the output buffer until it is received by the receiver. We extracted the simulation results of two cars, which are 300 meters away. From the simulation result, the average delay for all the messages sent is 6.467 ms. This simulation is used to decide the Key Release Delay δ as discussed before. Therefore, the Key Release Delay δ for the later experiments is conservatively set as 70 ms which is much bigger than the actual delay and thus ensures a high level of security.

We then conducted two sets of experiments. The first set investigates the impact of the vehicles' moving speed in a highway scenario, whereas the second set investigates the impact of vehicles' density in both highway and city scenarios.

3.6.1 Impact of Vehicle Moving Speed

In the first set of experiments, V (the average velocity of the vehicles) is changed from 10 m/s-40 m/s (36 km/hr-144 km/hr). The traffic load simulated is 60 and the initial inter-vehicle distance is 30 meters. The simulation results on the MD and MLR are shown in Figure 3-4 and Figure 3-5. In all four schemes, the variation of speed does not cause much influence on MD or MLR. But the proposed TSVC enhanced schemes yield larger MD which is slightly higher than the key release delay δ. However, when it comes to MLR, the two TSVC enhanced protocols reduce the message loss ratio compared with the original PKI and GSIS scheme under this normal traffic density. Another result is that the TSVC enhanced GSIS always has higher MLR and MD than the TSVC enhanced

[3] The 224-bit ECDSA cryptographic delays are quoted from the documentation of the MIRACL cryptographic lib [SS] with a 3GHz Pentium IV system. These values and the values that were used to compute the timings of the group signature scheme are estimated from the same MIRACL lib with the same system processing power. Therefore, the values from Table 2-5 and Table 3-1 are comparable.

PKI scheme; this is likely due to the longer signature verification delay, even if a signature verification is only performed for the first message.

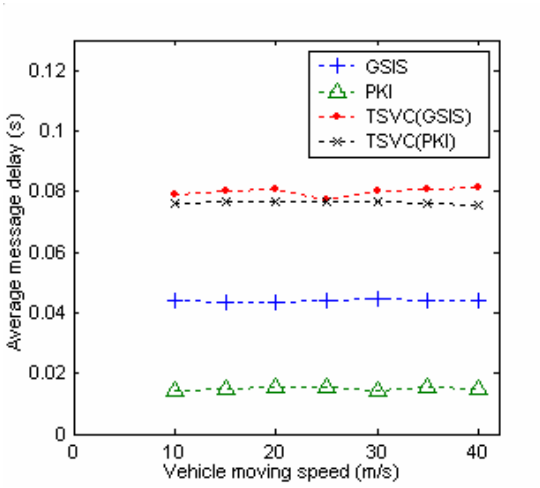

Figure 3-4. Impact of vehicles' moving speed on message end to end delay in highway scenario

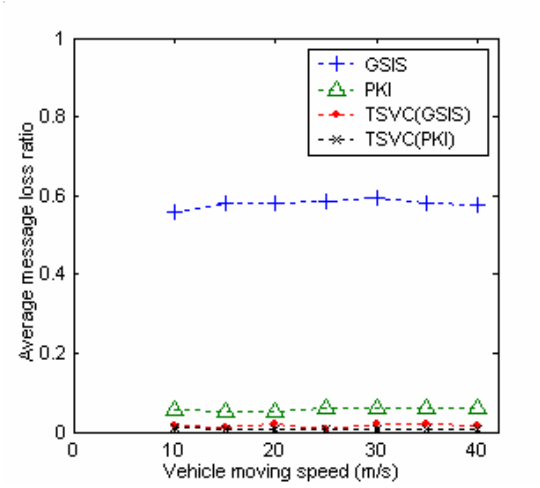

Figure 3-5. Impact of vehicles' moving speed on message loss ratio in highway scenario

3.6.2 Impact of Vehicle Density

In the second set of experiments, the impact of the node density for both highway and city traffic is studied. We set the reference speed as 100 ± 10 km/hr for the highway scenario and the same speed setting for the city scenario as was given in section 2.5.

In Figure 3-6 and Figure 3-8, it is shown that the message end-to-end delay of TSVC enhanced protocols is again higher than the key-release delay and therefore is much higher than the original schemes. In the city scenario, however, there are unexpected higher delays when the traffic load is greater than 120. We believe this high delay is caused by the irregularities of the vehicles' driving pattern in the city environment. Unlike in the highway where vehicles are driving on the same line, the vehicles in city environment may take turns all the time which in turn cause frequent changes to the group memberships. This indicates that more signed tips have to be sent, which therefore take a longer time to verify. This effect is more obvious when the traffic load is increasing. Another result is that delays in all situations are lower than 100 ms. This is because this 70 ms key release delay was informed by our simulation results. We aimed to make the overall delay lower than the maximum allowable latency while at the same time ensuring the security of the protocol.

From Figure 3-7 and Figure 3-9 we can see that both the PKI and GSIS schemes suffer a huge message-loss ratio especially when the traffic becomes dense, which is out of the allowable range; however, both TSVC enhanced schemes maintain a stable and very low message-loss ratio which is from 0.7% to 4 %. They are found to be much less sensitive to the traffic load.

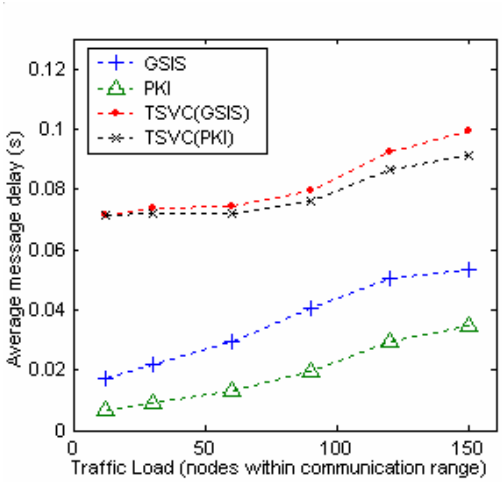

Figure 3-6. Impact of traffic load on the message end to end delay in city scenario

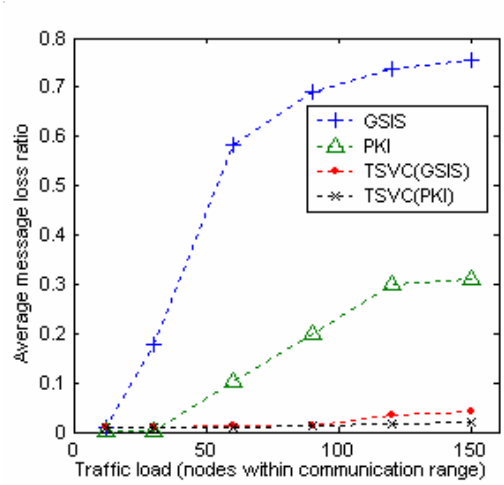

Figure 3-7. Impact of the traffic load on the message loss ratio in city scenario

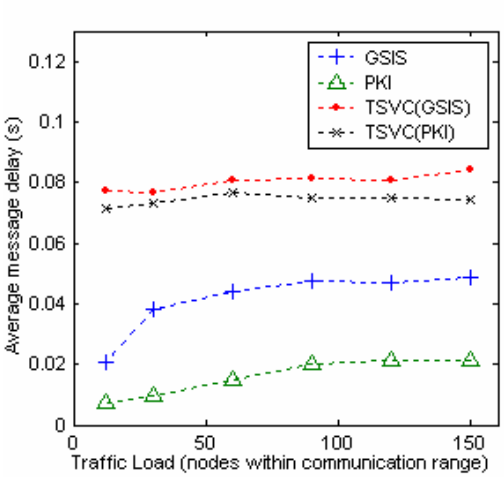

Figure 3-8. Impact of the traffic load on the message end to end delay in highway scenario

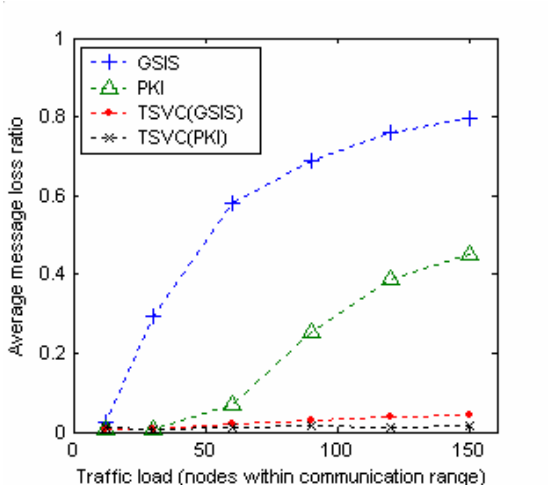

Figure 3-9. Impact of the traffic load on the message loss ratio in highway scenario

Chapter 4 Conclusion

This study first presents a new security mechanism called GSIS based on group signature and ID-based signature schemes for IVC applications. With group signatures, security, privacy, and efficient traceability can be achieved without inducing the overhead to manage a huge number of stored certificates. Meanwhile, public key and certificate management operations are further avoided for the communications between the RSU and OBU by using an ID-based signature technique to sign the messages sent by RSUs. Upon simulation, however, the observed message delays and loss ratios are not desirable in most traffic load scenarios. Better performance can be achieved in less dense traffic load conditions with powerful processors. We expect much better performance when the group signature verification is implemented in hardware. To enhance the performance of GSIS with software implementation, the study further proposes a novel TSVC security protocol. The new TSVC protocol can be applied to both GSIS and traditional PKI based security mechanisms. It significantly improves the system efficiency in terms of the packet length and the computation complexity without affecting the security and conditional anonymity requirements in VANETs. TSVC-enhanced protocols are measured through extensive simulations, which demonstrate that they incur a much lower message loss ratio compared to that of traditional public key based security schemes as well as the GSIS scheme, especially when the density of vehicles increases.

On the other hand, there are some shortcomings for our scheme as well. For example, the message end-to-end delay in TSVC-enhanced GSIS is increased by introducing a key release delay. Since the delay is still within the maximum allowable message latency, it is still acceptable. In addition, to maintain a comparatively stable group relationship, TSVC-enhanced GSIS cannot verify routine messages from the opposite side of the road. However, considering that routine messages in the same driving direction are much more useful, it is reasonable to make such a decision. One other concern for our scheme is that there are some centralized trusted authorities like MM who knows everybody's private key, and like TM who can reveal the identities of vehicles. This is a single point of failure. To overcome this weakness, cryptographic threshold technologies [BZ2004, DCL2004] can be used in real life to share secret keys and thus diminish the rights held by a single party.

Based on the above considerations, the TSVC-enhanced security protocols can serve as good candidates for real-world vehicular communication applications.

As for future research, how to improve the efficiency of the CRL checking procedure will be an interesting project. In our scheme, even if the hybrid revocation scheme of section 2.2.2.6 is used, the CRL checking procedure still incurs a high computational cost. Therefore, migrating these operations to the RSU side, which will instead perform the CRL checking process and broadcast the result to the vehicles in its communication range will be an interesting topic to examine. In addition, how to modify the TSVC-enhanced GSIS protocol so that it can achieve efficiency without affecting the 'unlinkability' property of the group signature scheme is a potential way to get improvements. In this paper, we authenticate the nodes in order to build the trust relationship which can not detect the node sending valid but fake messages. Therefore, how to detect valid but fake messages will be a challenging work as well. Another interesting topic is how to prevent movement tracking attack conducted by observing message contents and thus linking two consecutive messages from the same vehicle together.

Bibliography

[ABD2006] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmuller, Attacks on Inter Vehicle Communication Systems - an Analysis. *3rd International Workshop on Intelligent Transportation (WIT 2006)*, March, 2006.

[ACJT2000] G. Ateniese, J. Camenisch, M. Joye and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. *In Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology,* LNCS, Vol. 1880, pp. 255-270, 2000.

[AF1999] C. Adams and S. Farrell. RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols, March, 1999.

[ANSI X9.62-2005] American National Standards Institute. Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-1988, January, 2005.

[BBS2004] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. *In Proceedings of Crypto 2004*, LNCS, Vol. 3152, pp. 41-55, 2004.

[BF2001] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. *In Proceedings of Crypto 2001,* LNCS, Vol. 2139, pp.213-229, 2001.

[BLMQ2005] P. S. L. M. Barreto, B. Libert, N. McCullagh and J. Quisquater. Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. *In Proceedings of Asiacrypt*, LNCS, Vol. 3788, pp. 515-532, 2005.

[BLS2001] D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. *In Proceedings of Asiacrypt*, LNCS, Vol. 2248, pp. 514-532, 2001.

[BS2004] D. Boneh and H. Shacham. Group Signatures with Verifier Local Revocation. *In proceedings of the 11th ACM conference on Computer and Communications Security (CCS)*, pp. 168-177, 2004.

[BZ2004] J. Baek and Y. Zheng. Identity-Based Threshold Signature Scheme from the Bilinear Pairings. *International Conference on Information Technology: Coding and Computing(ITCC04)*, Vol.1, pp. 124-128, April, 2004.

[CvH1991] A. Chaum and E. van Heyst. Group Signatures. *In Proceedings of Eurocrypt*, pp. 257-265, 1991.

[CJW2005] J. Y. Choi, M. Jakobsson and S. Wetzel. Balancing Auditability and Privacy in Vehicular Networks. *In Proceedings* of *the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 2005.

[DCL2004] S. Duan, Z. Cao and R. Lu. Robust ID-based threshold signcryption scheme from pairings. *In Proceedings of the 3rd international conference on Information security*, Vol. 85, pp. 14-16, November, 2004.

[DoT2006] U.S. Department of Transportation. National Highway Traffic Safety Administration, Vehicle Safety Communications Project, Final Report. Appendix H: WAVE/DSRC Security, April, 2006.

[DoT_DSRC] DSRC, available at http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm

[FRF2007] J. Freudiger, M. Raya and M. Feleghhazi. Mix Zones for Location Privacy in Vehicular Networks. *In Proncessings of the 1st International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 07)*, Vancouver, Canada, August, 2007.

[GBW2007] J. Guo, J. P. Baugh, and S. Wang. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. *In Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, Anchorage, Alaska, May, 2007.

[GM2001] P. Golle and N. Modadugu. Authenticating Streamed Data in the Presence of Random Packet Loss. *ISOC Network and Distributed System Security Symposium*, pp.13-22, 2001.

[H2004] S. Han. An Efficient Identity-Based Group Signature Scheme over Elliptic Curves. *In Proceedings of Universal Multiservice Networks: Third European Conference (ECUMN 2004)*, Porto, Portugal, October, 2004.

[HAKL2005] Q. Huang, I. C. Avramopoulos, H. Kobayashi and B. Liu. Secure Data Forwarding in Wireless Ad Hoc Networks. *In Proceedings of IEEE International Conference on Communications(ICC 2005)*, Seoul, Korea, May, 2005.

[IEEE802.16e-2005] IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1, IEEE Std 802.16e-2005 and IEEE Std 802.14-2004/Cor1-2005, 2006.

[IEEE1609.2-2006] Intelligent Transportation Systems Committee, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, 2006.

[K2005] T. Kosch. Technical Concept and Prerequisites of CAR 2 CAR Communication. *The 5th European Congress and Exhibition on Intelligent Transport Systems and Services (ITS2005),* Hannover, Germany, June, 2005.

[L1981] L. Lamport. Password Authentication with Insecure Communication. *Communications of the ACM*, Vol. 24, pp. 770-772, November, 1981.

[LH2004] J. Luo and J. P. Hubaux. A Survey of Inter-Vehicle Communication. *Technical Report IC/2004/24, School of Computer and Communication Sciences,* EPFL, Lausanne, Switzerland, 2004.

[LY2006] C. Liu and J. T. Yu. An Analysis of DoS Attacks on Wireless LAN. *In Proceedings of the 6th IASTED International Multi-Conference on Wireless and Optical Communications*, pp. 346-351, 2006.

[M2005] J. V. E. Molsa. Increasing the DoS attack resiliency in military ad hoc networks. *In Proceedings of IEEE MILCOM*, Atlantic City, New Jersey, USA, 2005.

[NAG2004] V. Namboodiri, M. Agarwal and L. Gao. A study on the Feasibility of Mobile Gateways for Vehicular Ad-hoc Networks. *In Proceedings of the 1st ACM workshop on Vehicular ad hoc networks (VANET04)*, October, 2004.

[P2002] C. Popescu. An efficient ID-based Group Signature Scheme. Studia Univ. *Babes-Bolyai, Informatica*, Vol. XLVII, pp. 29-38, November, 2002.

[PCTS2002] A. Perrig, R. Canetti, J. D. Tygar and D. Song. The TESLA Broadcast Authentication Protocol. *Cryptobytes*, Vol. 5, No. 2, pp. 2-13, 2002.

[PKHK2006] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl. Privacy and Identity Management for Vehicular Communication Systems: A Position Paper. *Workshop on Standards for Privacy in User-Centric Identity Management*, Zurich, Switzerland, July, 2006.

[PNM2006] K. Plossl, T. Nowey and C. Mletzko. Towards a Security Architecture for Vehicular Ad Hoc Networks. *The 1st International Conference on Availability, Reliability and Security (ARES2006)*, pp. 374 -381, April, 2006.

[PP2005] B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. *In Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets-IV)*, November, 2005.

[PSWCT2002] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. *Wireless Networks*, Vol. 8, No. 11, pp. 521-534, 2002.

[RAH2006] M. Raya, A. Aziz and J. P. Hubaux. Efficient Secure Aggregation in VANETs. *In Proceedings of the 3rd International workshop on Vehicular ad hoc networks (VANET06)*, pp. 67-75, September, 2006.

[RH2005] M. Raya and J. P. Hubaux. The Security of Vehicular Ad Hoc Networks. *In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (SASN 2005)*, November, 2005.

[RH2007] M. Raya and J. P. Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, Vol. 15, pp. 39 - 68, 2007.

[RJPAH2006] M. Raya, D. Jungels, P. Papadimitratos, I. Aad and J. P. Hubaux. Certificate Revocation in Vehicular Networks. *EPFL Technical report LCA-REPORT-2006-006*, 2006.

[RPH2006] M. Raya, P. Papadimitratos, and J. P. Hubaux. Securing Vehicular Communications. *In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, October, 2006.

[RS1996] R. Rivest and A. Shamir. PayWord and MicroMint: Two Simple Micropayment Schemes. *In Proceedings of the 4th Security Protocols International Workshop*, LNCS, Vol. 1189, pp. 69-87, 1996.

[S2007] M. Scott, Implementing Cryptographic pairings. *Pairing 2007*, LCNS, Vol. 4575, pp. 177-196, Tokyo, Japan, July, 2007.

[SB2006] M. Scott and P. S. L. M. Barreto. Generating More MNT Elliptic Curves. *Designs, Codes and Cryptography*, Vol. 38, Issue 2, pp. 209- 217, February, 2006.

[SJ2004] A. K. Saha and D. B. Johnson. Modeling Mobility for Vehicular Ad Hoc Networks. *In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (VANET04)*, October, 2004.

[SS] Shamus Software. MIRACL library, available at http://www.shamus.ie/index.php?page=Elliptic-Curve-point-multiplication

[SURH2007] S. U. Rahman and U. Hengartner. Secure Crash Reporting in Vehicular Ad hoc Networks. *In Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm2007)*, Nice, France, September, 2007.

[TC2003] J. Tian and L. Coletti. Routing approach in CARTALK 2000 project. *In proceedings of the IST Mobile & Wireless Communications Summit 2003*, Vol. 2, 2003.

[USC] University of South California. The Network Simulator ns-2. Available at http://nsnam.isi.edu/nsnam/index.php/User_ Information

[USDoC] U.S. Department of Commerce. National Institute of Standards and Technology (NIST), Digital Signature Standard, FIPS PUB 186-2, 2000.

[USDoT2006] U.S. Department of Transportation. National Highway Traffic Safety Administration. Vehicle Safety Communications Project. Final Report, April, 2006.

[W2004] G. Wang. Security Analysis of Several Group Signature Schemes. http://eprint.iacr.org/2003/194, April, 2004.

[XSSSZ2007] Y. Xi, K. Sha, W. Shi. L. Scnwiebert and T. Zhang. Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks. *8th International Symposium on Autonomous Decentralized Systems (ISADS2007*), pp. 344-351, 2007.

[YASM2005] R. M. Yadumurthy, C. H. Adithya, M. Sadashivaiah and R. Makanaboyina. Reliable MAC Broadcast Protocol in Directional and Omni-directional Transmissions for Vehicular Ad hoc Networks. *In Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks (VANET 05)*, September, 2005.

[ZWW2003] J. Zhang, Q. Wu and Y. Wang. A Novel Efficient Group Signature with Forward Security. *Information and Communications Security (ICICS03)*, LNCS, Vol. 2836, pp. 292-300, 2003.