RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS

Lei Zhang

ISBN: 978-84-693-8865-5
Dipòsit Legal: T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Universitat Rovira i Virgili

Department of Computer Engineering and Maths

Ph.D. Dissertation

Research on Security and Privacy in Vehicular Ad Hoc Networks

Author:
Lei Zhang

Advisors:
Dr. Josep Domingo Ferrer and Dr. Qianhong Wu

Dissertation submitted to the Department of Computer Engineering and Maths in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science

June 2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy in Computer Science.

Dr. Josep Domingo-Ferrer
(Advisor)

I certify that I have read this dissertation and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy in Computer Science.

Dr. Qianhong Wu
(Advisor)

Approved by the University Committee on Graduate Studies:

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Preface

As information and communications technologies (ICT) become increasingly pervasive, vehicles are expected [Blau08] to be equipped in the near future with intelligent devices and radio interfaces, known as on-board units (OBUs). OBUs are allowed to talk to other OBUs and the road-side infrastructure formed by road-side units (RSUs). The OBUs and RSUs, equipped with on-board sensory, processing, and wireless communication modules, form a self-organized vehicular network, commonly referred to as vehicular *ad hoc* network (VANET), a commercial instantiation of mobile *ad hoc* networks with vehicles as the mobile nodes.

VANET systems aim at providing a platform for various applications that can improve traffic safety and efficiency, driver assistance, transportation regulation, infotainment, etc. There is substantial research and industrial effort to develop this market. Vehicular communications are supported by the Dedicated Short Range Communications (DSRC) standard [DSRC] in the USA and the Car 2 Car Communication Consortium [Car2car] in Europe. Microsoft Corp.'s MSN TV [Msntv] and KVH Industries, Inc. [KVH] have introduced an automotive vehicle Internet access system called TracNet, which can bring Internet service to any in-car video screen. In Europe, several projects such as SEVECOM [Secure] and NOW [NOW] are under way. It is estimated that the market for vehicular communications will reach

ISBN:978-84-693-8865-5/DL:T.1942-2010

several billion euros.

While the tremendous benefits expected from vehicular communications and the huge number of vehicles are strong points of VANETs, their weakness is vulnerability to attacks against security and privacy:

- In what regards security, attackers may exploit VANETs to send bogus information to cheat other vehicles. For instance, selfish vehicles may attempt to clear up the way ahead or mess up the way behind with false traffic reports; criminals being chased may disseminate bogus notifications to other vehicles in order to block police cars; terrorists may produce serious traffic collisions with contradictory traffic announcements. Such attacks may result in serious harm, even loss of lives.

- Regarding privacy, VANETs open a big window to observers. It is very easy to collect information about the speed, status, trajectories and whereabouts of the vehicles in a VANET. With this information, the traffic administration authorities can optimize the traffic and relieve jams. However, by exploiting this information, malicious observers can draw inferences about a driver's personality (*e.g.*, someone driving slowly is likely to be a calm person), living habits and social relationships (visited places tell a lot about people's lives). This private information may be traded in underground markets, exposing the observed vehicles and drivers to harass (*e.g.*, junk advertisements), threats (*e.g.*, blackmail if the driver often visits an embarrassing place, like a red-light district) and dangers (*e.g.*, hijacks).

Hence, both security and privacy should be taken into serious consideration at the time of general deployment of VANETs. These issues seem similar to those encountered in traditional communication networks, but there are

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

distinctive features. The seriousness of security and privacy failures, the self-organized nature of the network, the high mobility of vehicles, the relevance of their geographic position, and the very sporadic connectivity between nodes make the problem of achieving security and privacy in VANETs very novel and challenging. Further, the motivation of administrations and carmakers to deploy VANETs is precisely to decrease traffic congestion and accidents rather than increasing them: hence, security (and probably privacy) is a condition *sine qua non* for large-scale VANET deployment. This motivates the work described in this thesis.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Contents

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 1

Introduction

1.1 Background

With the fast advancement and pervasive deployment of information and wireless communication technologies, vehicular *ad hoc* networks (VANETs) are expected to develop in the near future. A VANET consists of on-board units (OBUs) embedded in vehicles serving as mobile nodes and road-side units (RSUs) working as the information infrastructure located in the critical points of the road. OBUs and RSUs are equipped with built-in sensory, data processing, and wireless communication modules. These modules allow vehicles and road-side infrastructure units to communicate with each other over single or multiple hops to exchange and share information about the routine driving status reports of vehicles and the driving environment changes. With these mechanisms, the OBUs and RSUs form a self-organized network which is the first commercial version of mobile *ad hoc* networks.

VANETs have various potential applications. The main thrust behind this type of networks are applications related to traffic safety. Tens of thousands of people die and hundreds of thousands get injured in traffic accidents

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

all over the world each year. Many traffic accidents come from the lack of cooperation between drivers. By giving more information about possible conflicts, most life-endangering accidents can be averted. VANETs also facilitate traffic optimization. Indeed, vehicles can collect data about traffic jams, weather or road surface conditions, construction zones, highway or rail intersections, emergency vehicle signal preemption, etc., and become information sources by sending those data to other vehicles in the VANET. These mechanisms enable transportation administration authorities to guide vehicles and manage them electronically (*e.g.*, speed control, permits, etc.), which is much more efficient than traditional manual administration. Finally, in addition to safety-related applications, value-added services can be provided via VANETs. By implementing advanced electronic payment protocols in VANETs, one can expect to pass a toll collection station without having to reduce speed, wait in line, look for some coins and so on. As GPS systems have become available in many vehicles, it is also possible to realize location-based services in VANETs, for instance, finding the closest fuel station, restaurant, hotel, etc. Other kinds of services include infotainment, vehicle-based electronic commerce and so on. All these services lead to a more comfortable driving experience for drivers.

Having realized the great commercial opportunities of VANETs, many academic and industrial organizations are committed to developing them. In the USA, the Dedicated Short Range Communications (DSRC, [DSRC]) standard is being developed to support wireless communications for vehicles and road-side infrastructure. The Car2Car Communication Consortium deals with vehicular communication standardization in Europe [Car2car]. With OBUs having a wireless connection to Internet, some infotainment can be provided, *e.g.*, Microsoft Corp.'s MSN TV [Msntv] and KVH Industries

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Inc. [KVH] have introduced an automotive vehicle Internet access system named TracNet, which can bring Internet service to any in-car video screen. It is predicted that the market of VANETs can be up to billions of Euros in the near future.

For those new services to make life easier rather than more difficult, they should rely on secure and privacy-preserving protocols that encourage users to participate without fear for their safety or personal privacy [Samp05]. Consequently, security and privacy are two critical concerns for the designers of VANETs that, if forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks:

- If message integrity is not guaranteed, a malicious vehicle could modify the content of a message sent by another vehicle to affect the behavior of other vehicles. By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, the vehicle that originally generated the message would be made responsible for the damage caused.

- If authentication is not provided, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.

- A malicious vehicle could report a false emergency situation to obtain better driving conditions (*e.g.*, deserted roads) and, if non-repudiation is not supported, it could not be sanctioned even if discovered.

From the previous examples, it becomes apparent that message authentication, integrity, and non-repudiation are primary requirements in VANETs.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

There is a need for mechanisms that provide VANETs with security, *i.e.*, protocols, methods and procedures that are able to: detect whether a message has been modified by an attacker and determine who is the real sender of a message.

Besides these essential security requirements, privacy is another important issue in VANETs that cannot be forgotten. If the importance of privacy protection measures is underestimated, the privacy of VANET users could be endangered. For example, an eavesdropper could collect messages sent by vehicles and track their locations; by doing so, he could infer sensitive data of users such as their residence and their real identities [Karg95]. Note that these privacy problems are similar to the ones of location-based services (LBS, cf. [Sola08a, Sola08b] for further details). Nevertheless, privacy in VANETs should be conditional, this is, user-related information such as license plate, current speed, current position, identification number, and the like, should be kept private from other users/vehicles in the system while authorized users (*e.g.*, police officers) should have access to it.

1.2 Characteristics of VANETs

VANETs have a number of distinctive features with respect to generic mobile *ad hoc* networks. Such features include the life-or-death importance of decisions, the potentially disastrous consequences of security and privacy failures, the high mobility of vehicles, etc. Due to these reasons, designing secure and functional VANETs is a challenging problem.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

1.2.1 Challenges

The life-or-death risk may be the most special feature of VANETs. In the traditional networks or other emerging mobile networks, security and privacy failures usually bring only financial losses. However, both security and privacy failures in VANETs could be much more serious. For instance, the failure to detect a tampered vehicular message in time may cause serious traffic accidents, with loss of lives. In case of privacy failures, a driver (*e.g.*, a well-known millionaire or movie star) may become the victim of kidnappers for ransom if organized criminals extract his/her driving routine by collecting and analyzing vehicular communications. This implies that every effort must be devoted to security and privacy concerns as a precondition for wide adoption of VANETs. To achieve security, mechanisms are required to guarantee authentication, integrity and non-repudiation of vehicular messages. At this point, one realizes that solving the inherent conflict between authentication and privacy poses a significant challenge.

Usually, to achieve security, vehicle-generated messages must be signed so that the receiving vehicles can verify that these messages have been originated by authentic sources and have not been modified during transmission [Goll02b]. However, with these signatures, it is possible for attackers to identify who generated a vehicular message containing speed, location, direction, time and other driving information. A lot of private information on the driver can be inferred if the driving pattern of his/her car can be tracked. Furthermore, the signed vehicle-generated messages have to be stored by the receiving vehicles for possible liability investigation: if some signed messages are later found to be false and to have misguided other vehicles into accident, the message generators and endorsers should be traceable. However, vehicular messages, especially their appended signatures, grow linearly with

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

time while the storage capacity of OBUs in the vehicles is limited. Therefore, security and privacy of vehicle-to-vehicle (V2V) communications need to be conciliated with data aggregation/compression [Viej09, Wase09].

Network volatility is another factor that increases the difficulty of securing VANETs. Connectivity among vehicles can often be highly transient due to their high speeds (*e.g.*, think of two vehicles crossing each other in opposite directions in a highway). This implies that protocols requiring multiple rounds or strong cooperation such as voting mechanisms may be impractical. Due to their high mobility, vehicles may never again connect with each other after one occasional connection. This puts the public key infrastructure implemented for securing VANETs under strain: if public-key certificates are used, vehicles are confronted to a lot of certificates probably issued by several different CAs; due to the mobility, there is little hope that caching the verified certificates of vehicles and CAs will result in any significant speed-up of the next verifications.

The size of VANETs deployed in metropolitan areas with millions of vehicles is another challenge. Transportation systems are governed by a multitude of authorities with different interests, which complicates things. A technically, and perhaps politically, convincing solution is a prerequisite for any security architecture. Another challenge is the sheer scale of the network: the system has to manage (tens of) millions of nodes of which some may join or leave the VANET occasionally and some may be compromised. This rules out protocols requiring massive distribution of data to all mobile nodes.

A final challenge comes from the time constraints of the envisioned safety and driver-assistance applications. In case of emergency braking, milliseconds of delay may cause a serious traffic accident. Hence emergency messages must be generated by the sender and verified by the receiver as soon as possible.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

In case of high vehicular density in metropolitan areas, each node may be flooded by a large number of messages to be verified. Ideally, the safety-related messages should be generated efficiently and given high verification priority even if the receiver is flooded. Unfortunately, very few efforts have been made so far to cater for these compelling concerns in practice.

1.2.2 Mitigating features

It follows from the above discussions that security in vehicular networks faces a multitude of challenges. Nevertheless, we also observe that VANETs possess special characteristics that can mitigate the above challenges and enable high security and privacy standards.

Unlike in most mobile *ad hoc* networks (MANETs), nodes in VANETs can be expected to have substantial power supply and computational capacity. Cars have ample supply of power compared to battery-powered cell phones or sensors. This implies that the communication protocols do not need to be especially power-efficient. Compared with the price of a car, the cost of computational capacity in OBUs is not an issue; in fact, an OBU can be assumed to be as powerful as a personal computer. The protocols can therefore exploit advanced cryptosystems to achieve high-end security in VANETs, in opposition to other mobile networks where minimization of cryptographic operations is necessary.

The security protocols in VANETs can also benefit from the existing transportation systems. In most countries, all vehicles must be registered at a central authority, which makes possible, for example, the assignment of unique identities to vehicles. Traffic lights, traffic sensors, radars, etc. have long been part of the infrastructure of current transportation systems. They can be updated to become road-side units in VANETs. Also, vehicles

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

undergo regular (annual) health inspections which permit sanity checks to be run against the components of the vehicular networking system of each car. The (tamper-proof) OBUs can be checked for integrity and updated to the manufacturer's latest version. Malfunctioning sensors that provide false data (maybe because of tampering by an adversary) can be replaced. Also, vehicles can leverage the additional input derived from the driver's responses with information provided by the networking subsystem. In many situations a human driver can do a better assessment of a situation and reliably check whether the information is correct or not, if the critical information is human-recognizable.

Redundancy in vehicular communications can be a beneficial factor that helps improving security and relieving the burden of message validation in VANETs. A vehicle periodically receives large numbers of messages. However, some of them may be reporting the same traffic conditions; this can be used to correct erroneous messages caused by occasional sensing errors or malicious attacks. Further, only a fraction of the non-redundant messages need validation. For example, a notification that the vehicle ahead will accelerate does not affect the vehicle receiving the report. Similarly, a vehicle does not need to validate a notification informing that the vehicle behind will brake. By taking these factors into consideration, the message validation burden can be greatly relieved without degrading security.

Finally, the existing law enforcement mechanisms are likely to be extended to cover malicious behavior in vehicular networks that compromises the drivers' safety. This can be a serious deterrent to attackers of VANETs. Note that such law enforcement is not available in other forms of wireless *ad hoc* networks. To exploit this deterrent, vehicular communications must offer non-repudiation so that the message generator cannot deny the fact that

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

he/she generated a message. In case of dispute, non-repudiable messages can be taken as valid evidence in court.

1.3 Objectives

Security and privacy are two critical concerns for the designers of VANETs. This Ph. D. thesis intends to:

- Design practical cryptographic schemes and develop novel methods for securing vehicular communications.
- Design vehicular authenction schemes conciliating security, privacy and performance in VANETs.
- Design secure value-added services (*e.g.*, location-based service) in VANETs.

1.4 Structure of this thesis

This thesis is organized as follows.

Chapter 2 reviews the state of the art on security and privacy in VANETs.

Chapter 3 reviews mathematical and cryptographic background used by our secure and privacy-preserving protocols: bilinear maps, complexity assumptions and the batch verification lemma.

Chapter 4 deals with several efficiency and security challenges (*i.e.*, certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper-proof devices) by introducing a new group authentication protocol which is decentralized in the sense that the group is maintained by each RSU rather than

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

by a centralized authority as in most existing protocols employing group signatures. In our proposal, we employ each road-side unit (RSU) to maintain and manage an on-the-fly group within its communication range. Vehicles entering the group can anonymously broadcast vehicle-to-vehicle (V2V) messages, which can be instantly verified by the vehicles in the same group (and neighbor groups). Later, if the message is found to be false, a third party can be invoked to disclose the identity of the message originator. Our protocol efficiently exploits the specific features of vehicular mobility, physical road limitations and properly distributed RSUs. Our design leads to a robust VANET since, if some RSUs occasionally collapse, only the vehicles driving in those collapsed areas will be affected. Due to the numerous RSUs sharing the load to maintain the system, performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.

Chapter 5 proposes a set of mechanisms that can actually conciliate traffic safety, driver privacy and system efficiency. We employ identity-based group signatures (IBGS) to divide a large-scale VANET into easy-to-manage groups and establish liability in vehicular communications while preserving privacy. Each party's known identity, such as a vehicle license plate, is used as its public key and no additional certificate is required. This efficiently avoids the complicated certificate management of existing protocols. We further investigate emergency message generation and selfish verification techniques to accelerate message processing in VANETs. Emergency message generation allows vehicles to authenticate announcements with almost no delay. With the selfish verification technique, a vehicle selects only the messages affecting its driving decisions and validates the selected messages as if they were a single one. These techniques effectively address the message processing bottleneck in protocols for securing VANETs.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Cryptographic authentication techniques have been extensively exploited to secure VANETs. Applying cryptographic authentication techniques such as digital signatures raises challenges to efficiently store signatures on messages growing with time and to alleviate the conflict between traffic liability investigation and limited storage capacity in vehicles. In Chapter 6, we efficiently address those challenges by aggregating signatures in VANETs. With our proposals, safety-related traffic messages can be significantly compressed so that they can be stored for a long period for liability investigation. Furthermore, our proposals allow a large number of traffic messages to be verified as a single one, which greatly speeds up the response of vehicles to messages. Analysis also shows that our proposals achieve high performance without degrading security.

In Chapter 7, we propose a privacy-preserving LBS scheme in VANETs. The proposed scheme employs identity-based cryptography and group signatures as building blocks. In our proposal, no certificate is required to guarantee the security of the system, which eliminates the certificate management overhead inherent to most existing systems. Our scheme achieves strong privacy in the sense that an attacker (even an LBS provider) cannot decide whether two different LBS requests were generated by the same vehicle. However, if the message is later found to be false, a third party can determine the identity of the vehicle. Analysis shows that cryptographic operations in LBSs introduce only very slight overhead to the underlying VANETs. Further, our scheme is robust in the sense that it does not rely on proxies, the latter being too instable due to volatile connections in VANETs.

Chapter 8 contains concluding remarks and guidelines for future research.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 2

State of the Art

Due to the extraordinary commercial and social potential of VANETs, they have attracted the attention of industry and academia. In Europe, the CAR 2 CAR Communication Consortium [Car2car] is leading the efforts to create a European industry standard for vehicle-to-vehicle (V2V) communication systems predicated upon wireless LAN components. In the US, the Intelligent Transportation Systems Committee, sponsored by the IEEE Vehicular Technology Society, has defined the standard for Wireless Access in Vehicular Environments (WAVE, [WAVE]). WAVE is a radio communications system intended to provide interoperable wireless networking services for transportation. These services include those recognized for Dedicated Short-Range Communications (DSRC) [DSRC] by the U.S. National Intelligent Transportation Systems (ITS) Architecture (NITSA) [National].

Security and privacy issues in VANETs have recently been studied by many researchers. Various security and privacy challenges in vehicular networks are discussed in [Cala07, Daza09, Duri02, Gerl05, Goll10c, Huba04a, Lee07, Parn05, Papa06, Papa07, Raya06, Raya05, Zark02]. In [Blum04], Blum and Eskandarian propose a secure communications architecture based

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

on a public key infrastructure (PKI) and a virtual network controlled by cluster-heads intended to counter the so-called "intelligent collisions", which are collisions intentionally caused by malicious vehicles. This approach produces a remarkable overhead and the use of cluster-heads can create bottlenecks. Gollan and Meinel [Goll02a] propose the use of digital signatures along with GPS technology to identify cars securely, improve the fleet management, and provide new applications for the private and the public sector. Considering the problem from a different point of view, Hubaux *et al.* [Huba04a] emphasize the importance of privacy and secure positioning, and propose the use of Electronic License Plates (ELP) to identify vehicles. Although they recognize the importance of conditional privacy, they do not provide any specific solution to the problem.

2.1 Secure and privacy-preserving protocols for vehicular communications

To address the security and privacy challenges in safety-related applications of VANETs, two techniques are generally used. The first one is based on anonymous certificates and the second one is based on group signatures.

2.1.1 Technique based on anonymous certificates

In this line, a foundational proposal is given by Raya and Hubaux in [Raya07]. The authors use anonymous certificates (*i.e.*, pseudonyms [Fons07]) to hide the real identities of users[1]. Even though anonymous certificates do not contain any publicly known relationship to the true identities of the key holders,

[1]Note that even when anonymous certificates are used, Trusted Authorities can trace the real identity of users.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

privacy can still be invaded by logging the messages containing a given key and tracking the sender until her identity is discovered (*e.g.*, by associating her with her residence)[2]. To avoid this attack, the way in which anonymous certificates are used should be modified so that an observer cannot track the owner of the keys. A natural way to do so, proposed in [Raya07], consists in storing a number of anonymous certificates (as well as the corresponding private/public key pairs) in a vehicle, so that the vehicle can use different key pairs and avert traceability. However, depending on the key change frequency, which can vary according to the current speed of the vehicle, vehicles will have to store a large number of pairs. Thus, the secure distribution of keys, key management, and storage become very complex; hence, this type of scheme should be avoided for the sake of practicality.

In [Lu08], Lu *et al.* proposed an alternative way to overcome the limitation of pre-storing a large number of anonymous certificates whilst preserving conditional privacy. They assume that vehicles and RSUs are able to collaborate actively. Each vehicle issues a request for a short-time anonymous certificate from an RSU when the vehicle is passing by the RSU, and obtains an anonymous certificate after running a two-round protocol. Since a vehicle should change the anonymous certificate quite often to avert linkability of the messages, it should interact with RSUs frequently. Such a frequent interaction may affect the efficiency of the VANET. This short-lived anonymous certificate needs to be sent and forwarded to verifiers for validating messages from the anonymous originator. It is also worth mentioning the schemes in [Freu07, Zhan08a], which also rely on RSUs. In [Freu07], the method of mix-zones is used to enhance the anonymity of vehicles. However, this scheme

[2]This attack is possible due to the linkability "property" of the messages.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

still relies on pre-loading a large set of anonymous certificates in each vehicle. In [Zhan08a], by exploiting a keyed hash message authentication code (HMAC), a scheme with low communication overhead is proposed to secure vehicle communications. This scheme requires a vehicle to obtain a symmetric key from an RSU using a key agreement protocol. In order to protect its privacy, the vehicle should use different public keys to communicate with the RSUs. Hence, the vehicle still needs to pre-load a certain number of anonymous certificates. As to robustness, the schemes in [Freu07, Zhan08a] fully rely on RSUs. If an RSU collapses, then these schemes will not work any more.

Recently, by using ID-based cryptography [Sham84] to avoid complicated certificate management, Zhang *et al.* [Zhan08b] designed an efficient conditional privacy-preserving protocol for vehicular communications. Their approach relies on tamper-proof devices embedded in the vehicles. The system's master key is stored in those tamper-proof devices so that pseudo-identities (the function of which is similar to the use of anonymous certificates) can be generated locally. Storing the system's master key in each vehicle may expose the system to powerful attackers and unpredictable risks even if the storage devices are assumed to be tamper-proof. Those expensive tamper-proof devices can prevent attackers from reading the secrets physically stored in them. However, since the system's master key will be involved in local computations, the attacker has the chance to measure the energy (or time) consumed by the computations, and the emitted electronic radiation, which contains information about the secret. With this information and by means of statistical methods, the attacker can launch powerful key extraction attacks such as side channel attack [Koch96, Stan09], which are well-known in cryptography. Although the side channel attack may be expensive to regular

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

users, it is attractive and practical to organized criminals since, once the master key is extracted, they have full control over the system.

2.1.2 Technique based on group signatures

Group signatures [Bone04b, Chau91, Grot07] are an alternative to achieve security and privacy in VANETs. Group signatures have been investigated for many years. In a group signature, there is a group manager (whose role can be separated into two parts: issuer and opener) who maintains the group; members may join or leave the group dynamically. After registering to the group, the member can anonymously sign any message on behalf of the group. A verifier can verify the group signature with only the group public key but cannot know which registered vehicle is the message generator. However, if necessary, the group manager can reveal the originator of any group signature. The main merit of the group signature based technique over the anonymous certificates approach is that the former overcomes the limitation of pre-storing a large number of anonymous certificates.

Following this research line, Guo *et al.* [Guo07] presented a novel security framework for vehicular communications based on group signatures. However, neither concrete instantiation nor experiment analysis are given in [Guo07]. The first concrete instantiation of a group signature based technique in VANETs is due to Lin *et al.* [Lin07]. In [Lin07], they presented GSIS, a conditional privacy-preserving vehicular communications protocol based on group signatures, and ID-based signatures [Sham84]. In the GSIS protocol, a single membership manager who issues secret member keys for vehicles is used. Unfortunately, this approach cannot effectively cope with the exclusion of compromised vehicles from the system. The solutions proposed by Lin *et al.* [Lin07] to deal with compromised vehicles seem to be

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

insufficient. The first option is to update the group public key pair for all non-revoked vehicles. That entails a considerable overhead. The second option, called Verifier-Local Revocation (VLR), is similar to the traditional certificate revocation list scheme. Since the signature verification time grows linearly with the number of revoked vehicles, the VLR procedure becomes very time-consuming and inefficient when the number of revoked vehicles grows.

2.2 Signature aggregation in VANETs

We notice that the solutions proposed to secure VANETs face several unsolved problems: i) how to store and process a large number of signatures in the limited storage capacity of OBUs; ii) how to verify these signatures and corresponding certificates in a short interval to enable effective response; iii) how to compact and store cryptographic traffic evidence; iv) how to alleviate the conflict between traffic liability investigation and data storage limitations of vehicles.

Picconi *et al.* proposed a solution using PKI-based authentication scheme [Picc06] for validating aggregated data. This scheme focuses on aggregating messages, rather than aggregating signatures. Their main idea is to use random checks to probabilistically catch the attacker, and thereby discourage attacks in the network. Their solution assumes a tamper-proof service in each car to carry out certain secure operations such as signing and time stamping. As noted by themselves, their solution suffers from some limitations. Firstly, their solution can prevent modification of records and inclusion of fake ones, but it cannot handle omission of records. Also, reaggregation is not addressed. Another limitation of their solution is that it cannot provide

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

a generic method to validate semantically aggregated data. Finally, their solution relies on the presence of a tamper-proof service in each car. While this does not compromise flexibility significantly, it implies additional hardware cost. And tamper-proof devices may have flaws [Ande96] in practice.

Zhu *et al.* [Zhu08] applied BLS signatures to aggregate emergency messages and perform batch authentication in VANETs. Their certificate aggregation is for one CA. Wasef *et al.* [Wase09] proposed an authentication scheme enabling each vehicle to simultaneously verify not only the signatures but also the certificates in the PKI scenario. They also employed aggregate signatures at the stage of signature verification. This method increases the vehicle capability to verify a large number of signatures and certificates in a timely manner. However, their proposal does not consider message relay nor evidence storage, which are both critical concerns in VANETs.

2.3 Privacy-preserving LBS protocols

Mobile networks and positioning technologies create a strong market push for location-based services (LSBs) offered to the users based on their locations. In the United States, Nextel and Sprint initially drove the LBS adoption with a focus on fleet applications [Sprint]. The NextBus [NextBus] service provides location-based transportation data. The CyberGuide [Abow97] project investigates context-aware location-based electronic guide assistants, and the Federal Communications Commission's (FCC) Phase II E911 requires wireless carriers to provide precise location information within 125 m in most cases for emergency purposes [Reed98]. Verizon Wireless also entered the market and currently has five applications available[ERIZONWireless]. More applications of LBSs can be found in [Shin08].

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

It is attractive to introduce LBS into VANETs. The above proposals focus on security and privacy in safety-related applications of VANETs. However, none of them studies user privacy protection when vehicles access LBS applications. To fill this gap, Sampigethaya *et al.* [Samp07] proposed a scheme called AMOEBA. In their scheme, the group concept[3] is introduced to provide robust anonymous access to prevent the profiling by LBS applications accessed by any target vehicle. With this concept, a group leader (a single vehicle in the group) is selected to represent the group, and used as a proxy for LBS access. However, we notice that VANETs are very dynamic and their connections are volatile; hence, the groups in this kind of networks are hard to maintain. Also, there are additional weaknesses. Firstly, the leader sacrifices its location privacy by continually revealing its locations. Secondly, the use of the leader as a proxy for LBS access implies the lack of end-to-end connectivity between the service provider and group members. Thirdly, relying on one leader suffers from the single point of failure problem.

[3]Grouping vehicles thwarts the location tracking of any target vehicle.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 3

Mathematical Background

In this chapter, we review bilinear maps, related complexity assumptions and the batch verification lemma.

3.1 Bilinear maps

Recently, bilinear maps have been extensively investigated to build efficient schemes [Bold07, Bone01a, Bone01b, Came07, Zhan09a, Zhan09b, Zhan10a]. Our protocols are also implemented with bilinear maps. Thus, we briefly review them.

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be three multiplicative groups of prime order p. Let g_1 denote a generator of $\mathbb{G}_1$, g_2 be a generator of $\mathbb{G}_2$, ψ be a computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, with $\psi(g_2) = g_1$. A map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ is called a bilinear map if it satisfies the following properties:

1. Bilinearity: $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$ for all $u \in \mathbb{G}_1, v \in \mathbb{G}_2, a, b \in \mathbb{Z}_p^*$.

2. Non-degeneracy: $\hat{e}(g_1, g_2) \neq 1$.

3. Computability: There exists an efficient algorithm to compute $\hat{e}(u, v)$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

for any $u \in \mathbb{G}_1, v \in \mathbb{G}_2$.

Such a bilinear map $\hat{e}$ can be constructed with the modified Weil [Mene93] or Tate [Frey94] or Eta [Hess06] pairings on elliptic curves. ψ can be a trace map as described in [Bone01a], and when $\mathbb{G}_1 = \mathbb{G}_2$ and $g_1 = g_2$, ψ can be the identity map.

3.2 Complexity assumptions

The security of our protocol is based on the hardness of the following problems, which are as follows:

Computational co-Diffie-Hellman (co-CDH) Problem in $(\mathbb{G}_1, \mathbb{G}_2)$: Given (g_1^a, g_2^b) for unknown $a, b \in \mathbb{Z}_p^*$, compute g_1^{ab}.

Decisional Diffie-Hellman (DDH) Problem in $\mathbb{G}_1$: given $g_1, g_1^a, g_1^b, u \in \mathbb{G}_1$ for unknown $a, b \in \mathbb{Z}_p^*$, decide whether $u = g_1^{ab}$.

Co-Decisional Bilinear Diffie-Hellman (co-DBDH) Problem in ($\mathbb{G}_1$, $\mathbb{G}_2$): Given $g_1, g_1^a, g_1^b \in \mathbb{G}_1, u \in \mathbb{G}_2, y \in \mathbb{G}_T$ for unknown $a, b \in \mathbb{Z}_p^*$, decide whether $y = (g_1, Q)^{ab}$.

***q*-Strong Diffie-Hellman (*q*-SDH) Problem** in $(\mathbb{G}_1, \mathbb{G}_2)$: Given a $(q+2)$-tuple $(g_1, g_2, g_2^s, g_2^{s^2}, ..., g_2^{s^q})$ as input, output a pair $(g_1^{1/(s+x)}, x)$ where $x \in \mathbb{Z}_p^*$.

Decision Linear Problem in $\mathbb{G}_1$: Given $u, v, h, u^a, v^b, h^c \in \mathbb{G}_1$ as input, output "yes" if $a + b = c$ and "no" otherwise.

***k*-CAA2 Problem** in $(\mathbb{G}_1, \mathbb{G}_2)$: Given $u, v \in \mathbb{G}_1, g_2, g_2^\gamma \in \mathbb{G}_2$ and pairs (A_i, e_i, λ_i) with distinct and nonzero e_i's satisfying $A_i^{e_i+\gamma} v^{\lambda_i} = u$ for $1 \leq i \leq k$ as input, output a pair $(A_{k+1}, e_{k+1}, \lambda_{k+1})$ satisfying $A_{k+1}^{\gamma+ek+1} v^{\lambda^{k+1}} = u$, with $e_{k+1} \neq e_i$ for all $1 \leq i \leq k$.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

The co-CDH assumption in $(\mathbb{G}_1, \mathbb{G}_2)$ (resp. DDH assumption in $\mathbb{G}_1$, co-DBDH assumption in $(\mathbb{G}_1, \mathbb{G}_2)$, q-SDH assumption in $(\mathbb{G}_1, \mathbb{G}_2)$, Decision Linear assumption in $\mathbb{G}_1$ and k-CAA2 assumption in $(\mathbb{G}_1, \mathbb{G}_2)$) is that there is no polynomial-time algorithm that can solve the co-CDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ (resp. DDH problem in $\mathbb{G}_1$, co-DBDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$, q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$, Decision Linear problem in $\mathbb{G}_1$ and k-CAA2 problem in $(\mathbb{G}_1, \mathbb{G}_2)$) with non-negligible probability.

3.3 Batch verification lemma

In a VANET, each vehicle periodically sends messages every 100-300 ms within a distance of 10 s travel time [DSRC], which means a distance range between 10 m and 300 m. This implies that a vehicle will receive a large number of messages to be verified in a given interval. If the signatures are verified one by one, this verification delay is usually much greater than the allowed maximum end-to-end message processing delay, *i.e.* 100 ms [European]. Hence, we need additional mechanisms to speed up message verification in large-scale VANETs.

As noted in Section 1.2.2 above, the great redundancy of vehicular communications can be exploited to alleviate the burden of message verification. Only a small fraction of relevant messages actually need verification. If the number of messages selected for verification is still large, additional ways to reduce the verification overhead need to be devised. In what follows, we employ the batch verification technique ([Bell98, Came07, Cao06, Cheo07, Ferr09, Wu10, Yoon05]) to enable time-saving message processing in VANETs. This technique exploits the fact that a multi-base exponentiation (bilinear map) takes similar time as a single-base exponentiation (bilinear

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

map).

Lemma 1 (Batch verification lemma) *To verify exponential equations*

$$t_i^{x_i} f_i^{y_i} = 1, \quad \text{for } i = 1, \cdots, n \tag{3.1}$$

where $x_i, y_i \in \mathbb{Z}_p^*$ are known, and t_i, f_i are two elements of a finite cyclic group $\mathbb{G}$ of prime order p, one can randomly pick a vector[1] $\Delta = (\delta_1, \cdots, \delta_n)$ for $\delta_i \in \{0,1\}^l$ and verify that

$$\prod_{i=1}^{n} t_i^{\delta_i x_i} f_i^{\delta_i y_i} = 1. \tag{3.2}$$

If Equations (3.1) are accepted whenever Equation (3.2) holds, a batch

$$\{(t_i, f_i) | i = 1, \cdots, n\}$$

will be always accepted if it is valid while an invalid batch will be accepted with probability at most 2^{-l}.

The above claim can also naturally be extended to batch verification of bilinear map equations since these are indeed exponentiation equations in $\mathbb{G}_T$. In this case, we only need to additionally note that $1 = \hat{e}(t_1, h)^a \hat{e}(t_2, h)^b$ can be equivalently rewritten as $1 = \hat{e}(t_1^a t_2^b, h)$ to save computations due to bilinearity and the fact that exponentiations in $\mathbb{G}_1$ are more efficient than those in $\mathbb{G}_T$.

[1] *We notice that, in [Cheo07], width-w Non-Adjacent Forms (w-NAFs) are also introduced to accelerate the batch verification procedure.*

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 4

Robust and Scalable Privacy-Preserving Vehicular Authentication

We observe that existing privacy-preserving protocols for securing VANETs face several challenges such as efficient certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong dependence on tamper-proof devices. This chapter addresses these challenges by exploiting the features of vehicular mobility, road limitations, and densely distributed RSUs. We propose a decentralized authentication protocol[1] which, unlike the existing proposals, uses RSUs to maintain an on-the-fly generated group within their communication range, which is normally much longer than the V2V communication range. Vehicles can anonymously broadcast V2V messages that can be verified by other vehicles in the group

[1]The protocol is still centralized in the system set-up stage for enrolling vehicles. The term "decentralized authentication" refers to the group authentication being maintained by each distributed RSU to achieve robustness and scalability, rather than by a centralized authority as in most existing protocols employing group signatures.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

and neighboring groups.

In our system, vehicles only request a new secret member key when (i) they pass by an RSU for the first time or (ii) when their existing secret member keys expire. Since each vehicle only verifies messages from vehicles that have moved into the range of the same RSU and its neighbors, it can easily check whether the anonymous sender was revoked with the help of those RSUs and does not need to retrieve the revocation list from a remote centralized authority. This greatly reduces the certificate management overhead. Compared with the millions of vehicles in a VANET, the number of active vehicles within range of a single RSU is much smaller. Hence, the system will not suffer from computation and communication bottlenecks. Although each party in our system needs a secret member key, the system's master key is only known and stored by a centralized authority, rather than being stored in each tamper-proof device embedded in vehicles. Furthermore, our system is robust since, if some RSUs occasionally collapse, only vehicles moving in those areas will be affected, and our protocol can still work with slight changes. Due to the numerous RSUs sharing the load to maintain the system, its performance does not significantly degrade when more vehicles join the VANET; hence, the system is scalable.

The remainder of this chapter is organized as follows. Section 4.1 gives some preliminaries, including the network model, the security requirements, and the concepts of signcryption and group signature. Our efficient conditional privacy-preserving protocol is explained in Section 4.2. In Section 4.3, the security of our protocol is examined. The performance of our protocol is evaluated in Section 4.4. Finally, Section 4.5 is a summary.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

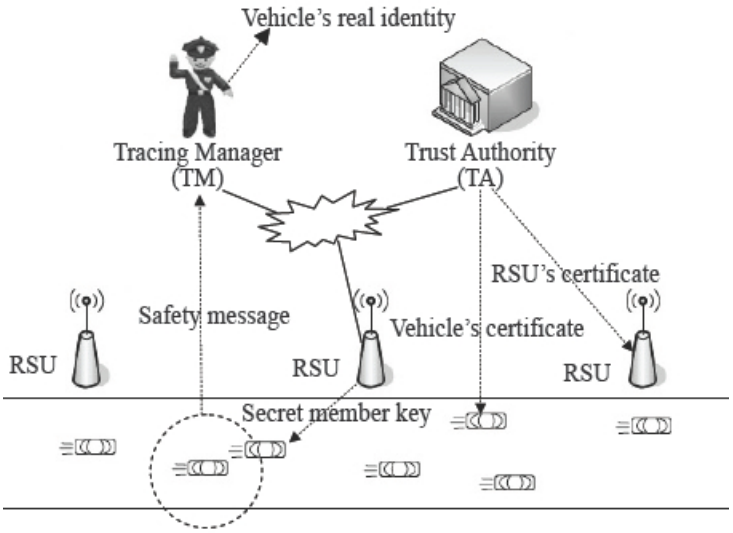

Figure 4.1: The network model

4.1 Preliminaries

4.1.1 Network model

Figure 4.1 illustrates the network model employed in our robust and scalable privacy-preserving vehicular authentication system. It consists of a Trusted Authority (TA), a Tracing Manager (TM), RSUs and vehicles.

- TA: The responsibility of the TA is to issue digital certificates for vehicles and RSUs. Also, it maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. The TA is assumed to be completely trustable, hard to compromise, and powerful, *i.e.* with sufficient computation and storage capacity.

- TM: When the content of a safety message broadcast by a vehicle is found to be false, the TM should be able to determine the vehicle's real

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

identity.

- RSU: RSUs are densely distributed in the road side. In our protocol, RSUs are used to issue secret member keys to vehicles and assist the TM to efficiently track the real identity of a vehicle from any safety message.

- Vehicle: Vehicles move along the roads, sharing collective environmental information, contained in safety messages, or requesting secret member keys from RSUs. OBUs are assumed to be embedded in each vehicle. By using OBUs, vehicles can communicate with each other as well as with the RSUs. The communication among them is based on the DSRC protocol [DSRC].

4.1.2 Security requirements

We consider several security requirements [Raya07, Lin07] in two communication scenarios: (i) confidential communication between a vehicle and an RSU; and (ii) V2V communication. The first scenario has three security requirements: *confidential communication*, *message authentication* and *privacy protection*; the second scenario should satisfy: *message authentication*, *privacy protection* and *anonymity revocability*. The detailed descriptions of the above requirements follow.

- **Confidential communication.** When a vehicle communicates with an RSU, only that vehicle and that RSU are aware of the information exchange. In our protocol, this implies that vehicles send a request to an RSU for a secret member key without being detected by other vehicles and receive a secret member key from the RSU secretly.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

- **Message authentication.** If a message has been modified after being sent, this modification is observable by a legitimate receiver. In addition, if the message has never been modified, it confirms to the legitimate receiver that the message was originated by a legitimate entity.

- **Privacy protection.** As mentioned above, privacy is an important concern in VANETs. We consider the following two cases.

  1. If the communication takes place between vehicles and RSUs, privacy means that an eavesdropper cannot decide whether two different messages come from the same vehicle.
  2. If the communication is between vehicles, privacy means that deciding whether two different valid messages were generated by the same vehicle is computationally hard for everyone except the TM.

- **Anonymity revocability.** The TM has the ability to retrieve the real identity of dishonest vehicles sending fake messages to other vehicles in order to disrupt traffic.

4.1.3 Signcryption

Our protocol uses a signcryption scheme and a group signature scheme. The signcryption scheme is used to help a vehicle to receive a secret member key from an RSU secretly. Signcryption [Zhen97], is a public-key primitive which has the ingredients of both digital signature and data encryption. A signcryption scheme allows a sender to simultaneously sign and encrypt a message. An attractive point is that it takes less computational time and it has a lower message expansion rate than the sign-then-encrypt procedure [Zhen97].

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

The basic requirements for a signcryption scheme are that it should satisfy the properties of *message confidentiality* and *signature unforgeability*.

- **Message confidentiality.** It allows the communicating parties to preserve the secrecy of their exchanges. This property can be used to fulfill the "*confidential communication*" requirement in VANETs.

- **Signature unforgeability.** A signcryption scheme offering non-repudiation prevents the sender of a signcrypted message from repudiating her signature. This can fulfill the "*message authentication*" requirement in VANETs.

Privacy is an important concern in VANETs. The signcryption scheme should also satisfy the "*ciphertext anonymity*" property that is defined by Boyen [Boye03]. *Ciphertext anonymity* captures the property that the ciphertext must contain no information in the clear that identifies the sender or recipient of the message.

- **Ciphertext anonymity.** A ciphertext should look anonymous to everyone but the actual recipient. The identities of both the sender and the recipient of the ciphertext should stay hidden from third parties. The "*privacy protection*" requirement in VANETs can be satisfied by this property.

The signcryption scheme in [Li07] is shown to satisfy *message confidentiality*, *signature unforgeability* and *ciphertext anonymity*. We employ this signcryption scheme to help a vehicle to safely receive secret member keys from RSUs.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

4.1.4 Group signature

In our system, after receiving a secret member key from an RSU, each vehicle can anonymously send messages on behalf of the group maintained by this RSU, by using a group signature scheme. Group signatures [Chau91] allow the members of a group to sign on behalf of the group. Everyone can verify the signature with a group public key while no one can know the identity of the signer except the the opener (In our protocol, the TM acts as the opener). Further, it is computationally hard to decide whether two different signatures were issued by the same member. We employ a group signature scheme to secure V2V communications.

Due to the security requirements of VANETs, the group signature scheme employed should satisfy the following properties:

- **Unforgeability.** Only the group members can sign messages on behalf of the group. This fulfills the "*message authentication*" requirement in VANETs.

- **Unlinkability.** Deciding whether two different valid signatures were computed by the same group member is computationally hard for anyone except the opener. This can deal with the "*privacy protection*" requirement in VANETs.

- **Traceability.** The opener (TM) is always able to open a valid signature and identify the signer. It can use this property to address the "*anonymity revocability*" requirement in VANETs.

Our protocol employs the signcryption scheme defined in [Li07] and the group signature scheme defined in [Ferr09]. The security of the signcryption is based on the co-CDH assumption in $(\mathbb{G}_1, \mathbb{G}_2)$ and the security of the

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

group signature scheme in [Ferr09] is based on the q-Strong Diffie-Hellman assumption in $(\mathbb{G}_1, \mathbb{G}_2)$ and the Decision Linear assumption in $\mathbb{G}_1$.

4.2 A robust and scalable protocol based on on-the-fly groups

In this section, we propose a concrete robust and scalable protocol based on on-the-fly groups for VANETs. This protocol employs the signcryption scheme defined in [Li07] and the group signature scheme proposed in [Ferr09] as building blocks. The signcryption scheme is used to help a vehicle to obtain a secret member key from an RSU secretly, and the group signature scheme is used for V2V communications.

4.2.1 High-level description

We outline the basic ideas in our decentralized privacy-preserving authentication protocol to secure vehicular communications. Figure 4.2 illustrates those basic ideas.

In our system, we let each RSU maintain an on-the-fly generated group consisting of vehicles that occasionally enter the RSU's communication range. The RSU will periodically broadcast its own certificate and its neighbor RSUs' certificates to the vehicles within its range. When a vehicle V passes by an RSU, if it is the first time it sees this RSU or if the vehicle's current secret member key has expired, the vehicle V and the RSU will run a KeyRequest protocol. V sends a signcrypted message ρ to the RSU to request a secret member key. When the RSU receives the request, first it de-signcrypts the

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

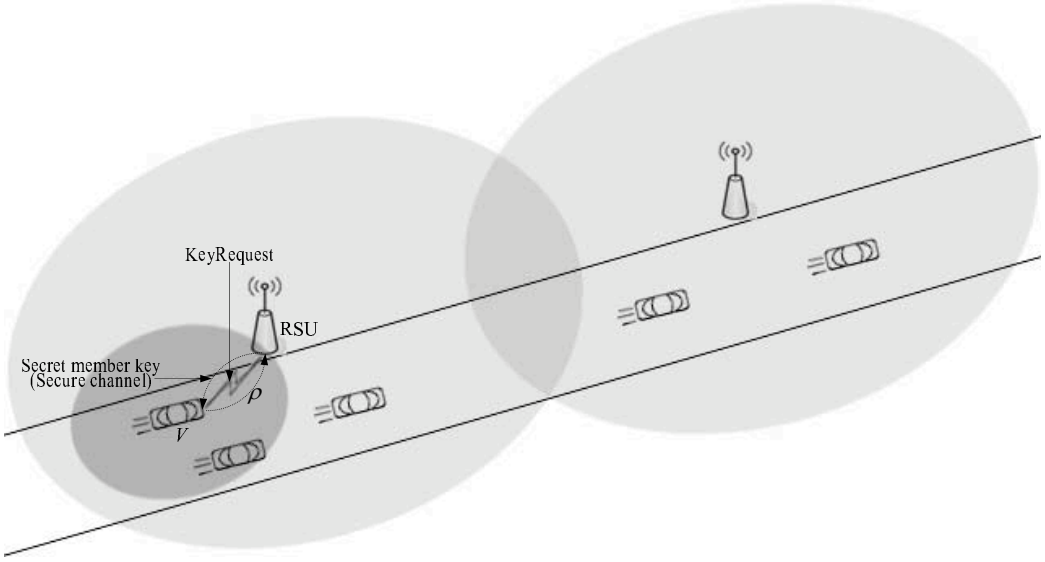

Figure 4.2: Basic ideas in the decentralized protocol

message ρ to obtain the plaintext m (which includes a session key, a timestamp, the certificate of V and a signature) and checks whether V is entitled to obtain a secret member key (*i.e.*, an anonymous group certificate), according to certain security policies to be detailed in specific implementations. If V satisfies the security criteria, a secure channel between V and the RSU will be opened and a secret member key generated by the RSU will be sent back to the vehicle V through the secure channel. After receiving the secret member key, V can anonymously sign with a group signature scheme any V2V messages during its stay within range of RSU. These signed messages can be verified by other vehicles in the areas covered by the current and neighboring RSUs. Most messages are about regular driving status information and do not need to be forwarded. In case of important messages, after verifying them, vehicles can sign again and forward them to other vehicles in the areas covered by the current RSU and its neighbors. This will allow

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

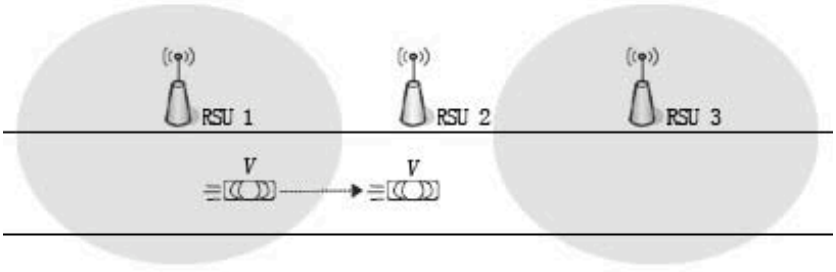

Figure 4.3: Collapsed RSU 2

important messages to be disseminated to the whole VANET.

The local processing of messages by the RSUs within range results in increased efficiency and robustness. As to efficiency, since each vehicle only verifies messages from vehicles that move into the range of the same RSU and its neighbors, it can easily check whether the anonymous sender was revoked with the help of the neighboring RSUs and does not need to retrieve the revocation list from a remote centralized authority. Regarding robustness, if some RSUs collapse, only vehicles entering the areas of those RSUs will be affected, and our protocol can still work with slight changes. For instance, as shown in Figure 4.3, assume that vehicle V has obtained the secret member key from RSU 1 and it is now in the cover range of RSU 2, which has collapsed. In this case, V can still use the secret member key from RSU 1 to sign the messages before it can join the group maintained by RSU 3; and RSU 1/3 only needs to broadcast a notification and the certificates of RSU 3/1 in its area as well. This mechanism may slightly decrease the security of the VANET in the case that a vehicle cannot get the up-to-date certificates of nearby RSUs (this problem can be alleviated by requesting the updated certificates from other vehicles, using a multi-hop mechanism).

We note that, in the early stages of VANET deployment, RSUs may not

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

be densely distributed. They are more likely to be deployed in metropolitan areas which suffer from heavy traffic. It seems reasonable to assume that there will be some sporadic RSUs in the early stage of VANETs, although the density of RSUs might not be very high. In this case, a measure similar to that in the above paragraph can be used to alleviate the dependence of RSUs. Finally, if the density of vehicles in an area is extremely low, similarly to the centralized group signature-based protocol in [Lin07], our protocol can also be used as a centralized authentication scheme. Furthermore, in Chapter 5, we will propose a set of mechanisms to address the security, privacy, and management requirements in a large-scale VANET without the assumption of densely distributed RSUs.

4.2.2 The concrete protocol

In this section, we describe our robust and scalable protocol for secure vehicular communication in detail. Our protocol consists of five stages: *System Setup*, *Key Issuance*, *Re-Key Issuance*, *Signing*, *Batch Verification* and *Tracing*.

Before describing our protocol, we first explain the notation used to simplify the description.

▷ TA: It is a trusted authority and can be viewed as an electronic counterpart of the traffic administration office in the real world. The TA owns the system's master key which is used to issue digital certificates for vehicles and RSUs. It also maintains a Certificate Revocation List (CRL) which contains the certificates of the revoked vehicles.

▷ TM: It is the tracing manager. It can be instantiated by the traffic police. It is able to trace the identity of a vehicle having generated a certain safety message.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Table 4.1: Format of a safety message: fields and lengths

Group ID	Payload	Timestamp	Signature
2 bytes	100 bytes	4 bytes	368 bytes

▷ R_i: The i-th RSU. The responsibility of an RSU in our protocol is to issue secret member keys for vehicles.

▷ V_i: The i-th vehicle.

▷ ID_{V_i}: The identity of V_i.

▷ TP: A timestamp.

▷ $Cert_{R_i}$: The certificate of R_i.

▷ $Cert_{V_i}$: The certificate of V_i.

▷ $E_K(.)/D_K(.)$: The encryption/decryption algorithm of a symmetric-key encryption scheme, where K is a key which specifies the particular transformation of plaintext into ciphertext during encryption, or vice versa during decryption.

▷ SK: A session key that will be used as the key of $E_K(.)/D_K(.)$.

▷ $||$: The message concatenation operation.

▷ SM: A safety message. The format of a safety message sent by a vehicle is shown in Table 4.1.

The Group ID is used to identify to which group a vehicle belongs and its length is 2 bytes. Position, current time, direction, speed, acceleration/deceleration, traffic events, etc. of a vehicle are included in the message payload. According to [USDe], the length of a payload is 100 bytes. We add the timestamp into a safety message to prevent the message replay attack. The last field is the signature of the first three parts of the safety message. The length of a signature in our protocol is 368 bytes (we will elaborate on that later). Therefore, the total message length is 474 bytes.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Now we describe the *System Setup*, *Key Issuance*, *Re-Key Issuance*, *Signing*, *Batch Verification* and *Tracing* stages of our protocol in detail.

System Setup. At this stage, the TA generates the parameters for the whole system by using the TAKeyGen algorithm. Using the TMKeyGen algorithm, the TM generates its private and public keys. Similarly, each RSU or Vehicle generate their private and public keys by using RKeyGen or VKeyGen.

- TAKeyGen: TA proceeds as follows:

  1. Select $p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \psi, \hat{e}$ as Section 3.1.
  2. Choose cryptographic hash functions $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1, H_2 : \{0,1\}^* \longrightarrow \{0,1\}^f, H_3 : \{0,1\}^* \longrightarrow \mathbb{Z}_p^*$ and $E_K(.)/D_K(.)$.
  3. Publish the system parameters as

  $$params = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \psi, \hat{e}, H_1 \sim H_3, E_K(.)/D_K(.)),$$

  where f is the total length of the messages to be signcrypted. $params$ are pre-stored in the TM and in each R_i, V_i.

- TMKeyGen: Randomly select $h \in \mathbb{G}_1^*$, $x, y \in \mathbb{Z}_p^*$, and set $u, v \in \mathbb{G}_1$ such that $u^x = v^y = h$. The TM's public key is $g_{TM} = (h, u, v)$. The private key of TM is $s_{TM} = (x, y)$. TM's public key is pre-stored in each R_i, V_i.

- RKeyGen: Select $\zeta_i \in \mathbb{Z}_p^*$ at random, and compute $w_i = g_2^{\zeta_i}$. The private and public keys of an RSU R_i are ζ_i and w_i, respectively, and the corresponding certificate of R_i is $Cert_{R_i}$.

- VKeyGen: Choose a random $\xi_i \in \mathbb{Z}_p^*$, and compute $pk_{V_i} = g_2^{\xi_i}$. Vehicle V_i's private and public keys are ξ_i and pk_{V_i}, respectively, while $Cert_{V_i}$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

is V_i's certificate.

Note that the certificates of vehicles and RSUs are issued by the TA.

Key Issuance. In this stage a vehicle joins a group maintained by an RSU. An RSU is assumed to be more powerful than a vehicle, and its communication range longer. RSUs are distributed in the road side and they broadcast their certificates and the ones of their adjacent RSUs. When V_i passes by R_i, if V_i is already a member of the current group maintained by R_i, then R_i does nothing. Otherwise, V_i requests a secret member key from R_i by using the KeyRequest protocol:

- KeyRequest: This is an interactive protocol run between V_i and R_i. V_i has private and public keys ξ_i and pk_{V_i}, respectively, and certificate $Cert_{V_i}$; R_i has private and public keys ζ_i and w_i, respectively, and certificate $Cert_{R_i}$. This protocol employs the signcryption scheme described in [Li07] and consists of three steps:

  1. At this step, V_i takes as input $SK, TP, Cert_{V_i}, \xi_i$ to generate a signcrypted message and sends the signcrypted message to R_i. To do this, V_i does the following:

     (a) Choose a session key SK.

     (b) Select a random $r \in \mathbb{Z}_p^*$, and compute

     $$\begin{cases} s = g_1^r \\ \sigma = H_1(SK||Cert_{V_i}||TP||s||w_i||\psi(w_i^r))^{\xi_i} \\ \varphi = (SK||TP||Cert_{V_i}||\sigma) \oplus H_2(s||w_i||\psi(w_i^r)). \end{cases}$$

     (c) Send $\rho = (s, \varphi)$ to R_i.

  2. After receiving $\rho = (s, \varphi)$ from V_i, R_i first de-signcrypts ρ to get the plaintext. It checks the validity of the signature and the

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

certificate in the plaintext. If they are valid, a secure channel between R_i and V_i is opened. Through this secure channel, a secret member key will be returned to V_i. The concrete procedure is as follows

(a) Compute the plain text

$$(SK||TP||Cert_{V_i}||\sigma) = \varphi \oplus H_2(s||w_i||s^{\zeta_i}).$$

(b) Check the validity of $Cert_{V_i}$. If it is invalid, 'abort'; otherwise, extract pk_{V_i} from $Cert_{V_i}$.

(c) Verify the signature by checking

$$\hat{e}(\sigma, g_2) \stackrel{?}{=} \hat{e}(H_1(SK||Cert_{V_i}||TP||s||w_i||s^{\zeta_i}), pk_{V_i}).$$

If the check is satisfied, using ζ_i, generate a tuple (η_i, θ_i): select $\theta_i \in \mathbb{Z}_p^*$, and set

$$\eta_i = g_1^{\frac{1}{\zeta_i + \theta_i}}.$$

Otherwise, 'abort'.

(d) Compute $\kappa = E_{SK}((TP||\eta_i||\theta_i))$ and send κ to V_i.

(e) Store $(Cert_{V_i}, \eta_i)$ to R_i's database.

3. When V_i receives κ from R_i, it computes $(TP'||\eta_i||\theta_i) = D_{SK}(\kappa)$. If $TP = TP'$, V_i accepts the secret member key (η_i, θ_i), where TP is the timestamp used by V_i in the first step.

Note that, to further enhance the anonymity of a vehicle and reduce the frequency of interaction between vehicles and RSUs, we can let several

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

seriate RSUs (*e.g.*, all the RSUs along the same street) to share the same private/public key.

Re-Key Issuance. A vehicle V_i can revoke its certificate $Cert_{V_i}$ for some reasons, for example when its private key has been stolen. If this happens, to ensure the security of the VANET, the RSUs whose databases contain $Cert_{V_i}$ should update their private/public keys as well as their certificates. Specifically, if an RSU R_i finds that there is a certificate $Cert_{V_i}$ in the CRL and $(Cert_{V_j}, \eta_j)$ on R_i's database such that $Cert_{V_i} = Cert_{V_j}$, R_i runs the following ReKey protocol.

- ReKey: This protocol consists of the following steps:

  1. R_i first runs RKeyGen to generate a new private/public key pair (ζ_i', w_i') and the corresponding certificate $Cert'_{R_i}$. After this step, the public key of the group maintained by R_i is updated to w_i'.
  2. Then R_i broadcasts within its communication range its new certificate and a lifetime (during this lifetime, both the new certificate and the old certificate of R_i are considered valid).
  3. When a vehicle V_i receives the above messages from R_i, it should launch the KeyRequest protocol used in the *Key Issuance* stage to request a fresh secret member key corresponding to the new public key w_i' of R_i.

Signing. As mentioned above, if a vehicle broadcasts a message M (M = Group ID|| Payload||Timestamp) directly without any secure mechanism, VANETs may suffer from some serious attacks. To avoid or detect those attacks and simultaneously protect the privacy of users, we use the group signature scheme proposed by Ferrara *et al.* in [Ferr09]. Before sending a message M, V_i first signs it by using the following VBSign algorithm:

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

- VBSign: Let $(\eta_i||\theta_i)$ be V_i's secret member key, V_i computes the group signature π_{V_i} on M as follows

  1. Randomly select $\alpha, \beta \in \mathbb{Z}_p^*$ and compute

$$\begin{cases} T_1 = u^{\alpha} \\ T_2 = v^{\beta} \\ T_3 = \eta_i h^{(\alpha+\beta)} \\ \gamma_1 = \theta_i \alpha \\ \gamma_2 = \theta_i \beta \end{cases}$$

  2. Select $r_\alpha, r_\beta, r_\theta, r_{\gamma_1}, r_{\gamma_2} \in \mathbb{Z}_p^*$ at random, compute

$$\begin{cases} R_1 = u^{r_\alpha} \\ R_2 = v^{r_\beta} \\ R_3 = \hat{e}(T_3, g_2)^{r_\theta} \hat{e}(h, w_i)^{-r_\alpha - r_\beta} \hat{e}(h, g_2)^{-r_{\gamma_1} - r_{\gamma_2}} \\ R_4 = T_1^{r_\theta} u^{-r_{\gamma_1}} \\ R_5 = T_2^{r_\theta} v^{-\gamma_2}. \end{cases}$$

  3. Compute $c = H_3(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$.

  4. Compute

$$\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_\theta = r_\theta + c\theta_i \\ s_{\gamma_1} = r_{\gamma_1} + c\gamma_1 \\ s_{\gamma_2} = r_{\gamma_2} + c\gamma_2 \end{cases}$$

  5. Output the group signature

$$\pi_{V_i} = (T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, s_\alpha, s_\beta, s_\theta, s_{\gamma_1}, s_{\gamma_2}).$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Batch Verification. A vehicle may receive many safety-related messages from other vehicles in a very short time. Before accepting these safety messages, it should first verify their validity by checking the signatures of the safety messages. As remarked in [Wu10], fast validation of vehicular messages is crucial for a wide deployment of VANETs in practice. To meet this requirement, we use the batch verification technique described in Section 3.3. When a vehicle receives safety messages from other vehicles in the group maintained by R_i whose public key is w_i, it runs the following VBVerify algorithm to check the validity of these safety messages.

- VBVerify: Assuming a vehicle should verify n safety messages at the same time. Let

$$\pi_j = (T_{1,j}, T_{2,j}, T_{3,j}, R_{1,j}, R_{2,j}, R_{3,j}, R_{4,j}, R_{5,j}, s_{\alpha,j}, s_{\beta,j}, s_{\theta,j}, s_{\gamma_1,j}, s_{\gamma_2,j})$$

be the signature on the message M_j in the j-th safety message. For each $j = 1, ..., n$, first compute

$$c_j = H_3(M_j, T_{1,j}, T_{2,j}, T_{3,j}, R_{1,j}, R_{2,j}, R_{3,j}, R_{4,j}, R_{5,j})$$

and take random width-w non-adjacent forms (w-NAFs, [Cheo07]) $\delta_1, ..., \delta_n$, to batch verify the following bilinear map-based equation

$$\prod_{j=1}^{n} R_{3,j}^{\delta_j} \stackrel{?}{=} \hat{e}(\prod_{j=1}^{n} (T_{3,j}^{s_{\theta,j}\delta_j} h^{(-s_{\gamma_1,j}-s_{\gamma_2,j})\delta_j} g_1^{-c_j\delta_j}), g_2) \cdot \hat{e}(\prod_{j=1}^{n} (h^{(-s_{\alpha,j}-s_{\beta,j})\delta_j} T_3^{c_j\delta_j}), w_i).$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Then verify the validity of the following non-bilinear map equations,

$$\begin{cases} u^{s_{\theta,j}} \stackrel{?}{=} T_{1,j}^{c_j} \\ v^{s_{\beta,j}} \stackrel{?}{=} T_{2,j}^{c_j} R_{2,j} \\ T_{1,j}^{s_{\theta,j}} u^{-s_{\gamma_1,j}} \stackrel{?}{=} R_{4,j} \\ T_{2,j}^{s_{\theta,j}} v^{-s_{\gamma_2,j}} \stackrel{?}{=} R_{5,j} \end{cases}$$

by picking random w-NAFs [Cheo07] $\varrho_{1,1}, ..., \varrho_{1,n}$; $\varrho_{2,1}, ..., \varrho_{2,n}$; $\varrho_{3,1}, ..., \varrho_{3,n}$; $\varrho_{4,1}, ..., \varrho_{4,n}$ and batch verifying

$$\prod_{j=1}^{n} (u^{s_{\theta,j}\varrho_{1,j}} T_{1,j}^{-c_j\varrho_{1,j}} v^{s_{\beta,j}\varrho_{2,j}} T_{2,j}^{-c_j\varrho_{2,j}} R_{2,j}^{-\varrho_{2,j}} T_{1,j}^{s_{\theta,j}\varrho_{3,j}} u^{-s_{\gamma_1,j}\varrho_{3,j}} \cdot R_{4,j}^{-\varrho_{3,j}} T_{2,j}^{s_{\theta,j}\varrho_{4,j}} v^{-s_{\gamma_2,j}\varrho_{4,j}} R_{5,j}^{-\varrho_{4,j}}) \stackrel{?}{=} 1.$$

Finally, accept the safety messages if and only if all checks succeed.

The bilinear map operation is the most time-consuming operation in the above VBVerify algorithm. Using the batch verification technique requires only two (rather than $2n$) bilinear map operations. In addition to saving in bilinear map computation, the above batch verification performs approximately 4.8 times faster than the individual verifications [Cheo07].

Tracing. Malicious entities (vehicles) may exist in VANETs. They may send fake messages to other vehicles to influence the traffic. If this happens, the TM can disclose the identity of the actual sender by invoking the following Open algorithm.

- Open: This algorithm is used by TM to trace a signature included in a safety message. Let

$$\pi_{V_i} = (T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, s_\alpha, s_\beta, s_\theta, s_{\gamma_1}, s_{\gamma_2})$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

be a valid signature on M_i under an RSU's public key w_i (according to the group ID in M_i, TM can download the public key of the corresponding RSU from TA). TM proceeds as follows:

1. Recover the vehicle's η_i as $\eta_i = T_3/(T_1^x \cdot T_2^y)$.
2. Get $(Cert_{V_i}, \eta_i)$ from RSU's database.
3. Extract ID_{V_i} from $Cert_{V_i}$.

4.3 Security analysis

In this section, we analyze the security of the proposed protocol. We will show that our protocol meets all the security requirements described in Section 4.1.2.

We first consider the scenario of a confidential communication between a vehicle and an RSU. It can be divided in two phases.

- The first is the vehicle-to-RSU communication phase. This scenario has three security requirements: *confidential communication*, *message authentication* and *privacy protection*. In this phase, a vehicle V_i that wants to join a group maintained by R_i, first selects a session key, generates a ciphertext ρ by using a signcryption scheme which takes as input the session key, a timestamp TP, etc.; then V_i sends ρ to R_i. Since the signcryption scheme we choose satisfies the *message confidentiality*, *signature unforgeability* and *ciphertext anonymity* properties which provide *confidential communication*, *message authentication* and *privacy protection*, respectively, it is easy to see that the communications in this phase meet the desired security requirements in VANETs.

- The second phase is the RSU-to-vehicle communication. This scenario

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

also has three security requirements: *confidential communication*, *message authentication* and *privacy protection*. In this phase, R_i first extracts the secret member key (η_i, θ_i) for V_i, then uses the session key SK received from V_i and the symmetric-key encryption algorithm $E_{SK}(.)$ to encrypt $(TP||\eta_i||\theta_i)$ and get the ciphertext κ, and finally sends the ciphertext κ to V_i. Since only V_i knows the corresponding session key, only V_i can decrypt $(TP'||\eta_i||\theta_i)$ from κ. Therefore, the *confidential communication* requirement is guaranteed. Furthermore, the session key is only used once. Hence, *privacy protection* is also satisfied. After getting $(TP'||\eta_i||\theta_i)$, V_i checks $TP \stackrel{?}{=} TP'$. This is used to fulfill the *message authentication* requirement.

Finally, we turn to the V2V communication scenario. The security requirements of *message authentication*, *privacy protection* and *anonymity revocability* should hold in this scenario. Here, the group signature scheme is used in our protocol and the group signature has the *unforgeability*, *unlinkability* and *traceability* properties which ensure *message authentication*, *privacy protection* and *anonymity revocability*, respectively. Hence, the desired security requirements for this scenario are naturally fulfilled.

4.4 Performance evaluation

In this section, we evaluate the performance of our protocol by comparing it with the up-to-date protocols GSIS [Lin07] and ECPP [Lu08], which offer similar security and privacy properties.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

4.4.1 Transmission overhead of safety messages

According to DSRC [DSRC], a vehicle sends each message with a time interval from 100 to 300 ms. and the minimal data rate in DSRC is 6 Mbps (for safety messaging it is typically 12 Mbps). In the following, we will consider two scenarios. Our analyses show that our protocol is practical in both of them.

First, we consider a six-lane two-way highway, each lane being 3 m wide. We assume a uniform presence of vehicles, with an inter-vehicle space of 30 m. Vehicles are in movement and transmit DSRC safety messages every 300 ms over a 300 m communication range. According to [Raya07], a vehicle can hear at most 120 vehicles per 300 ms, which amounts to a system throughput of 1.45 Mbps ($\frac{120\times3.33\times474\times8}{1024\times1024}$ Mbps). This throughput is much smaller than 6 Mbps.

Second, we consider the same highway but this time vehicles are very slow or even stopped (*i.e.* a congestion scenario). The vehicles are separated by 5 m (including the vehicle length). Each vehicle transmits a safety message over a range of 15 m every 100 ms. In the worst case [Raya07], a vehicle can hear at most 36 other vehicles per 100 ms. Hence, we have a maximal throughput of 1.30 Mbps ($\frac{36\times10\times474\times8}{1024\times1024}$ Mbps), which is also smaller than the minimum bandwidth available of 6 Mbps.

4.4.2 RSU service efficiency

In this section, we compare the RSU service efficiency (the cost for a vehicle to receive a secret member key or a short-time anonymous certificate from an RSU) of our protocol with the ECPP protocol.

According to the execution time results shown in [Scot07], the measured

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Table 4.2: RSU service efficiency

	T_V	T_R	Rounds
ECPP	3 ms ($5\tau_e$)	10.2 ms ($2\tau_m, 2\tau_e$)	2
Our Protocol	1.8 ms ($3\tau_e$)	10.2 ms ($2\tau_m, 2\tau_e$)	1

processing time[2] for one bilinear map operation (τ_m) is about 4.5 ms and the time for one point exponentiation (τ_e) is about 0.6 ms. In the sequel, we denote by T_V the computation overhead of a vehicle and by T_R the computation overhead of an RSU.

From Table 4.2, regarding the computational cost, we can find that the RSU service efficiency of our protocol is slightly better than the efficiency of the ECPP protocol in [Lu08]. In addition, our protocol is round-efficient. To obtain a secret member key from an RSU, our protocol requires only one round, while the ECPP requires two rounds (for a short-time anonymous certificate). A two-round protocol causes more delay than a single-round one. Sometimes, a vehicle may pass by an RSU at a very high speed. Hence, if a two-round protocol is used, the vehicle may not receive the secret member key or the short-time anonymous certificate in time.

4.4.3 Computational overhead of signature verification

This section compares the computational overhead of signature verification in our protocol with that in ECPP and GSIS (V2V communication scenario).

With our protocol, to verify n safety messages (essentially, to verify n signatures in n safety messages) from the same group, the required time cost

[2]For an MNT curve [Miya01] of embedding degree $k = 6$ and 160-bit q, and an implementation run on an Intel Pentium IV 3.0 GHZ machine.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

is

$$T_o = 2\tau_m + \frac{14n\tau_e}{4.8} = 2 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms.}$$

Generally, a vehicle may receive safety messages from at most two groups. The required time cost to verify n safety messages from two different groups is

$$T'_o = 4\tau_m + \frac{14n\tau_e}{4.8} = 4 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms.}$$

With ECPP, to verify n safety messages, the time cost is

$$T_E = 3n\tau_m + 11n\tau_e = 3n \times 4.5 + 11n \times 0.6 \text{ ms.}$$

With GSIS, the time cost of verifying n safety messages increases with the number of revoked certificates of vehicles in the revocation list. It is fair to compare our protocol with GSIS when the revocation list is empty. In this case, the computation time of signature verification with GSIS is

$$T_G = 5n\tau_m + 12n\tau_e = 5n \times 4.5 + 11n \times 0.6 \text{ ms.}$$

Figure 4.4 shows the time cost ratio $T1 = T_o/T_E$ and $T2 = T_o/T_G$. Figure 4.5 shows the time cost ratio $T3 = T'_o/T_E$ and $T4 = T'_o/T_G$.

From Figures 4.4 and 4.5, it is apparent that the computational overhead of signature verification in our protocol is always much lower than that in [Lin07, Lu08]. This advantage of our protocol is more obvious when the number of vehicles within the communication range grows. In VANETs, vehicles broadcast safety messages every 100-300 ms to other vehicles. In this way, a vehicle may receive lots of safety messages from other vehicles in a very short period of time. Hence, the efficiency of the signature verification is vital when the number of vehicles within the communication range is high. In [Lin07],

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

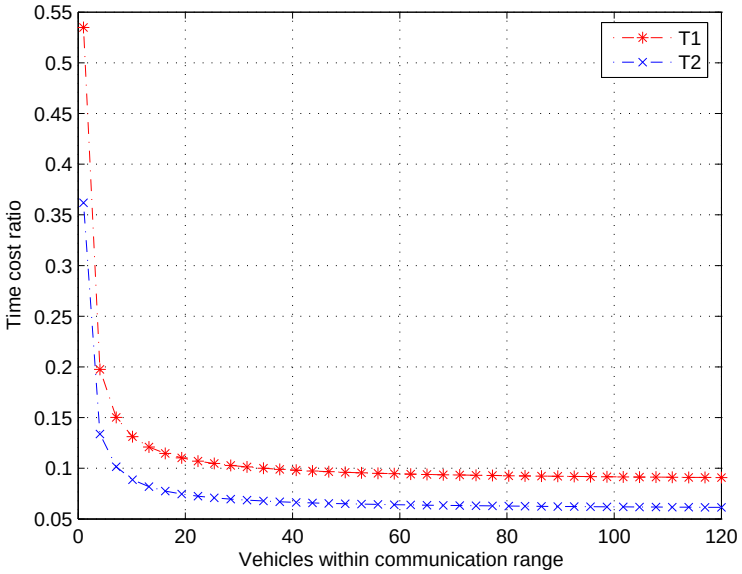

Figure 4.4: Time efficiency ratio $T1 = T_o/T_E$ and $T2 = T_o/T_G$

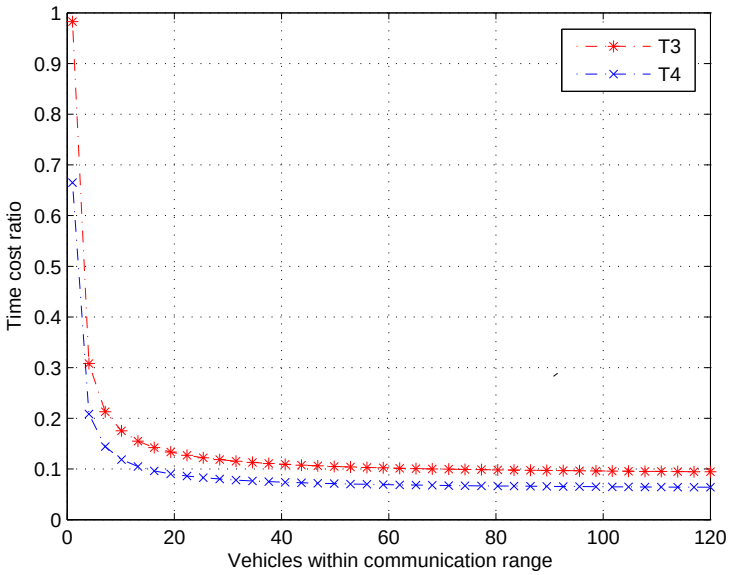

Figure 4.5: Time efficiency ratio $T3 = T'_o/T_E$ and $T4 = T'_o/T_G$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

the group signature can only be verified one by one, while in [Lu08], before verifying a signature from a vehicle, one should first verify the short-time anonymous certificate of the vehicle. In contrast, in our protocol, no short-time anonymous certificates are required and the batch verification technique is used. This largely improves the efficiency of our signature verification.

4.4.4 Simulation

In this section, by using NS-2 [NS2], we carry out some simulations to evaluate the average message delay and message loss rate to determine the practical performance of our protocol. In our simulations, the road scenario considered covers an area of 1×1 km^2 and is shown in Figure 4.6. The vehicles were generated at random and their average speed was 56 km/h, which is typical in urban areas. The communication range of each vehicle is from 10 m to 300 m. The channel bandwidth bound is 6 Mbps and the packet size is 474 bytes (see Section 4.2.2). For each experiment, the simulation time is 200 s. In addition, since the communication range of an RSU is much longer than the one of a vehicle, for most cases, a vehicle only verifies safety messages from the members in the same on-the-fly group. As shown in Section 4.4.3, to verify n safety messages, the required time cost is

$$T_o = 2 \times 4.5 + \frac{14n \times 0.6}{4.8} \text{ ms.}$$

The average message delay D_{msg} is defined as follows [Wu10]:

$$D_{msg} = \frac{1}{L_{\mathbb{D}}} \sum_{\ell \in \mathbb{D}} \left(\frac{1}{M_{\ell_{\rightarrow}}} \sum_{m=1}^{M_{\ell_{\rightarrow}}} \left(T_{\overrightarrow{sgn}}^{\ell_m} + \frac{1}{K_\ell} \sum_{k=1}^{K_\ell} \left(T_{\overrightarrow{trnsmsn}}^{\ell_m k} + \sum_{j=1}^{\lceil MAD/\tau \rceil} j P_{m,j} \tau \right) \right) \right),$$

where $\mathbb{D}$ is the sample district in the simulation, $L_{\mathbb{D}}$ is the number of vehicles

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

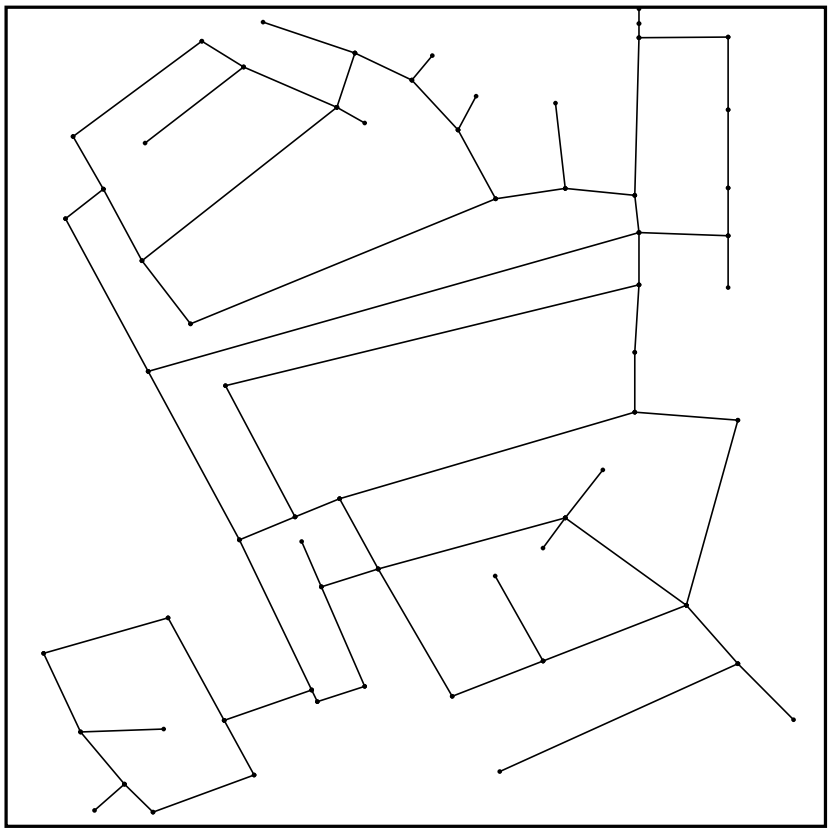

Figure 4.6: Road scenario corresponding to a square area of size 1×1 km^2

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

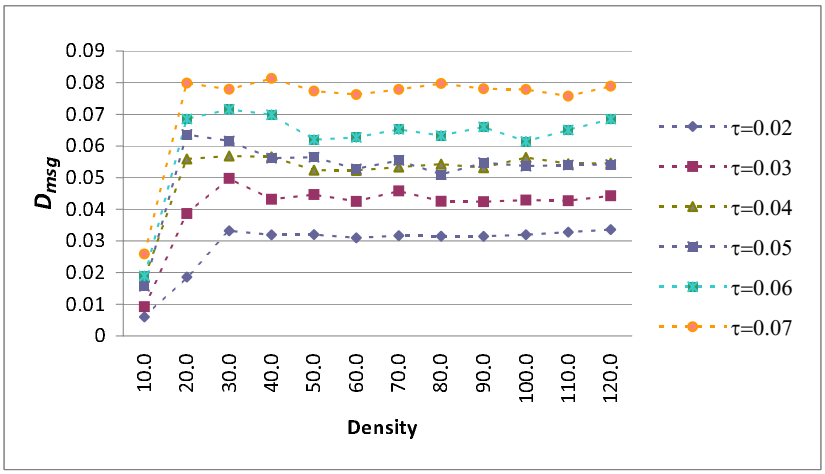

Figure 4.7: Impact of authentication on message delay

in $\mathbb{D}$, $M_{\ell\rightarrow}$ is the number of messages sent by vehicle ℓ, K_ℓ is the number of vehicles within a one-hop communication range of vehicle ℓ, $T_{sgn}^{\ell_m}$ is the time taken by vehicle ℓ to sign message m, $T_{trnsmsn}^{\ell_m k}$ is the time taken to transmit message m from vehicle ℓ to vehicle k, τ is the time period taken to perform a batch verification and MAD is the maximum allowable delay for end-to-end message transmissions. According to [European], MAD is 100ms. $P_{m,j} = \frac{v_{m,j}}{V_m}$, where V_m is the total number of vehicles processing m among the K_ℓ vehicles, and $v_{m,j}$ is the number of vehicles processing m in the interval $((j-1)\tau, j\tau]$ for $j\tau \leq MAD$. Clearly, we have that $V_m = \sum v_{m,j}$.

The average message delay D_{msg} reflects the average time latency for a message to be processed and must be smaller than MAD. Figure 4.7 shows the relationship between D_{msg}, the vehicle density and the batch verification period τ. From this figure, one can see that, for a fixed vehicle density, D_{msg} increases with τ. For a fixed τ, in the case of very low density, D_{msg} sharply grows when the vehicle density is increased from 10/km^2 to 30/km^2.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

However, the delay stabilizes for vehicle densities above 30/km^2. These experimental results seem to contradict the intuition that the delay will keep increasing as more messages will be received for verification. We observe that such a stable curve is due to the fact that most received messages can be verified in batch, and the average message delay does not increase for larger densities. We also note that, for all combinations of different densities and batch verification intervals, the average message delay is lower than $MAD = 100$ ms, which implies that our protocol works well for various traffic environments.

When the arriving messages surpass the processing capacity of the vehicle in a batch verification period, some messages cannot be verified, which results in message loss due to the authentication mechanism. The average message loss (induced by cryptographic operations) rate can be computed as follows:

$$R_{loss} = 1 - \frac{1}{L_{\mathbb{D}}} \sum_{v_i \in \mathbb{D}} \frac{n_\tau}{n_{v_i}}$$

where n_τ is the maximum number of messages that a vehicle can verify in a given batch period τ, n_{v_i} is the number of messages that a vehicle v_i receives for verification in a given batch period τ. If $n_{v_i} \leq n_\tau$, then we set $\frac{n_\tau}{n_{v_i}} := 1$.

Figure 4.8 shows that, when $\tau = 0.02$ s and 0.03 s, R_{loss} increases as the vehicle density grows and, when $\tau \geq 0.04$ s, R_{loss} is almost 0 for a density between 0 vehicles/km^2 and 120 vehicles/km^2. This is because that when τ is small, only a few messages are received in a batch period, and the advantage of batch verification is not well exploited; when τ and the vehicle density grow, the messages received in τ also grow. However, the arriving message growth rate cannot surpass the message processing capacity which also grows with τ.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

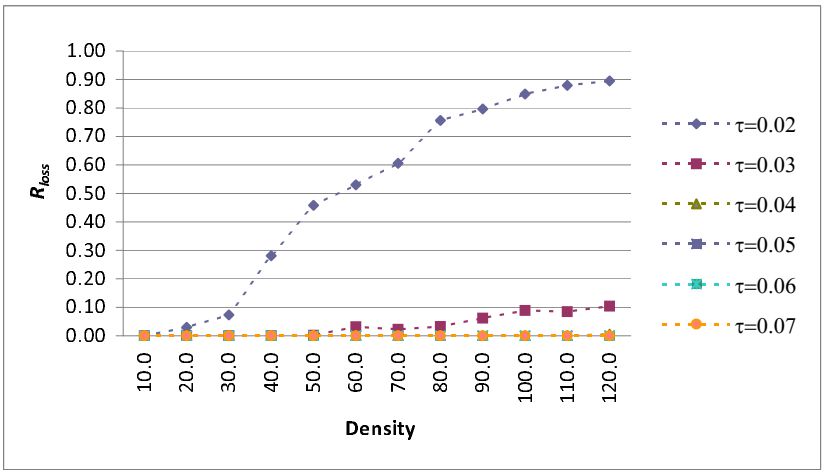

Figure 4.8: Impact of authentication on message loss rate

From the results illustrated in Figures 4.7 and 4.8, one may find that there is a conflict between the average message delay D_{msg} and the average message loss rate R_{loss}. We expect low average message delay as lower latency implies that vehicles can take less time to respond to the traffic environment changes. To obtain lower average message delay, the batch verification interval τ should be as small as possible. However, if τ is too small, some messages cannot be verified and the average message loss rate grows. Hence, a balance point has to be found, and from Figure 4.7 and 4.8, $\tau = 0.05$ s might be an ideal balance point.

4.5 Summary

A number of challenges such as efficient certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong dependence on tamper-proof devices arise in existing protocols for securing VANETs. We have proposed a new privacy-preserving

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

authentication protocol that efficiently addresses those challenges by considering the special features of vehicular mobility, road limitations and densely distributed RSUs in VANETs. In our system, each RSU maintains an on-the-fly generated group within its communication range, in which vehicles can anonymously generate V2V messages, and verify anonymous V2V messages from other vehicles. Vehicles generating false/bogus messages can be traced by a third party. Our scheme has been shown to be robust, scalable and practical. Furthermore, it clearly outperforms state-of-the-art alternatives in the case of dense traffic.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 5

Conciliating Liability and Privacy for Large-Scale VANETs

At the early stage of VANET deployment, the RSUs may not be well distributed. In this chapter, we propose a set of mechanisms to address the security, privacy, and management requirements of a large-scale VANET without the assumption of densely distributed RSUs. The conflicting requirements are conciliated by exploiting identity-based group signatures (IBGSs). IBGSs allow us to divide a large-scale VANET into a number of easy-to-manage smaller groups. This feature greatly reduces the security-related management challenges.

In the system, each party, including the group managers (*i.e.*, the transportation offices) and the signers (*i.e.*, the vehicles), has a unique, human-recognizable identity as its public key, and a corresponding secret key generated by some trusted escrow authority. For instance, the public keys of

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

the administration offices, road-side units [Lee99] and vehicles can be, respectively, the administration name, the RSU geographical address and the traditional vehicle license plate. This eliminates the overhead of managing public key certificates in VANETs: certificates are no longer needed because the public key of each party is a human-recognizable identity. After registering to transportation offices, any vehicle can anonymously authenticate any message which can be verified by the identities (*e.g.*, the name) of the transportation offices and the public key of the escrow authority. If the message is later found to be false, the identity of the message generator can be traced by traffic police offices.

We present a number of approaches to further improve the robustness and efficiency of the system. First, threshold secret sharing techniques are employed in the key generation procedure so that the system can securely work even if some trusted authorities collapse or are disabled by attackers. This makes the system robust and avoids the so-called single-point of failure problem of centralized systems. Second, given that emergency announcements need to be processed as soon as possible, we present an emergency authentication mechanism which introduces almost no delay. This is realized by an offline signing technique which allows pre-authenticating messages in the idle time to minimize the online processing time. Third, considering the redundancy in vehicular communications, we present a selfish verification mechanism to speed up message processing in VANETs. With this technique, although each vehicle may receive a large number of messages, the vehicle only selects for verification those messages affecting its traffic decisions. The selected messages are verified with the batch verification technique in Section 3.3 which can verify a batch of messages as if they were a single one. These mechanisms accelerating message processing are crucial to deploy

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

VANETs in densely populated urban areas.

The remainder of the chapter is organized as follows. A high-level description of our protocol is provided in Section 5.1. We propose a basic protocol in Section 5.2 and extend it in Section 5.3. Simulations are reported in Section 5.4 to evaluate the performance of our proposals. Section 5.5 is a summary.

5.1 High-level description of the system

In this section, we give an overview of the proposed system.

5.1.1 Security requirements

In order to obtain an implementable system to enhance the trustworthiness in V2V communications by conciliating public safety and vehicle privacy, we consider the following three types of security requirements:

- **Liability.** Most attackers of VANETs can be assumed rational, but there may also exist irrational attackers whose behavior cannot be predicted. Judicial deterrence or financial penalties can be effective countermeasures to thwart rational attackers. Although irrational attacks cannot be prevented, mechanisms can be devised to relieve the damage, *e.g.*, financial compensations. Hence, the fundamental security functions in vehicular communications will consist of ensuring liability for the originator of a data packet. Liability implies that the message author has to be responsible for the message generated. To establish liability without disputes, authentication, integrity and non-repudiation must be provided in vehicular protocols. Authentication allows verifying that the message was generated by the originator as claimed, rather

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

than by an impersonator. Integrity guarantees that the message has not been tampered with after it was sent. Non-repudiation implies that the message generator cannot deny message authorship.

- **Anonymity.** There is anonymity if, by monitoring the communication in a VANET, message originators cannot be identified, except perhaps by designated parties. The goal is to protect the privacy of vehicles. Since message authentication requires knowledge of a public identity such as a public key or the license plate, if no anonymity was provided, an attacker could easily trace any vehicle by monitoring the VANET communication. This would be surely undesirable for the drivers.

- **Revocability.** Revocability means that, if necessary, designated parties can identify the originator of any doubtable message. The goal here is to conciliate personal privacy and public safety. If anonymity is realized without any revocability mechanism, an attacker can anonymously broadcast authenticated wrong messages to fool other vehicles without fear of being caught, which contradicts the liability requirement and may seriously compromise public safety. Revocability is critical to provide judicial arguments for law enforcement investigation and accident reconstruction.

5.1.2 A framework using identity-based group signatures

In Chapter 4, we proposed an efficient protocol for vehicle communications. However, it relies on the existence of densely distributed RSUs. There are other proposals [Guo07, Lin07] which are based on group signatures to secure VANETs with conditional privacy. For these proposals to be deployable in

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

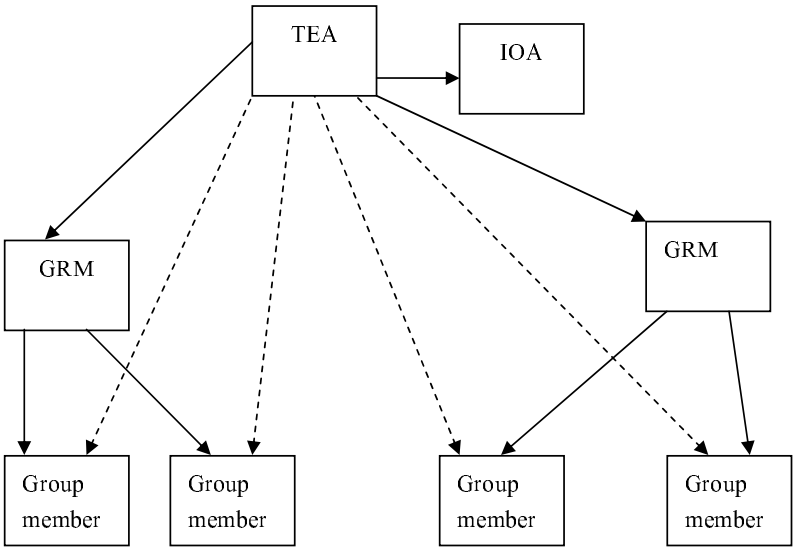

Figure 5.1: Model of identity-based group signature

metropolitan areas, they must meet several constraints. It is impractical to have millions of vehicles register to a single group, which implies that the group public parameters may change whenever any vehicle joins/leaves the system. It is resource-consuming to distribute these frequent changes to all the nodes. As suggested in those recent proposals [Guo07, Lin07], it seems reasonable to divide a large VANET into much smaller groups. A new challenge posed by this approach is how to manage these groups. For instance, how to convince each node that the group public keys are authentic and up-to-date. This is a crucial concern because the uncertainty in group public keys may cause serious security failures.

To allay the above situation and sufficiently exploit the existing transportation systems, we suggest the use of identity-based group signatures

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

(IBGS) to safeguard large VANETs. The notion of identity-based group signatures was introduced by Weil *et al.* in 2005 [Wei05]. In an IBGS scheme, there are four types of parties, *i.e.*, the trusted escrow authority (TEA), the group registration manager (GRM) (*i.e.*, issuer), an identity-opening authority (IOA) (*i.e.*, opener) and the group members, as illustrated in Figure 5.1. Each of them has a unique identity, *i.e.*, its name. TEA has a public-private key pair and the public key can be accessed by any entity. By taking as input the identity of any entity in the system, TEA generates a private key for that entity. Any group member having obtained a private key from TEA can register to GRM to become a group member and then can anonymously sign any message on behalf of the group. The signature can be verified using TEA's public key and the identities of GRM and IOA. If necessary, IOA can open the identity of the signer of any doubtable signature.

We now describe an IBGS framework to simplify the system management overhead. In most cities, the transportation administration authorities include the public security department, vehicle management bureaus and traffic police offices, who can serve as the TEA, GRMs and IOAs, respectively. The public security department's public key can be stored in each vehicle. The public keys of GRMs and IOAs are their respective identities. Each vehicle's public key is also its unique identity. GRMs and IOAs first need to contact TEA to generate their private keys and set up the corresponding administration units.

Vehicles can be divided in groups in light of their regulatory status, *e.g.*, one can distinguish groups like police cars, ambulances, fire trucks, taxis, buses, commercial vehicles, personal vehicles, etc. Observe that the number of personal cars may be very large in densely populated areas and most personal cars run around the residence of the owner. For convenience in

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

management, personal vehicles can be further divided into smaller groups according to the regions where they have registered. After contacting TEA and obtaining the private key corresponding to its identity, each vehicle can register to the GRM of the group to which it belongs.

After registration, a vehicle can authenticate messages anonymously. When receiving an authenticated message, the receiver can verify it with the stored system public key of TEA and the identity of the group the vehicle belongs to. Note here that the signing vehicle's identity is not required for validation of the signed message due to anonymity. If the verification procedure indicates that the message is authentic (but not necessarily correct), then the receiving vehicle can use it as a proof. This proof can be submitted to the traffic police office for investigation if the message is later found to be incorrect and causes any harm. If necessary, the police can open the identity of the message generator and perhaps punish him/her.

Unlike the public key in traditional cryptosystems which is a long random string that must be certified to bind it with the corresponding private key, the identity working as public key in IBGS is human-recognizable and the corresponding private key is generated with its identity and the TEA master private key. Hence, there is no need of CAs in IBGS-based VANETs. This significantly reduces the system management overhead.

5.2 Basic liability and privacy-preservation protocol

In this section, we propose an authentication protocol to enforce liability, privacy and revocability in vehicle-generated messages. Underlying is an

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

efficient IBGS scheme [Wei05] to avoid the heavy burden of certificate generation, delivery and verification in a large-scale VANET. The protocol exploits the features of existing transportation systems to simplify the system administration overhead.

5.2.1 System set-up

The TEA, *e.g.*, the public security department, generates $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \hat{e})$ as in Section 3.1. Let u_1, u_2, u_3, u_4, u_5 be randomly selected generators of $\mathbb{G}_1$. Define cryptographic hash functions $H_V : \{0,1\} \rightarrow \mathbb{G}_1$, $H_O : \{0,1\} \rightarrow \mathbb{G}_1$, $H_R : \{0,1\} \rightarrow \mathbb{Z}_p^*$, $H : \{0,1\} \rightarrow \mathbb{Z}_p^*$. The TEA's private key is a randomly chosen value $x \in \mathbb{Z}_p^*$ and its public key is $K = g_2^x \in \mathbb{G}_2$. Then the public system parameters are

$$param = (\Upsilon, u_1, \cdots, u_5, H_R, H_V, H_O, H, K)$$

which can be accessed by each party in the VANET.

5.2.2 Key generation

With this procedure, the TEA generates private keys for the group registration managers (GRMs), the identity-opening authorities (IOAs) and the individual vehicles by taking as inputs their public identities.

- On input the identity ID_R of a GRM, TEA randomly generates $r \in \mathbb{Z}_p^*$ and computes

$$A = g_2^r, x_1 = r + H_R(A||ID_R)x \mod p$$

Finally GRM gets (x_1, A), where A is an auxiliary string that can be

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

known by the vehicles in the group, and x_1 is the private key of the GRM.

- On input the identity ID_O of an IOA, TEA generates the IOA's private key by computing
$$x_0 = H_O(ID_O)^x.$$

- On input a vehicle's identity ID_V, TEA uses x to compute the vehicles's private key
$$X = H_V(ID_V)^x.$$

5.2.3 Registration to a group

With this procedure, a vehicle with identity ID_V can register to one of the groups ID_R in the VANET. Note that the vehicle does not need to contact the identity-opening authority and the registration procedure is simple.

- The vehicle firstly proves to the GRM that it knows the secret key $X = H_V(ID_V)^x$ corresponding to its identity ID_V without leaking any information on X. This can be done with the protocol due to Qin *et al.* [Qin09] to guarantee that the vehicle has identity ID_V as claimed.

- GRM randomly selects $e \in \mathbb{Z}_p^*$, and computes
$$B = (u_5/H_V(ID_V))^{1/(e+x_1)}.$$
The GRM sends the secret group certificate (B, e, A) to the vehicle via a confidential channel.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

- The vehicle accepts the certificate if and only if

$$\hat{e}(u_5, g_2) = \hat{e}(B, g_2)^e \hat{e}(B, S)\hat{e}(H_V(ID_V), g_2),$$

  where $S = AK^{H_R(A||ID_R)} = g_2^{x_1}$.

- GRM computes $W = \hat{e}(H_V(ID_V), g_2)$, and records (ID_V, B, e, W) in its local database.

5.2.4 Authentication of vehicular communications

A registered vehicle ID_V in group ID_R with secret key X and certificate (B, e, A) can anonymously sign message m while allowing the identity-opening authority IOA to open the signature. The detailed instantiation is as follows.

- The vehicle randomly selects $s_1 \in Z_p^*$, and computes

  $s_2 = es_1 \mod p$,

  $\sigma_0 = g_1^{s_1}$,

  $\sigma_1 = Xu_1^{s_1}$,

  $\sigma_2 = H_V(ID_V)u_2^{s_1}$,

  $\sigma_3 = Bu_3^{s_1}$,

  $\sigma_5 = \sigma_3^e u_4^{s_1}$.

- The vehicle randomly selects $d \in Z_p^*$ and computes

  $C_1 = \hat{e}(H_V(ID_V), g_2)\hat{e}(H_O(ID_O), K)^d$,

  $C_2 = g_2^d$.

- The vehicle randomly selects $r_1, r_2, r_3, r_4 \in \mathbb{Z}_p^*, R_1, R_2, R_3 \in \mathbb{G}_1$, and computes

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

$$\rho_0 = g_1^{r_1},$$

$$\rho_1 = R_1 u_1^{r_1},$$

$$\rho_2 = R_2 u_2^{r_1},$$

$$\rho_3 = R_3 u_3^{r_1},$$

$$\rho_4 = [\hat{e}(u_1, g_2)^{-1} \hat{e}(u_2, K)]^{r_1},$$

$$\rho_5 = \sigma_3^{r_3} u_4^{r_1},$$

$$\rho_6 = \hat{e}(u_3, g_2)^{r_2} [\hat{e}(u_3, S) \hat{e}(u_2 u_4, g_2)]^{r_1},$$

$$\rho_7 = g_2^{r_4},$$

$$\rho_8 = \hat{e}(H_O(ID_O), K)^{r_4} \hat{e}(u_2, g_2)^{-r_1}.$$

- The vehicle computes the hash challenge

$$c = H((\sigma_0, \cdots, \sigma_3, \sigma_5)||(\rho_0, \cdots, \rho_8)||A||C_1||C_2||m).$$

- The vehicle computes the responses to the hash challenge

$$z_0 = r_1 - cs_1 \mod p,$$

$$Z_1 = R_1 X^{-c},$$

$$Z_2 = R_2 H_V(ID_V)^{-c},$$

$$Z_3 = R_3 B^{-c},$$

$$z_4 = r_3 - ce \mod p,$$

$$z_5 = r_2 - cs_2 \mod p,$$

$$z_6 = r_4 - cd \mod p.$$

- The resulting signature σ on message m is:

$$\sigma = (\sigma_0, \cdots, \sigma_3, \sigma_5)||(z_0, Z_1, Z_2, Z_3, z_4, z_5, z_6)||c||A||C_1||C_2.$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

5.2.5 Message verification

Upon receiving a signature σ on message m, the receiver computes

$$\begin{aligned}
\sigma_4 &= \hat{e}(\sigma_1, g_2)^{-1}\hat{e}(\sigma_2, K) \\
\sigma_6 &= \hat{e}(u_5, g_2)^{-1}\hat{e}(\sigma_2\sigma_5, g_2)\hat{e}(\sigma_3, S) \\
\sigma_8 &= C_1 \cdot \hat{e}(\sigma_2, g_2)^{-1} \\
\rho_0 &= g_1^{z_0}\sigma_0^c \\
\rho_1 &= Z_1 u_1^{z_0}\sigma_1^c \\
\rho_2 &= Z_2 u_2^{z_0}\sigma_2^c \\
\rho_3 &= Z_3 u_3^{z_0}\sigma_3^c \\
\rho_4 &= [\hat{e}(u_1, g_2)^{-1}\hat{e}(u_2, K)]^{z_0}\sigma_4^c \\
\rho_5 &= \sigma_3^{z_4} u_4^{z_0}\sigma_5^c \\
\rho_6 &= \hat{e}(u_3, g_2)^{z_5}[\hat{e}(u_3, S)\hat{e}(u_2u_4, g_2)]^{z_0}\sigma_6^c \\
\rho_7 &= g_2^{z_6} C_2^c \\
\rho_8 &= \hat{e}(H_O(ID_O), K)^{z_6}\hat{e}(u_2, g_2)^{-z_0}\sigma_8^c \\
S &= AK^{H(A||ID_R)}
\end{aligned} \tag{5.1}$$

and checks

$$c = H((\sigma_0, \cdots, \sigma_3, \sigma_5)||(\rho_0, \cdots, \rho_8)||A||C_1||C_2||m) \tag{5.2}$$

If Equation (5.2) holds, the receiver accepts the message. Else, the message is rejected.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

5.2.6 Revoking doubtable messages

If the verifying vehicle receives a message with a valid signature but the message is doubtable, *e.g.*, a bogus message, the verifier can submit the message along with its signature to IOA. IOA can use its secret key x_0 to open the encryption in the signature σ. IOA computes

$$W = \hat{e}(H_V(ID_V), g_2) = C_1/\hat{e}(x_0, C_2)$$

and looks up W in the registration table reg. If no entry W is found, IOA reports failure for the tracing procedure, else it outputs the vehicle identity ID_V.

Regarding revocation of malicious signers in group signature-based authentication in VANETs, another subtle issue is the case that some signer's secret key was compromised (*e.g.*, stolen) for various reasons. It is a known open problem how to efficiently distinguish the compromised signers in group signatures. Some proposals suggest a public revocation list (by releasing the secret signing information of the compromised signer) and, whenever a verifier verifies a vehicular-generated message [Lin07], the verifying vehicle first checks whether the signer is in the revocation list. If the signer is in the list, then the message will be discarded. Note that the revocation list grows linearly after the system is deployed. Hence, the performance of the system degrades as time passes. Another disadvantage is that one can also determine the authorship of the messages previously signed by the compromised vehicle. Hence, the vehicle's privacy cannot be guaranteed for messages signed before it was compromised. To mitigate these disadvantages, we suggest that, when requesting the private key from TEA, each GRM's identity be appended a tag specifying the lifetime (*e.g.*, days or weeks) of the GRM's public key, *i.e.*,

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

(GRM's identity, lifetime). Before the lifetime expires, each vehicle managed by this GRM contacts the GRM and updates its secret group signing key (see Section 5.2.3). For the verifying vehicles, they can just verify the received message as in Section 5.2.5 by additionally comparing its local time with the lifetime of the GRM's public key. This mechanism is very efficient because it only affects a subgroup of vehicles, *i.e.*, the signing vehicles managed by the GRM, while the verifying vehicle (which can be any vehicle in the VANET) will not be affected. After employing this approach, an attacker can only sign messages on behalf of the compromised vehicles during a short time interval. If the signed message is false and is forwarded to IOA by the receiving vehicles, the misbehaving compromised vehicle can be located immediately and stopped by police cars.

5.2.7 Message size

A vehicle-generated message consists of six fields: (`Message Type`; `Payload`; `Timestamp`; `TTL`; `Group ID`; `Signature`). Message ID defines the message type, and the payload field may include information on the vehicle's position, direction, speed, traffic events, event time and so on. According to the DSRC standard [DSRC], the payload of a message is 100 bytes. The timestamp specifies the signature generation time, which is used to prevent replay attacks. It also ensures that an honest vehicle can report the same traffic situation at different times without being accused of multiple signatures on the same message. The TTL field is Time To Live and determines how long the message is allowed to remain in the VANET. Group ID is used to identify which group the vehicle belongs to. The signature field is the vehicle's signature on the first five fields.

We denote the subset of the first five fields by m and the set of all six

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Table 5.1: Format of vehicle-generated messages (suggested field lengths in bytes)

Mes. Type	Payload	Timestamp	TTL	Group ID	Sig.
2	100	4	1	2	460

fields[1] by M. Table 5.1 specifies the suggested length for each field. The length of vehicle-generated messages can be expressed as

$$L_M = L_{\texttt{MessageType}} + L_{\texttt{Payload}} + L_{\texttt{Timestamp}} + L_{TTL} + L_{\texttt{GroupID}} + L_{\texttt{Signature}}.$$

To provide a typical security level of 2^{80}, we can set p a 170-bit long prime and then the element in $\mathbb{G}_1$ is 171 bits long [Galb06], and $L_{sig} = 460$ bytes. Thus, from Table 5.1, $L_M = 2 + 100 + 4 + 1 + 2 + 460 = 569$ bytes.

5.2.8 Security analysis

We first analyze liability in our vehicular authentication protocol. The underlying IBGS scheme is proven non-frameable under the co-CDH assumption in $(\mathbb{G}_1, \mathbb{G}_2)$ in the sense that no player except the trusted TEA can produce a signature that can be accepted by the verification procedure and for which the tracing procedure outputs the identity of a signer who did not generate the signature, even if the attacking players are allowed to collude [Wei05]. This strong security property guarantees that, if a vehicle does not register to the VANET, it cannot generate messages accepted by other vehicles, and no vehicles, IOAs or GRMs can impersonate an innocent registered vehicle to authenticate vehicular communications. In other words, if a message is accepted as valid, it must have been generated by a single registered vehicle and not have been tampered with since it was sent. A message which

[1]It is clear from the context when a message means either the first five fields or all six fields. We do not insist on this hereafter.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

passes the verification procedure can be used as a convincing argument in accident investigation if necessary. With this feature, the liability desirable in VANETs is properly guaranteed.

The underlying IBGS scheme is shown to be anonymous under the DDH assumption in $\mathbb{G}_1$ and the co-DBDH assumption in $(\mathbb{G}_1, \mathbb{G}_2)$ [Wei05], even if there are only two signers in the group. This implies that no one except the designated IOA can distinguish messages from the various vehicles in a VANET. Thus an attacker cannot trace the vehicles by monitoring the communications in the VANET and the identity privacy of vehicles is well protected.

It is shown that the underlying IBGS is traceable under the k-CAA2 assumption in $(\mathbb{G}_1, \mathbb{G}_2)$ and no group member or set of colluding members can generate a group signature accepted by the verification procedure which is not linkable to the actual signer [Wei05]. In other words, if a vehicular message is accepted, the third-party IOA can always identify the actual message generator. This fact guarantees that cheating vehicles can always be caught by revoking their anonymity whenever fraudulent vehicular communications are detected.

5.3 Improved protocol

In this section, we propose several ways to improve the security and efficiency of the basic privacy-preserving protocol described in Section 5.2.

5.3.1 Robust key generation

In the basic protocol, a single TEA generates the private keys for all the parties. If the TEA is compromised, the whole system is jeopardized. Also, if

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

the TEA occasionally collapses, then new vehicles cannot join the system. To address such issues in the implementation, we present a robust key generation procedure with secret-sharing techniques.

We employ Shamir's (t, k)-threshold secret sharing scheme [Sham79]. Let $\mathbb{Z}_p$ be a finite field with $p > k$ and $x \in \mathbb{Z}_p$ be the secret to be shared. The master TEA picks a polynomial $p(\alpha)$ of degree at most $t-1$ at random, whose free term is the secret x, that is, $p(0) = x$. The master TEA sets its public key as $K = g_2^x \in \mathbb{G}_2$. The polynomial $p(\alpha)$ can be written as

$$p(\alpha) = s + \sum_{j=1}^{t-1} a_j \alpha^j,$$

where $a_j \in \mathbb{Z}_p$ has been randomly chosen. Each TEA_i is assigned a known index $i = 1, \cdots, k$ and the master TEA privately sends to TEA_i a share $x_i = p(i)$ and erases x and a_i after TEA_i receives x_i for $i = 1, \cdots, k$. Then any set $\mathbb{A} \subset \{1, \cdots, k\}$ of at least t TEA_i's can recover the secret $x = p(0)$ by interpolating the set of shares they hold

$$x = p(0) = \sum_{i \in \mathbb{A}} x_i \lambda_i = \sum_{i \in \mathbb{A}} x_i (\prod_{j \in \mathbb{A}}^{j \neq i} \frac{j}{j-i})$$

where $\lambda_i = \prod_{j \in \mathbb{A}}^{j \neq i} \frac{j}{j-i}$ are the Lagrange coefficients.

With the above secret-sharing technique, the set of TEA_i's can jointly generate keys for each party as follows:

- On input the identity ID_R of a GRM, TEA_i randomly generates $r_i \in \mathbb{Z}_p^*$ and computes

$$A_i = g_2^{r_i}, x_{1,i} = r_i + H_R(A||ID_R)x_i \mod p$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

After receiving t pairs $(x_{1,i}, A_i)$ from a set $\mathbb{A}$ of at least t TEA$_i$'s, GRM can recover (x_1, A) in the basic protocol as follows

$$A = \prod_{i \in \mathbb{A}} A_i^{\lambda_i} = g_2^{\sum_{i \in \mathbb{A}} \lambda_i r_i} = H_V(ID_V)^r,$$

$$x_1 = \sum_{i \in \mathbb{A}} \lambda_i x_{1,i} = r + H_R(A||ID_R)x \mod p.$$

- On input the identity ID_O of an IOA, TEA$_i$ generates a partial private key for IOA by computing

$$x_{0,i} = H_O(ID_O)^{x_i}.$$

After receiving partial private keys $x_{0,i}$ from a set $\mathbb{A}$ of at least t TEA$_i$'s, IOA can recover its full private key by computing

$$x_0 = \prod_{i \in \mathbb{A}} x_{0,i}^{\lambda_i} = H_O(ID_O)^{\sum_{i \in \mathbb{A}} \lambda_i x_i} = H_O(ID_O)^x.$$

- On input a vehicle's identity ID_V, TEA$_i$ generates a partial private key for IOA by computing

$$X_i = H_V(ID_V)^{x_i}.$$

After receiving partial private keys X_i from a set $\mathbb{A}$ of at least t TEA$_i$'s, a vehicle V can recover its full private key by computing

$$X = \prod_{i \in \mathbb{A}} X_i^{\lambda_i} = H_V(ID_V)^{\sum_{i \in \mathbb{A}} \lambda_i x_i} = H_V(ID_V)^x.$$

In the improved key generation procedure, there exist k TEAs and at

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

least $t(1 < t < k)$ of them will distributively generate the private key for each GRM, IOA and vehicle. The system can work securely even if some TEAs collapse or are compromised, provided that the number of simultaneously collapsing or compromised TEAs is at most $k - t$. These features imply that the system is robust against accidental failures and malicious attacks.

5.3.2 Emergency message generation

The DSRC standard provides an emergency vehicle subsystem (EVS) which is the communication lifeline connecting emergency personnel in the field with emergency dispatch, other emergency personnel, and other resources that support emergency response [DSRC]. In EVS, the most important issue is to generate and process emergency messages as fast as possible. We employ the chameleon hashing technique [Sham01] to accelerate online message generation. Let $\bar{g_1} = g_1^{\nu}$ be a generator of $\mathbb{G}_1$ and $\bar{H} : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$ be a regular hash function, where ν is known only by the signer while $\bar{H}$ can be publicly shared in the system. For an input $(m', \gamma') \in \{0,1\}^* \times \mathbb{Z}_p^*$, the chameleon hash $CH : \{0,1\}^* \times \mathbb{Z}_p^* \rightarrow \mathbb{G}_1$ is defined as

$$CH(m', \gamma') = g_1^{\bar{H}(m')} \bar{g_1}^{\gamma'}.$$

With the chameleon hash, a vehicle can generate the authentication message in its idle time as follows:

- During the offline stage, the vehicle randomly chooses $(m', \gamma') \in \{0,1\}^* \times \mathbb{Z}_p^*$, and computes

$$m = CH(m', \gamma') = g_1^{\bar{H}(m')} \bar{g_1}^{\gamma'}.$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Then the vehicle authenticates m as specified in the basic protocol in Section 5.2.4, except that the hash challenge should take $\bar{g_1}$ as a part of the input:

$$c = H((\sigma_0, \cdots, \sigma_3, \sigma_5)||(\rho_0, \cdots, \rho_8)||A||C_1||C_2||m||\bar{g_1}).$$

- In the online stage, if the vehicle has an emergency message $\bar{m}$ to announce, it computes

$$\bar{\gamma} = (\bar{H}(m') - \bar{H}(\bar{m}))\nu + \gamma' \mod p.$$

Then the vehicle sends $\bar{g_1}, \bar{m}, \bar{\gamma}$ and σ to other vehicles for verification.

- Upon receipt of the above data, any other vehicle can compute

$$m = CH(\bar{m}, \bar{\gamma}) = g_1^{\bar{H}(\bar{m})} \bar{g_1}^{\bar{\gamma}}$$

and verify (m, σ) as specified in the basic protocol in Section 5.2.5 except that the hash challenge check is updated accordingly as the following equation

$$c = H((\sigma_0, \cdots, \sigma_3, \sigma_5)||(\rho_0, \cdots, \rho_8)||A||C_1||C_2||m||\bar{g_1}).$$

With the above approach, the online stage is very efficient and needs only two regular hashes, two modular additions and one modular multiplication. This overhead is almost negligible compared with the exponentiations and bilinear map computations of the basic protocol. Hence the above protocol is very suitable for generation of emergency messages.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

5.3.3 Selfish batch verification

To employ the batch verification technique in Section 3.3, the basic group signature needs to be extended. That is, the extended signature is now

$$\sigma' = \sigma||(\sigma_4, \sigma_6, \sigma_8)||(\rho_0, \cdots, \rho_8)||S.$$

Clearly, this modification does not affect any security property of the group signature because $(\sigma_4, \sigma_6, \sigma_8)||(\rho_0, \cdots, \rho_8)||S$ can be reconstructed from σ (see Section 5.2.5). The receiving vehicle needs to check Equations (5.1) and (5.2).

Let the vehicle select n message-signature pairs (m_i, σ'_i) for batch verification, where $1 \leq i \leq n$ and $\sigma'_i = \sigma_i||(\sigma_{4,i}, \sigma_{6,i}, \sigma_{8,i})||(\rho_{0,i}, \cdots, \rho_{8,i})||S_i$. Then the vehicle needs to verify the following equations:

$$\sigma_{4,i}\hat{e}(\sigma_{1,i}, g_2)\hat{e}(\sigma_{2,i}^{-1}, K) = 1 \tag{5.3}$$

$$\sigma_{6,i}^{-1}\hat{e}(u_5^{-1}\sigma_{2,i}\sigma_{5,i}, g_2)\hat{e}(\sigma_{3,i}, S_i) = 1 \tag{5.4}$$

$$\rho_{4,i}^{-1}\hat{e}(u_1^{-z_{0,i}}, g_2)\hat{e}(u_2^{z_{0,i}}, K)\sigma_{4,i}^{c} = 1 \tag{5.5}$$

$$\rho_{6,i}^{-1}\hat{e}(u_3^{z_{5,i}}(u_2u_4)^{z_{0,i}}, g_2)\hat{e}(u_3^{z_{0,i}}, S_i)\sigma_{6,i}^{c_i} = 1 \tag{5.6}$$

$$\rho_{8,i}^{-1}\hat{e}(H_O(ID_{O_i})^{z_{6,i}}, K)\hat{e}(u_2^{-z_{0,i}}, g_2)\sigma_{8,i}^{c_i} = 1 \tag{5.7}$$

$$\sigma_{8,i}^{-1}C_{1,i}\hat{e}(\sigma_{2,i}^{-1}, g_2) = 1 \tag{5.8}$$

$$\rho_{0,i}^{-1}g_1^{z_0}\sigma_{0,i}^{c_i} = 1 \tag{5.9}$$

$$\rho_{1,i}^{-1}Z_{1,i}u_1^{z_{0,i}}\sigma_{1,i}^{c_i} = 1 \tag{5.10}$$

$$\rho_{2,i}^{-1}Z_{2,i}u_2^{z_{0,i}}\sigma_{2,i}^{c_i} = 1 \tag{5.11}$$

$$\rho_{3,i}^{-1} Z_{3,i} u_3^{z_{0,i}} \sigma_{3,i}^{c_i} = 1 \tag{5.12}$$

$$\rho_{5,i}^{-1} \sigma_{3,i}^{z_{4,i}} u_4^{z_{0,i}} \sigma_{5,i}^{c,i} = 1 \tag{5.13}$$

$$\rho_{7,i}^{-1} g_2^{z_{6,i}} C_{2,i}^{c_i} = 1 \tag{5.14}$$

$$S_i^{-1} A_i K^{H(A_i||ID_{R_i})} = 1 \tag{5.15}$$

and

$$c_i = H((\sigma_{0,i}, \cdots, \sigma_{3,i}, \sigma_{5,i})||(\rho_{0,i}, \cdots, \rho_{8,i})||A_i||C_{1,i}||C_{2,i}||m_i).$$

Note that Equations (5.3) to (5.7), (5.8) to (5.13) and (5.14, 5.15) are in the same finite cyclic groups $\mathbb{G}_T$, $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. Then the batch verification lemma in Section 3.3 can be applied to each of those three batches of equations. We roughly compare the overheads of individual message verification with those of batch verification. For n messages, without using the batch approach, we need $O(N)$ multi-base bilinear map computations and multi-base exponentiations, as well as n hashes. However, after the batch verification is applied, the verifying vehicle needs only $O(1)$ multi-base bilinear map computations and multi-base exponentiations, as well as n hashes. According to state-of-the-art experimental results [Ferr09], a typical bilinear map takes much longer than one exponentiation in $\mathbb{G}_1$, and compared to an exponentiation, the overhead of a hash computation is negligible. Hence, the batch approach offers a significant cost reduction and is very useful to speed up message verifications when the vehicular density is high, as in metropolitan areas.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

5.4 Simulation

In this section, we report on the results of simulations conducted to evaluate the efficiency, effectiveness and applicability of the proposed scheme with emergency message generation and selfish message verification. The network simulator NS-2 [NS2] was used. The VANET scenario was built using the scenario generator presented by Saha and Johnso [Saha04]. The communication range was taken from 10 m to 300 m. The road network considered covered an area of 6.7×2.7 km^2 and is shown in Figure 5.2. The channel bandwidth was 6 Mbps and the packet size was 569 bytes. The time-to-live (TTL) of messages was set to 20 s and the duration of each experiment was 200 s.

The delay introduced by cryptographic operations in the NS-2 simulation was taken to be the computation times of the cryptographic library MIRACL [Multiprecision]. When running MIRACL in a PC environment, the times to compute an exponentiation and a bilinear map are, respectively, about 0.2 ms and 3.5 ms. Hence, in the simulation, we let the batch verification period range from 10 ms to 60 ms.

An important factor for the performance of the security protocol is the latency introduced by verifying the messages from other vehicles. Clearly, a lower latency implies that it takes vehicles less time to respond to the reported traffic environment changes. In turn, a shorter response time means more traffic efficiency and less accidents. The average message delay (seconds) is the average time latency for a message to be processed after it has been sent from one vehicle to another within a one-hop communication range. The latency must be smaller than the maximum allowable end-to-end transmission delay [European] because some messages (*e.g.*, those related to serious traffic jams) need to be forwarded to other vehicles.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

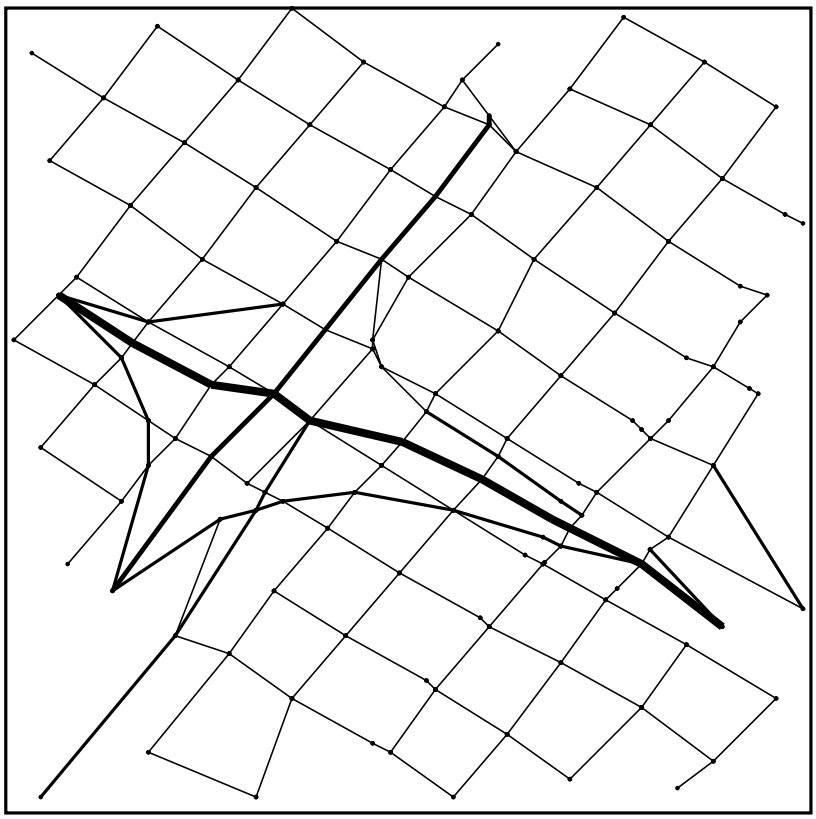

Figure 5.2: Road network considered in the simulation

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

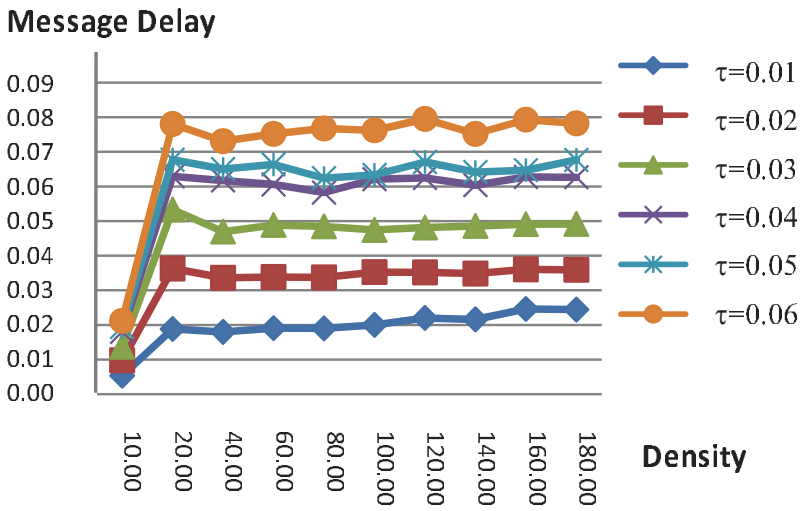

Figure 5.3: Impact of authentication on message delay

In Figure 5.3, the average message delay is presented in seconds for different batch verification periods τ, traffic densities (vehicles/km^2), and message lifetime $TTL = 20$ s. One may notice that, given a fixed batch verification period, the average message delay sharply increases as the vehicle density grows to about 20 vehicles/km^2. After that, the average message delay only grows very slightly, although vehicles receive an increasing number of messages to be verified. This is reasonable, since the proposed selfish batch message verification allows a batch of messages to be verified as if it was a single message. The average message delay is also affected by the batch verification period. As illustrated in Figure 5.3, for a fixed vehicle density, the average message delay increases as the batch verification period increases. This is because vehicles can only perform the verification procedure after the current verification period is over. A longer verification period implies that

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

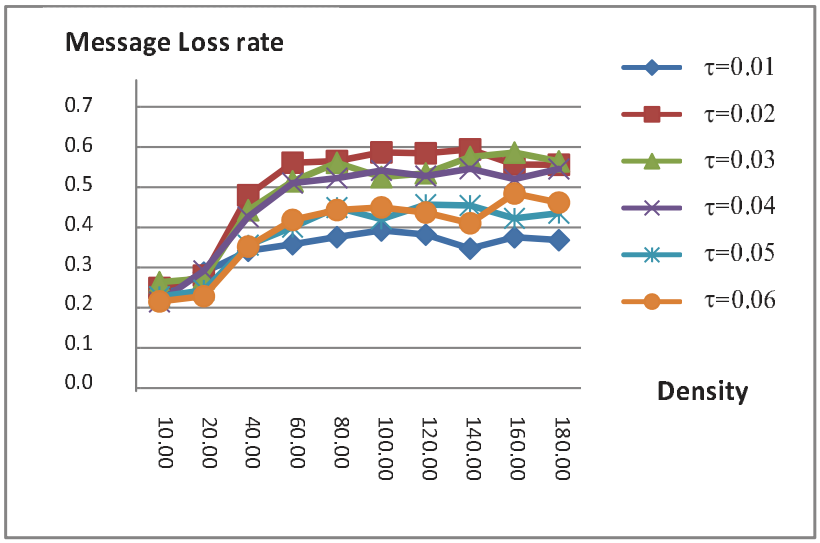

Figure 5.4: Impact of authentication on message loss rate

each vehicle spends more time waiting for the next verification period. Note that the verification period must be at least as long as the time need by a vehicle to perform a batch verification. We also notice that, with the experiment parameters, the average message delay in all cases is less than 100 ms, which is the suggested maximum message delay in VANETs [European]. This implies that our protocol is effective and applicable in practice.

The average message loss ratio is the average relative frequency of a message not being processed before it expires. The average message loss ratio reflects the applicability of the scheme. If security-related processing introduced substantial message loss, then it would be impractical. Loss occurs if the message cannot reach its destination or the queue is full because the message arrival rate is higher than the message processing rate.

In Figure 5.4, the message loss ratio is computed for different verification periods and vehicle densities. One may observe that the average message loss

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

ratio does not always increase as the vehicle density increases. In the case of normal vehicle density (20 vehicles/km^2 or less), the message loss rate is lower than 30%. Then the loss rate grows quickly up to nearly 50% as the vehicle density grows to 40 vehicles/km^2. After that, the message loss rate does not grow greatly even if the vehicle density is very high. This is reasonable, as the large number of messages arrived can be verified as a batch. One may note that a loss rate approaching 60% only happens when the vehicle density is also very high. For a heavy traffic load, it is also acceptable if a large number of messages are lost because most of the messages are repeatedly sent by vehicles. Hence, the high loss rate in this case may not affect the applicability of the protocol in practice. Although there exist variations, the system achieves lower average message loss rate for a shorter verification period. Since message delay also improved for shorter verification periods, we can optimize the performance of our authentication protocol by setting the batch verification period as short as possible, that is, just slightly longer than the time needed by a vehicle to do a batch verification.

5.5 Summary

The first VANETs are likely to be deployed in urban areas which particularly suffer from traffic accidents and congestions. In addition to vulnerabilities to attacks against traffic safety and drivers' privacy, a large-scale VANET in a metropolitan area poses a management problem. This section proposes a set of mechanisms which conciliate efficiency, security and privacy requirements very well. We exploited an up-to-date cryptographic primitive, *i.e.* identity-based group signatures, to divide a large-scale VANET into easy-to-manage groups and establish liability in vehicular communications while preserving

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

privacy. We further presented emergency message generation and selfish batch verification techniques to accelerate message processing in VANETs. These techniques make our protocol scalable for deployment in big metropolitan areas.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 6

Compressing Cryptographic Witnesses in VANETs

The signed vehicle-generated messages have to be stored by the receiving vehicles for possible liability investigation: if some signed messages are later found to be false and to have misguided other vehicles into accident, the message generators and endorsers should be traceable. However, vehicular messages, especially their appended signatures, grow linearly with time while the storage capacity of OBUs in the vehicles is limited. Therefore, security and privacy of vehicle-to-vehicle (V2V) communications need to be conciliated with data aggregation/compression.

Group signatures can be implemented in VANETs to achieve vehicular communications authentication and vehicle privacy, by letting the transportation office play the role of group manager and vehicles the role of group members. The main merit of the group signature based technique over the pseudonym approach is that the former overcomes the limitation of prestoring a large number of anonymous certificates. Authentication of vehicular communications based on group signatures is conceptually simple. However,

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

group signatures are usually much longer than regular signatures and the existing secure group signatures do not allow aggregation. If a message is endorsed by a number of anonymous vehicles, then the same number of group signatures have to be appended. This causes a heavy communication overhead for message relay and an expensive storage load for saving witnesses for the purpose of accident investigation.

The existing proposals for securing VANETs extensively employ cryptographic authentication techniques. A concern that arises from these proposals is how to store a large number of traffic messages, including their cryptographic signatures, for establishing liability and accident reconstruction, considering the fact that they grow with time passing and the storage capacity of vehicles is limited. Another concern is how to verify numerous cryptographic signatures received by vehicles in case of high traffic density. This section efficiently addresses these concerns in order to make a high level of security achievable in VANETs. Our general idea is to aggregate a large number of signatures into a single one without degrading security. Observing that most exiting security proposals are suggested in either PKI-based or ID-based environment, we accordingly provide solutions to aggregate signatures in PKI-based and ID-based scenarios, respectively.

We notice that our solutions efficiently mitigate the challenges in existing security approaches to secure VANETs. With our solutions in the PKI scenario, all the received signatures can be aggregated into a single signature on many messages, much less storage capacity is required and the single signature can be stored for a long period and later used for liability investigation. The aggregation requires only multiplications rather than time-consuming exponentiations or bilinear map computations. In the ID-based scenario, we partially solved this problem. The aggregated signature can be verified as

a regular signature. Compared with verifying those signatures one by one, this enables a significantly faster message response by vehicles. Our analyses illustrate that our solutions are efficient and practical, especially in the case of high traffic density in metropolitan areas.

The remainder of this chapter is organized as follows. Section 6.1 describes the security architecture of VANETs, and security requirements and cryptographic techniques to be applied. We propose our solutions in Section 6.2. A comparison of computation and communication efficiency and a security analysis are reported in Section 6.3. Section 6.4 is a summary.

6.1 Preliminaries

6.1.1 Security architecture of vehicular *ad hoc* networks

Following [Wase08], the VANET architecture is divided into three levels (as shown in Figure 6.1) in the PKI setting. Level 1 is the vehicle administration office (VAO); level 2 consists of lower-level vehicle management offices (LVMO); level 3 includes RSUs and OBUs (or vehicles). VAO is the root certificate authority (RCA) which generates all the system parameters and publishes them on its bulletin board. VAO also issues a certificate for each LVMO, which issues certificates to the RSUs and vehicles in its management domain.

In the ID-based scenario, the system architecture is divided into two levels (as shown in Figure 6.2). Level 1 is the vehicle administration office (VAO); level 2 includes RSUs and OBUs. VAO serves as PKG (public key generator) in ID-based cryptosystems. It generates all the system parameters

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

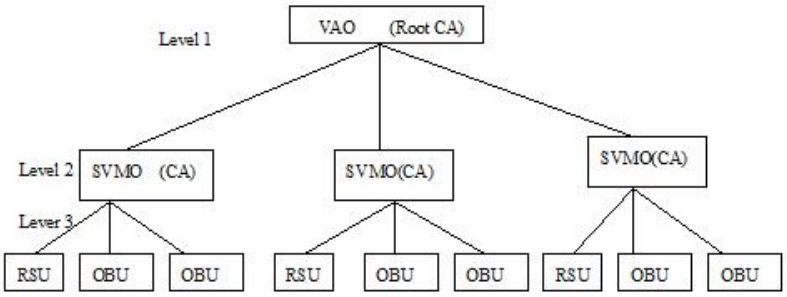

Figure 6.1: PKI-based system structure model

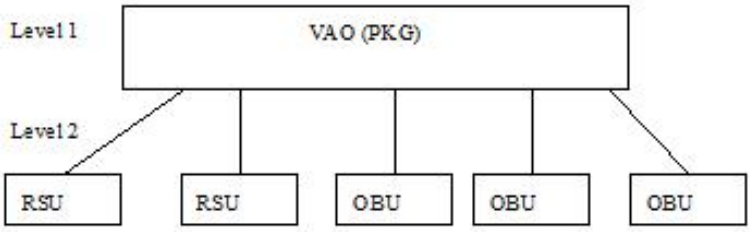

Figure 6.2: ID-based system structure model

and publishes them. The RSUs and vehicles in the city register to VAO and get their secret keys from VAO.

In both cases, the communication among RSUs and OBUs (vehicles) follows the DSRC protocol. Each vehicle has its own ID (*e.g.* plate number) or certificate issued by sub vehicle management office (LVMO). Considering that the presence of RSUs is not pervasive at the beginning of the VANET deployment stage, we do not place much system management burden on RSUs. However, with more vehicles joining the VANET, RSUs can take over some work from VMO or LVMOs to achieve a robust and scalable system.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

6.1.2 Security requirements and challenges

The main thrust behind VANETs is to build a safe and easy driving environment. The messages transmitted in VANETs must be trustworthy so that they can guide drivers. If vehicles produce bogus messages for their own benefit, *e.g.*, clear up the road ahead by broadcasting that the road is in emergency status due to a sequence of traffic accidents, it must be possible to catch (later) the fake message originator. In general, it must be possible to catch the sender of a false message whenever that message causes damage and liability needs to be investigated. Hence, message authentication, integrity, and non-repudiation are identified as the primary requirements in VANETs. As shown in most existing schemes, these security requirements can be met with cryptographic signatures. However, using cryptographic signatures in VANETs raises several challenges such as how to distinguish true messages and react instantly to them, how to compact and store cryptographic traffic evidence and how to alleviate the conflict between traffic liability and data storage limitation of the vehicle's OBU.

6.1.3 Underlying cryptographic technologies

As discussed above, regular signatures suffer from heavy overhead introduced by signature relay, verification and storage, although they can meet the security requirements in VANETs. An alternative might be to use multisignatures [Bold03, Okam98]. However, a multisignature scheme requires all the signers to sign the same message, which implies that the vehicles have to interact to endorse the message. This is somewhat impractical due to high mobility of vehicles with relative speed up to more than 200 km/h. The extremely short connection interval among vehicles does not allow them to interactively sign

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

a message.

We realize that aggregate signatures [Bone03, Zhan10b] are especially suitable for securing VANETs. In a cryptographic sense, an aggregate signature can be thought of as a multisignature without the restriction that the signed message be the same. It allows many independently generated signatures to be aggregated into a single one. Ideally, the length of the aggregate signature (excluding the messages and the public keys of the signers) should be constant, independent of the number of signed messages. The validity of all the signatures can be verified by merely validating the aggregate signature. This property matches both the security and efficiency requirements in VANETs. After a vehicle (or an RSU) receives thousands of message-signature pairs from other vehicles within its communication range, it can aggregate all the signatures into a single one, namely an aggregate signature, and then verify it with one verification operation for all the received signatures. If the verification shows all the signatures are valid, then the vehicle can make its driving decision and, if necessary, the vehicle (or the RSU) can forward these messages and the aggregate signature to vehicles nearby. Finally, the vehicle deletes all the original signatures and just saves the aggregate signature as well as the messages in its onboard storage device. With this approach, much less bandwidth and storage capacity are consumed, both of them scarce resources in VANETs.

Boneh *et al.* presented the first aggregate signature scheme [Bone03], which is derived from the BLS signature in finite cyclic groups equipped with efficiently computable bilinear maps. Subsequently, Lysyanskaya *et al.* presented a sequential aggregate RSA signature scheme [Lysy04] that, while more limited, could be instantiated using more general assumptions. In a

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

sequential aggregate signature scheme the aggregate signature must be constructed sequentially, with each signer modifying the aggregate signature in turn. Lu *et al.* presented an aggregate signature scheme [Lu06] that is provably secure without random oracles. Their signatures are also sequentially constructed. Unlike in the scheme of Lysyanskaya *et al.*, a verifier need not know the order in which the aggregate signature was created. However, in a VANET environment, the messages sent by the vehicles nearby are random, dynamic and instantaneous; hence, sequential aggregate signatures [Chen05, Lysy04] are less suitable than non-sequential aggregate signatures.

The above schemes are all in the PKI setting. As for the ID-based setting, several ID-based aggregate signature schemes have been presented [Cheo06, Gent06, Herr06, Pate06, Xu05]. Herranz [Herr06] proposed an ID-based partial aggregate signature with linear size in the number of messages. Gentry *et al.* proposed an identity-based aggregate signature [Gent06]. In their schemes, the verifier does not need to obtain and/or store several signer public keys; instead, the verifier only needs a description of who signed what, along with two constant-length "tags": the short aggregate signature and the single public key of a private key generator. However, in their scheme, all signers must use the same (unique) random string w when signing each time. This limitation makes their scheme impractical for securing VANETs due to the volatile signature generation-verification relation between vehicles.

6.2 The proposals

We propose vehicular authentication schemes based on aggregate signatures.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Table 6.1: Format of vehicle-generated message

Emergency Level	Payload	Timestamp	Signature
1 bytes	100 bytes	4 bytes	$\leq$ 128 bytes

6.2.1 High level description of our solutions

The safety-related messages transmitted in VANETs can be sorted according to their emergency levels. The first level might be about traffic congestion or accident warning; the second level might be about turning intention, driving status (*e.g.*, brake, accelerate, wait for traffic light, etc.); and the third level might be regular reports about location, speed, direction, time, etc. After the vehicles and RSUs receive lots of messages in one interval, they deal with them immediately or defer processing some of them according to their level. After aggregation, the first-level messages are arranged at the top of the list, in order to ensure a fast propagation of emergency and local warning messages to the approaching vehicles that is helpful to prevent accidents. The format of vehicle-generated messages (length in bytes) is shown in Table 6.1. The payload field may include information on the vehicle's position, direction, speed, traffic events, event time and so on. According to DSRC, the payload of a message is 100 bytes. A timestamp is used to specify the signature generation time, which is employed to prevent replay attacks.

By taking into account the available up-to-date aggregate signatures and the number of vehicles and RSUs within communication range, in a small or medium city we propose to apply PKI-based aggregate signatures, while in a metropolitan area identity-based aggregate signatures are preferable. ID-based signatures have the big advantage of eliminating the need for managing the certifications of a large number of vehicles. In the PKI-based signature

case, a full aggregate signature [Bone03] is employed, by which all the different messages signed by different OBUs and RSUs can be aggregated into a single signature; consequently, verification can be done as for a single regular signature and the storage consumption is minimal. In the ID-based signature case, a partial aggregate signature [Herr06] is employed. Although in this case the underlying aggregate signature is still partially linear with the number of the received messages, we relieve this limitation by pre-storing a part of each signature in vehicles thereby obtaining a constant compressed signature.

Aggregate signatures in both [Bone03] and [Herr06] rely on the computational co-Diffie-Hellman assumption in $(\mathbb{G}_1, \mathbb{G}_2)$.

6.2.2 Aggregate PKI-based vehicular witnesses

Our scheme uses the property of bilinear maps. The scheme also employs a full-domain hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_1$. The transmitted message is denoted by $m_i \in \{0,1\}^*$ where the first byte represents the message emergency level. If the message is not traffic-safety related, then its emergency level is set to 0.

We next apply the BGLS aggregate signature [Bone03] to a medium-scale VANET. The system architecture is as shown in Figure 6.1. All the entities including VAO, LVMO, RSUs and OBUs use the BGLS scheme to generate their public and private key pairs. Since a PKI certificate is in fact the signature of a message related to identity, time period, public key, etc., we treat a certificate as a regular message signature. Hence, *the certificates can also be aggregated to save verification time and storage space.*

Setup: VAO generates a tuple $\gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \hat{e})$ as in Section 3.1 and a hash function H as defined above. The system parameters

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Table 6.2: Format of a certificate: fields and size

Certificate ID	Public Key	User ID	Lifetime	Signature
4 bytes	22 bytes	4 bytes	4 bytes	22 bytes

are $\pi =< \gamma, H >$. The system parameters are embedded into VAO, LVMO, RSUs and OBUs.

Key-Certificate Generation: VAO picks a random $x \in \mathbb{Z}_p$, and computes $v = g_2^x$. VAO's public key is $v \in \mathbb{G}_2$ and its secret key is $x \in \mathbb{Z}_p$. The LVMO can freely choose their public and private key similarly as VAO does, and then run a zero-knowledge proof protocol [Qin09] with VAO to prove their public key binding with their private key and get a certificate from VAO. VAO generates the certificate on each LVMO's public key with x. Similarly, OBU (or RSU) generates its secret key and public key; each LVMO generates certificates for RSUs and OBUs within its management domain. The format of a certificate is shown in Table 6.2.

Signing: The format of the message m_i is (ELevel, MPayload) where ELevel denotes the the emergency level of the message and MPayload is the message payload. Assume that a vehicle has public key $v_i = g_2^{x_i}$ and secret key $x \in \mathbb{Z}_p$, and it wants to send a message m_i. It computes $h_i = H(m_i)$ and $\sigma_i = h_i^{x_i}$. The signature on m_i is $\sigma \in \mathbb{G}_1$. Then the vehicle outputs a vehicular message $M_i = (m_i, \sigma_i,$ certificate). Note that the certificate can be viewed as a signature $\sigma_{i'}$ on a message $m_{i'}$ of the first four fields in the certificate. Hence, we can view a vehicular message $M_i = (m_i, \sigma_i, m_{i'}, \sigma_{i'})$ as two regular BLS message-signature pairs. Notice here that we neglect the certificates of LVMOs as the few LVMOs are static and their certificates can be verified separately and cached during their lifetime.

Aggregation and verification: For clarity, we assume that only the

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

OBUs or vehicles will verify, store and relay the vehicular messages. However, our description easily extends to RSUs. Before aggregation, a vehicle first checks that the received vehicular messages are of the correct format, and discard the incorrect ones. Vehicular messages are classified according to their emergency level. Emergency messages will be aggregated and verified upon their arrival. Then the vehicle aggregates and verifies the second-level messages and finally the third-level ones. For each class of vehicular messages, the vehicle first computes

$$\sigma_A = \prod_{i=1}^{n} \sigma_i \sigma_{i'}$$

as the aggregate signature on the received n messages M_i of the same emergency level, and then accepts the aggregate signature σ_A if and only if

$$\hat{e}(\sigma, g_2) = \prod_{i=1}^{n} \hat{e}(h_i, v_i)\hat{e}(h_{i'}, v_{i'}).$$

Finally, the vehicle adds M_i to its local database

$$\mathbb{M} = (m_1||...||m_{i-1}; \sigma_0 \cdots \sigma_{i-1}; m_{0'}||...||m_{(i-1)'}; \sigma_{0'} \cdots \sigma_{(i-1)'}).$$

We note that the second and fourth fields are always of constant size, 22 bytes for each field in the above proposal. The saving in storage cost is significant.

The following measures can further improve the proposal. If a vehicle receives many signatures from a second vehicle (which is possible when they both move in the same direction), the sender's certificate needs to be verified only in the first aggregation and then cached for other signatures. To avoid verifying duplicate messages, a vehicle can check the first field of its local database $\mathbb{M}$. The vehicle only needs to store one copy of the duplicate messages from OBUs. If the duplicate messages are from the same OBU,

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

the vehicle discards them directly. Finally, when aggregation verification has failed, we can use the "divide-and-conquer" search algorithm in [Matt09] to identify the invalid signatures.

The underlying aggregate signature is shown in [Bone03] to be correct and secure against existential forgery in the aggregate chosen-key model. Correctness implies that the messages generated by vehicles honestly following the protocol will always be accepted. If the aggregate signature on received vehicular messages is valid, then all the received vehicular messages can be viewed as valid to guide vehicles. Unforgeability guarantees that, if a vehicle does not register to the VANET, it cannot generate aggregate message signatures accepted by other vehicles, even if the cheating vehicle is allowed to access valid message signatures over the VANET. If an aggregate message signature passes the verification procedure, it must be on intact fresh messages generated by registered vehicles. This implies that the attacker cannot cheat other vehicles by forging a new valid message or by modifying an existing valid message or by replaying a once valid but now expired message. Unforgeability also implies that, if the aggregate signature on a number of vehicular messages is accepted by the verification procedure, then all the message originators indicated by their certificates must be responsible for these messages. This is because if not all the originators endorsed the message, then the aggregate signature could not be valid; otherwise unforgeability would be contradicted. Hence, liability can be established via the aggregate signature.

6.2.3 Aggregate ID-based traffic witnesses

When PKI-based aggregate signatures are employed for large-scale VANETs, the overhead of certificate management (issuing, distributing, revoking and

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

retrieving certificates) becomes a heavy burden, even with full aggregation. In this case, the ID-based aggregate signature in [Herr06] is preferable. The resulting system architecture is illustrated in Figure 6.2. Here, VAO works as a trusted PKG.

Setup: VAO generates a tuple $\gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \hat{e})$. Here, $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and $g_1 = g_2 = g$. Two hash functions are selected: $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$. The system parameters $\pi =< \lambda, \gamma, H_1, H_2 >$ are embedded into VAO, RSUs and OBUs.

Key Generation: Let N be the maximum number of nodes including RSUs and OBUs in a VANET. VAO randomly selects $r_i \in \mathbb{Z}_p^*$ and computes $R_i = g^{r_i}$ for $i = 1, \cdots, N$. VAO also randomly chooses an element $x \in \mathbb{Z}_p^*$ and computes $Y = g^x$. VAO's secret master key is set as $(x, r_1, \cdots, r_N)$. VAO's public key is $(Y, R_1, \cdots, R_n)$ which can also be embedded into VAO, RSUs and OBUs. For a large-scale VANET up to one million nodes, the size of the system public key is only 22 Mbytes, which is affordable in practice.

An OBU or a vehicle registers to VAO with an identity ID_i. By computing a Schnorr signature on the message ID, VAO generates the private key for the vehicle as follows:

1. VAO looks up $r_i \in \mathbb{Z}_p^*$ in its private key list and $R_i = g^{r_i}$ in its public key list;

2. VAO computes the value $\sigma_i = r_i + xH_1(ID_i, R_i) \mod p$;

3. VAO privately sends the secret key σ_i to the OBU (or RSU) through a confidential channel;

4. The OBU (or RSU) can verify the correctness of the received secret key by checking whether $g^{\sigma_i} \stackrel{?}{=} R_i Y^{H_1(ID_i, R_i)}$.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Signing: Let a vehicle hold identity ID_i and secret key σ_i. When it wants to endorse a message m_i, it computes $\theta = H_2(m_i, ID)^{\sigma_i}$ as the resulting signature on m_i. The vehicle sends the endorsed vehicular message $M_i = (m_i, ID_i, \theta_i)$ to other vehicles nearby.

Aggregation and verification: The vehicular messages can be processed similarly to those in the previous PKI-based solution, according to their emergency level. Assume that a vehicle receives n vehicular messages $M_i = (m_i, ID_i, \theta_i)$ to be verified in an interval, where one can have $ID_i = ID_j$ while $m_i \neq m_j$. Firstly, the vehicle computes the aggregate

$$\theta_A = \prod_{i=1}^{n} \theta_i$$

for messages $m_1, \cdots, m_n$. Then the vehicle accepts all the messages if and only if:

$$\hat{e}(\theta_A, g) = \prod_{i=1}^{n} \hat{e}(H_2(ID_i, m_i), R_i \cdot Y^{H_1(ID_i, R_i)}).$$

Finally, the vehicle adds M_i to its local database

$$\mathbb{M} = (m_1||...||m_{i-1}; ID_1||\cdots||ID_{i-1}; \theta_1 \cdots \theta_{i-1}),$$

One may note that the last field is always of constant size, *i.e.*, 22 bytes in the above proposal. The saving in storage cost is significant.

The correctness of the protocol is straightforward to verify. This means that the aggregate signature will be accepted if all the messages are generated by honestly following the protocol. If the aggregate signature on the received messages is viewed as valid after verification, then all the messages can be trusted to guide vehicles, which potentially improves traffic safety

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Table 6.3: Comparison of verification and storage

	Verification cost	Signature size (bytes)
PKI_{BA}	$2nE + 4nP$	$44n$
PKI_{AA}	$2nE + nM + (2n + 1)P$	44
ID_{BA}	$2nE + 2nP$	$22n$
ID_{AA}	$2nE + nM + (n + 1)P$	22

and efficiency. As for security, it has been shown that, in the random oracle model [Bell93], the underlying aggregate signature is unforgeable under adaptive chosen-message attacks. This guarantees that, if a vehicle does not register to the VANET, it cannot generate message signatures accepted by other vehicles in the aggregate-verification procedure, even if the cheating vehicle is allowed to access valid messages signatures over the VANET. If an aggregate signature passes the verification procedure, it must be a signature on intact fresh messages generated by registered vehicles. An attacker cannot cheat other vehicles by forging a new valid message or by modifying an existing valid message or by replaying a once valid but now expired message. Hence, if the verification of the aggregate signature on stored messages shows that all the messages are valid but, later on, some of them are found to be deceitful, then the originators or endorsers of these messages can be traced by their identities for liability. This is essential to guarantee trustworthiness in vehicular communications.

6.3 Performance evaluation

We briefly evaluate the performance of our approaches. To assess the cost savings, we compare the verification cost and signature size with aggregation and without aggregation in Table 6.3.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

In the above table, PKI_{BA} denotes PKI-based authentication using the scheme in Section 6.2.2 without aggregation while PKI_{AA} is the scheme in that section with aggregation. Similarly, ID_{BA} and ID_{AA} are ID-based authentication without/with the aggregation technique in Section 6.2.3. The number of messages is n, while M, E, and P are, respectively, the multiplication, exponentiation and bilinear map operations; for clarity, we do not differentiate those operations for different groups. Also, we view the hash to $\mathbb{G}_1$ (or $\mathbb{G}$) as one exponentiation but we consider the hash to $\mathbb{Z}_p^*$ as negligible, compared to other operations. Among all the operations, the bilinear map is most expensive and then comes the exponentiation.

From the above table, the saving in storing cryptographic signatures is very impressive as signatures growing linearly with time are compressed into constant length. This is very critical if a large number of signatures have to be stored for a long period for the purpose of liability investigation. As to computation cost, the verification overhead after aggregation is about half of that without aggregation. Computation savings seem less impressive than storage savings. However, one may further note that the aggregation verification allows the use of fast multi-bilinear map computation techniques. In practice, the actual improvement in signature verification should be much more than twofold. This is also important to enable vehicles to react to emergency messages as soon as possible.

6.4 Summary

This chapter proposed efficient authentication protocols for securing VANETs. Proposals were made for the PKI-based and ID-based scenarios. In both cases, the signatures are compressed into constant size and much storage

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

space is saved in the vehicle onboard device. The proposals also allow fast message verification to speed up vehicle response to traffic environment changes.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 7

Privacy-Preserving Location Based Services in VANETs

In addition to safety-related applications, VANETs will enable a broad range of value-added applications, like payment services (toll collection, parking fee collection), location based services (LBSs, *e.g.*, to locate the closest fuel station), infotainment [Tell08], etc. It is expected that those value-added applications of VANETs will open substantial business opportunities [Car2car].

Security and privacy are two critical concerns in VANETs. In traditional wired networks, sophisticated cryptographic technologies have been developed to protect parties in value-added applications (mainly location based services); examples of such technologies are anonymous credential systems, First Virtual, SSL, iKP secure electronic payments [Bell00] and the SET protocol [Mastercard]. However, VANETs are very dynamic and their communications are volatile, which makes the aforementioned complex protocols unsuitable.

LBS applications raise additional challenges in VANETs. A way to achieve security in a VANET is for any message broadcast by a vehicle to contain a

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

verifiable identity as well as authentic data. However, in that case, messages broadcast can reveal the originating vehicle's identity as well as its location, which facilitates abuses consisting of tracking the movement of the vehicle by linking its traversed locations. Such tracking may be useful not only for terrorists to monitor a target vehicle, but also for LBS applications accessed by the vehicle to profile the locations of the vehicle user, which enables inference of personal interests and thus encroaches on the user's privacy [Pool09].

In this chapter, we investigate the security requirements of LBS in VANETs and propose a new privacy-preserving LBS scheme for those networks. The new proposal integrates an identity-based cryptosystem (Section 7.1.3) and group signatures (Section 7.1.4). In our scheme, the public keys of an RSU and an LBS provider are just their identities. On the vehicle side, only a member key is needed which is used to generate authenticated data to access LBSs. This eliminates the certificate management overhead. Furthermore, our system does not need to maintain groups in dynamic networks with volatile connections. Instead, we exploit group signatures to protect the vehicle privacy. Hence, our system is robust because it does not depend on an instable proxy. Finally, with our scalable hierarchical technique, the proposed system maintains efficiency even if the system hosts a huge number of LBS users.

The chapter is organized in the following way. In Section 7.1, we discuss some preliminaries, including the system architecture, the security requirements, identity-based cryptography, group signature and bilinear maps. Section 7.2 proposes our basic LBS scheme. We evaluate the new protocol in Section 7.3. Section 7.4 develops an improved LBS System. Section 7.5 is a concluding summary.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

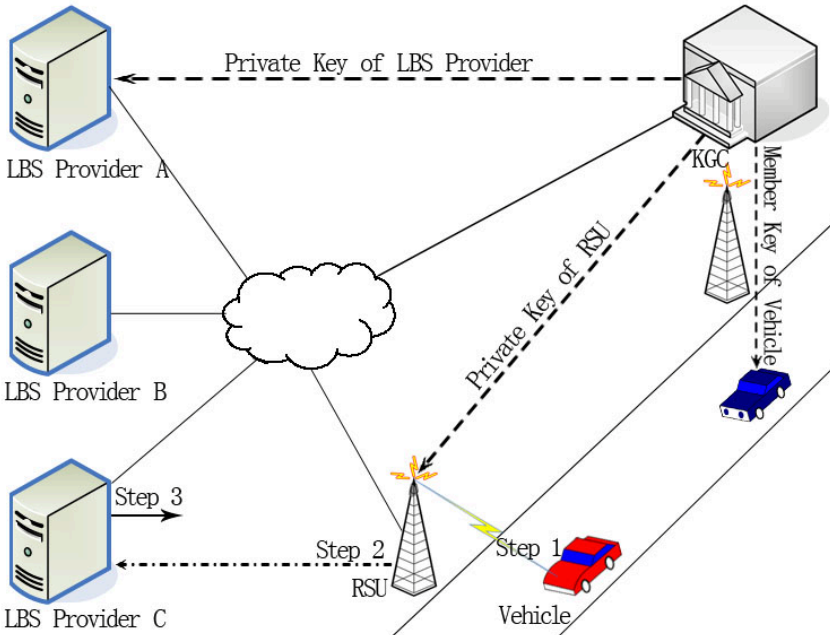

Figure 7.1: System architecture

7.1 Preliminaries

7.1.1 System architecture

The system architecture is illustrated in Figure 7.1. In the system, there are key generation center(s) (KGC(s)), RSUs, vehicles and providers of location based services (LBS providers):

- A KGC is a trusted third party. It generates private keys for vehicles and LBS providers and it issues secret member keys for vehicles. In addition, the KGC is assumed to be able to determine the real identity of vehicles and LBS providers.

- RSUs are equipped with on-board sensory, processing, and wireless communication modules, and they are distributed along the road side.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

They are connected to LBS providers by a wired network. RSUs are assumed to be semi-trusted (*i.e.*, some of them might be compromised).

- Vehicles move along the roads, sharing environmental information with each other and/or querying LBSs through RSUs using the DSRC protocol [DSRC]. Each vehicle is equipped with on-board sensory, processing, and wireless communication modules.

- LBS providers process the data forwarded by RSUs and offer LBSs to vehicles.

7.1.2 Security requirements

We analyze the security requirements of an LBS system in a VANET. We first show the communication model of an LBS protocol. As illustrated in Figure 7.1, an LBS protocol can be described in three steps. In the first step, a vehicle sends its request to a nearby RSU using the DSRC protocol in a single-hop or multi-hop manner. In the second step, the RSU receives the request from the vehicle and detects what kind of services the vehicle is asking for; then it forwards the request to the corresponding LBS provider. In the last step, the LBS provider authenticates the vehicle. If the vehicle is a subscriber, the LBS provider returns the requested service to the vehicle by routing its response through RSUs neighboring the RSU the vehicle request came from.

[Security requirements at Step 1]

In this step the security requirements are:

- **Message confidentiality.** An LBS request may contain sensitive information of a vehicle. For instance, if a vehicle requests a priced service, the e-cash (usually a blind signature [Chau82, Chen09, Zhan09c])

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

may be included in the query. If the vehicle sends this request to the LBS provider through an RSU, anyone can learn the e-cash information and an attacker can steal the e-cash by disabling the communication from the requesting vehicle to the RSU. Hence, message confidentiality is required. Message confidentiality at this step has two levels. Level 1 provides confidentiality when the attacker does not know the private key of the RSU. It requires that only the vehicle and the RSU be aware of the information exchange. Level 2 provides confidentiality even if the attacker learns the private key of the RSU. In this case, we require that no one but the vehicle and the designated LBS provider can learn the content of the LBS request.

- **Vehicle privacy.** Privacy in this step has also two levels. Level 1 guarantees privacy when the attacker does not know the private key of the RSU. It requires that it be computationally hard for everyone (except the message generator or some trusted third party) to decide whether two different messages were generated by the same vehicle. Level 2 guarantees privacy even when an RSU is compromised by an attacker. In this case, we require that the attacker can only learn the service type a vehicle is requesting.

[Security requirements at Step 2]

In our system, an RSU serves as a router. For an LBS protocol in VANETs, an RSU only needs to know the service type that a vehicle is requesting so that it can forward the request to the right LBS provider. Hence, in our design, we only let RSUs learn the kind of service the vehicle wants to access. This step needs to meet the following security requirements:

- **Message confidentiality.** No one but the vehicle and the designated

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

LBS provider can learn the content of the message forwarded by the RSU.

- **Vehicle privacy.** It is computationally hard for everyone (except the message generator or some trusted third party) to decide whether two different messages were generated by the same vehicle.

[Security requirements at Step 3]

This step has the following requirements:

- **Vehicle authentication.** The LBS provider must be sure that the request comes from some registered vehicle, *i.e.*, a subscriber.

- **Vehicle privacy.** The LBS provider only learns that a vehicle is queryihg the LBS but it cannot learn the vehicle's identity. Furthermore, the LBS provider cannot decide whether two different requests were generated by the same vehicle.

- **Vehicle traceability.** In VANETs, the privacy of a vehicle should be conditional. That is, if necessary, some trusted third party should be able to revoke the anonymity of doubtable vehicles. Otherwise, a malicious vehicle might send fake messages to jeopardize the system without fear of being caught. KGC is endowed with the ability to trace the real identity of dishonest vehicles sending fake messages to LBS providers in order to disrupt services.

7.1.3 Identity-based encryption

In our protocol, we will use an Identity-Based Cryptosystem (IBC) to guarantee the security of the system. In VANETs, since we need not consider the privacy of RSUs and LBS providers, we can use the location information and

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

service type as the identity of an RSU (and LBS provider). For instance, if an RSU is located at street A in city B, then we can use '$RSU, streetA, cityB$' as the identity of this RSU; for an LBS provider who provides online map service in city B, we can use '$onlinemap, cityB$' as the identity of the LBS provider. Furthermore, in our system, a trusted third party, called the Key Generation Center (KGC), generates the corresponding private keys for the entities in IBC. To operate, the KGC first publishes the system parameters and keeps secret the corresponding master key. Given the system parameters, any party can compute the public key corresponding to an identity ID by combining the system parameters with the identity value. To obtain a corresponding private key, the party authorized to use identity ID contacts the KGC, and the KGC uses the master key to generate the private key for identity ID.

7.1.4 Group signatures with verifier-local revocation

Group signatures [Bone04b, Chau91] allow the members of a group to sign on behalf of the group. Everyone can verify the signature with a group public key while no one can know the identity of the signer except the group manager. Further, except for the opener, it is computationally hard for anyone to decide whether two different signatures were issued by the same group member.

Member revocation is needed to disable members who left the group or whose secret member key and/or member certificate were/was compromised. Most group signatures suffer from inefficient member revocation.

Recently, an efficient approach to membership revocation in group signatures was proposed, called verifier-local revocation [Bone04a]. The idea is that only verifiers are involved in the revocation mechanism, while signers

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

have no involvement. This approach is especially suitable for mobile environments where mobile signers (*i.e.,* the vehicles in our case) have much less computational power than the verifying servers (*i.e.*, the LBS providers).

We will use the group signature scheme with optimized verifier-local revocation in [Naka05] to achieve 'Vehicle Authentication', 'Vehicle Privacy' and 'Vehicle Traceability'.

7.2 Privacy-preserving LBS proposal

In this section, we propose a privacy-preserving LBS scheme for VANETs. Before describing the scheme in detail, we first explain the notations used to simplify the description.

Table 7.1: Description of notation

Notation	Description
$\mathcal{V}$:	A vehicle.
$\mathcal{R}$:	An RSU.
$\mathcal{L}$:	An LBS provider.
$ID_{\mathcal{A}}$:	The identity of entity $\mathcal{A}$.
$S_{\mathcal{A}}$:	The secret key of $\mathcal{A}$.
$\|\|$:	Message concatenation operation.
Des:	The description of an LBS request.
Add:	The addresses of some RSUs near $\mathcal{R}$ through which the LBS response to $\mathcal{V}$ will be routed.
TP:	A time stamp.
IEK:	The identity enrolment key, used to generate private keys for RSUs and LBS providers.
MEK:	The member enrolment key, used to issue member keys for vehicles.
$\mathcal{E}_K(\cdot)/\mathcal{D}_K(\cdot)$:	A symmetric-key encryption scheme (*e.g.*, AES).

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

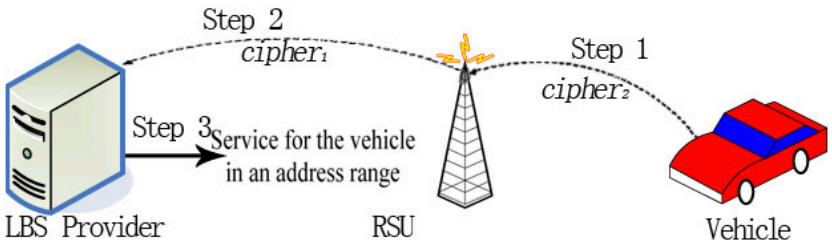

Figure 7.2: The LBS protocol

7.2.1 High level description

This section outlines the basic ideas of our LBS system for application in VANETs. We refer to the three steps mentioned in Section 7.1.2 and shown in Figure 7.2.

In the first step, the vehicle $\mathcal{V}$ first prepares a request of the form $Des||Add||TP||Sig$ and encrypts this request under $\mathcal{L}$'s identity to generate a ciphertext $cipher_1$, where Sig is the group signature with verifier-local revocation on $Des||Add||TP$. Then it encrypts $TP||ID_{\mathcal{L}}||cipher_1$ under the identity of its nearby RSU to generate the ciphertext $cipher_2$. Finally, $cipher_2$ is sent to the RSU.

In the second step, when the RSU receives $cipher_2$ from $\mathcal{V}$, RSU decrypts the ciphertext $cipher_2$ to get $TP||ID_{\mathcal{L}}||cipher_1$. If TP is fresh, RSU forwards $cipher_1$ to the LBS provider with identity $ID_{\mathcal{L}}$.

In the last step, the LBS provider decrypts the ciphertext $cipher_1$ to get $Des||Add||TP||Sig$. It then checks whether TP is fresh and Sig is a valid signature on $Des||Add||TP$. If TP is fresh and Sig is valid, the LBS provider provides the service described by Des to Add.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

7.2.2 The concrete scheme

In this section, we propose our concrete LBS scheme, consisting of the following five stages.

[System Setup]

At this stage, KGC initializes the system-wide parameters. It does the following.

1. Generate a tuple $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, \hat{e})$. Here, $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and $g_1 = g_2 = g$.

2. Choose $u_0, u_1 \in \mathbb{G}$.

3. Pick $\kappa, \rho \in \mathbb{Z}_p^*$ as its master secret key, and compute $u_2 = g^{\kappa}, u_3 = g^{\rho}$ as its master public key. Hereafter, we will also call κ as IEK and ρ as MEK.

4. Compute
$$\begin{cases} Y_0 = \hat{e}(u_0, u_3) \\ Y_1 = \hat{e}(u_0, g) \\ Y_2 = \hat{e}(u_1, g) \\ Y_3 = \hat{e}(g, g). \end{cases}$$

5. Choose a symmetric-key encryption scheme $\mathcal{E}_K(.)/\mathcal{D}_K(.)$. We assume that the bit-length of K is λ.

6. Select cryptographic hash functions $H_0(\cdot) : \{0,1\}^* \longrightarrow \mathbb{G}$, $H_1(\cdot) : \{0,1\}^* \longrightarrow \mathbb{Z}_p^*$ and $H_2(\cdot) : \mathbb{G}_T \longrightarrow \{0,1\}^{\lambda}$.

7. Publish the system parameters as

$$\Psi = (\hat{e}, p, \mathbb{G}, \mathbb{G}_T, g, u_0, u_1, u_2, u_3, H_0, H_1, H_2, Y_0, Y_1, Y_2, Y_3, \mathcal{E}_K(\cdot)/\mathcal{D}_K(\cdot)).$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Ψ is assumed to be pre-loaded in each vehicle, RSU and LBS provider.

The KGC also maintains a member list ML and a revocation list RL, where ML is kept secret while RL is published. We will define these lists later.

[Registration]

Before a vehicle, an LBS provider or an RSU joins a VANET, it registers with the KGC. The KGC generates a secret key or a member key for them using the following algorithms.

RSUJoin: This algorithm is used to generate the secret key for an RSU. Suppose that the identity of an RSU $\mathcal{R}_i$ is $ID_{\mathcal{R}_i}$. The KGC computes $S_{\mathcal{R}_i} = H_0(ID_{\mathcal{R}_i})^{\kappa}$.

ServiceJoin: This algorithm is used to generate the secret key for an LBS provider. Suppose that the identity of an LBS provider is $ID_{\mathcal{L}_i}$. The KGC computes $S_{\mathcal{L}_i} = H_0(ID_{\mathcal{L}_i})^{\kappa}$.

VehicleJoin: This algorithm is used to generate the member key for a vehicle. The KGC maintains a member list ML of tuples $(ID_{\mathcal{V}}, w, x, v)$, where $v = u_1^x$. When a vehicle wants to join the system, the KGC accepts a vehicle's identity $ID_{\mathcal{V}_i}$ and generates the member key as follows.

1. Select $x_i \in \mathbb{Z}_p^*$.
2. Compute $w_i = g^{1/(\rho+x_i)}$ and set (w_i, x_i) as the member key of $\mathcal{V}_i$.
3. Add $(ID_{\mathcal{V}_i}, w_i, x_i, v_i)$ to ML, where $v_i = u_1^{x_i}$ is the revocation token of $\mathcal{V}_i$.

[LBS Protocol]

As discussed in Section 7.1.2, an LBS protocol consists of three steps.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Step 1: The first step is the vehicle-to-RSU communication. Suppose that $\mathcal{V}_i$ wants to access the LBS provider $\mathcal{L}_k$ and its nearby RSU is $\mathcal{R}_j$. $\mathcal{V}_i$ does the following:

1. Choose $s \in \mathbb{Z}_p^*$ and compute

$$C_1 = g^s, SK_1 = H_2(\hat{e}(u_2^s H_0(ID_{\mathcal{L}_k})))$$

   where SK_1 will be the key of the symmetric-key encryption scheme $\mathcal{E}_K(\cdot)/\mathcal{D}_K(\cdot)$.

2. Set $m_1 = Des||Add||TP||Sig$, and compute $C_2 = \mathcal{E}_{SK_1}(m_1)$, where Sig is the signature on $m_0 = Des||Add||TP$ which is generated using the SigGen algorithm in Figure 7.3.

3. Choose $t \in \mathbb{Z}_p^*$ and compute

$$C_3 = g^t, SK_2 = H_2(\hat{e}(u_2^t, H_0(ID_{\mathcal{R}_j}))).$$

4. Set $cipher_1 = C_1||C_2$, $m_2 = TP||ID_{\mathcal{L}_k}||cipher_1$.

5. Compute $C_4 = \mathcal{E}_{SK_2}(m_2)$.

6. Send $cipher_2 = (C_3||C_4)$ to $\mathcal{R}_j$.

Step 2: When $\mathcal{R}_j$ receives $cipher_2 = (C_3, C_4)$, it does the following:

1. Compute $SK_2 = H_2(\hat{e}(C_3, S_{\mathcal{R}_j}))$.

2. Compute $m_2 = TP||ID_{\mathcal{L}_k}||cipher_1 = \mathcal{D}_{SK_2}(C_4)$.

3. Check TP to decide whether the request is fresh. If it is, send $cipher_1 = (C_1, C_2)$ to $\mathcal{L}_k$; otherwise abort.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

1. Randomly select $\alpha, \beta, \gamma \in \mathbb{Z}_p^*$ and compute $\delta = x_i\alpha, \zeta = x_i\beta, \eta = x_i\gamma$.
2. Compute $t_1 = w_i u_0^{\alpha}, t_2 = g^{\alpha} u_0^{\alpha}, T_3 = Y_2^{\eta}$ and $t_4 = g^{\gamma}$.
3. Select $r_{\alpha}, r_{\beta}, r_{\gamma}, r_{x_i}, r_{\delta}, r_{\zeta}, r_{\eta} \in \mathbb{Z}_p^*$ at random.
4. Compute

$$\begin{cases} R_1 = g^{r_\alpha} u_0^{r_\beta} \\ R_2 = t_2^{r_{x_i}} g^{-r_\delta} u_0^{-r_\zeta} \\ R_3 = \hat{e}(t_1, g)^{-r_{x_i}} Y_0^{r_\alpha} Y_1^{r_\delta} \\ R_4 = Y_2^{r_\eta} \\ R_5 = g^{r_\gamma} \\ R_6 = t_4^{r_{x_i}} g^{-r_\eta}. \end{cases}$$

5. Compute $c = H_1(\Psi, m_0, t_1, t_2, T_3, t_4, R_1, ..., R_6)$.
6. Compute $s_\alpha = r_\alpha + c\alpha, s_\beta = r_\beta + c\beta, s_\gamma = r_\gamma + c\gamma$, $s_{x_i} = r_{x_i} + cx_i, s_\delta = r_\delta - c\delta, s_\zeta = r_\zeta + c\zeta$ and $s_\eta = r_\eta + c\eta$.
7. Output the group signature $Sig = (t_1, t_2, T_3, t_4, c, s_\alpha, s_\beta, s_\gamma, s_{x_i}, s_\delta, s_\zeta, s_\eta)$.

Figure 7.3: The group signature generation algorithm SigGen

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

1. Compute

$$\begin{cases} R_1 = g^{s_\alpha} u_0^{s_\beta} t_2^{-c} \\ R_2 = t_2^{s_{x_i}} g^{-s_\delta} u_0^{-s_\zeta} \\ R_3 = \hat{e}(t_1, g^{-s_{x_i}} + u_3^{-c}) Y_0^{s_\alpha} Y_1^{r_\delta} Y_3^{c} \\ R_4 = Y_2^{s_\eta} T_3^{-c} \\ R_5 = g^{s_\gamma} t_4^{-c} \\ R_6 = t_4^{s_{x_i}} g^{-s_\eta}. \end{cases}$$

2. Check $c \stackrel{?}{=} H_1(\Psi, m_0, t_1, t_2, T_3, t_4, R_1, ..., R_6)$.
3. Output *valid* if the signature passes the above check.

Figure 7.4: The group signature verification algorithm SigVer

Step 3: When $\mathcal{L}_k$ receives $cipher_1 = (C_1, C_2)$, it does the following:

1. Compute $SK_1 = H_2(\hat{e}(C_1, S_{\mathcal{L}_k}))$.
2. Compute $m_1 = Des||Add||TP||Sig = \mathcal{D}_{SK_1}(C_2)$. If TP is fresh, go to next step; otherwise, abort.
3. Extract $Sig = (t_1, t_2, T_3, t_4, s_\alpha, s_\beta, s_\gamma, s_{x_i}, s_\delta, s_\zeta, s_\eta)$.
4. Check whether Sig is a valid group signature on $Des||Add||TP$ using the SigVer algorithm in Figure 7.4. If the signature is valid, provide the service to *Add* according to *Des*[1].

[Revocation]

Two mechanisms are suggested to tackle the revocation problem. Firstly, the KGC maintains a revocation list RL. Under normal circumstances, when a

[1]In *Des*, an AES key can be included, so that the outcome could be broadcasted by the LBS provider in encrypted form under that AES key.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

vehicle $\mathcal{V}_i$ is compromised, the KGC first finds the corresponding $(ID_{\mathcal{V}_i}, w_i, x_i, v_i)$ in ML and then adds v_i to the revocation list RL. To detect whether a group signature $Sig = (t_1, t_2, T_3, t_4, s_\alpha, s_\beta, s_\gamma, s_{x_i}, s_\delta, s_\zeta, s_\eta)$ is generated by a revoked vehicle, the LBS provider checks $T_3 \stackrel{?}{=} \hat{e}(t_4, v_j)$ for all $v_j \in \mathsf{RL}$. If none of the equations holds, it means that the vehicle is not revoked. Secondly, when there are too many revoked vehicles in RL, we may allow the KGC to choose a threshold τ; and when the number of revoked vehicles in RL is greater than τ, the KGC updates its MEK and corresponding public key, and re-issues member keys for all the vehicles. This mechanism gives a trade-off between revocation checks by LBS providers and key updates for entities in a VANET. The key updates may cause heavy overhead in case of a very large-scale VANET. In Section 7.4, we further propose a hierarchical approach to alleviate the overhead so that the system can stay efficient even if the VANET hosts a large number of vehicles.

[Trace]

Let $Sig = (t_1, t_2, T_3, t_4, s_\alpha, s_\beta, s_\gamma, s_{x_i}, s_\delta, s_\zeta, s_\eta)$ be a valid group signature. To trace a vehicle, the KGC checks $T_3 \stackrel{?}{=} \hat{e}(t_4, v_i)$ for the tuple $(ID_{\mathcal{V}_i}, w_i, x_i, v_i)$ on ML. If this equation holds, KGC outputs $ID_{\mathcal{V}_i}$.

7.3 Evaluation

7.3.1 Security analysis

In this section, we analyze the security of the LBS protocol. The following analysis shows that the proposal meets all the security requirements described in Section 7.1.2.

First, we show that the message confidentiality and the vehicle privacy of

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Step 1 are satisfied.

- *Level 1 message confidentiality and vehicle privacy.* At this step, the ciphertext $cipher_2$ is generated by using the basic identity-based encryption (IBE) scheme which was proven secure by Boneh and Franklin [Bone01b]. Therefore, level 1 message confidentiality naturally follows. Furthermore, in each session of the protocol, a random value t is chosen. Therefore, in each session, C_3 and C_4 are different and independent from those in other sessions.

- *Level 2 message confidentiality and vehicle privacy.* In our protocol, the content of the LBS request is encrypted under the LBS provider's identity in $cipher_1$ using the Boneh and Franklin IBE scheme [Bone01b]. Only the designated LBS provider owns the secret key corresponding to this identity. Hence, even if the private key of the RSU is leaked to the attacker, no one except the vehicle and the designated LBS provider can read the content of the LBS request. Furthermore, in each session of the protocol, a random value s is chosen. Therefore, in each session, C_1 and C_2 are also different and independent from those in other sessions.

In Step 2, the RSU can decrypt $cipher_2$ to get $TP||ID_{\mathcal{L}_k}||cipher_1$. From $ID_{\mathcal{L}_k}$, the RSU can learn what kind of service the vehicle wants to access. However, since the RSU does not know the private key of the LBS provider, it cannot learn the content of $cipher_1$. Therefore, message confidentiality for this step is met. Furthermore, $cipher_1$ is also generated under the Boneh and Franklin IBE scheme. Vehicle privacy for this step accordingly follows.

Finally, we show that our protocol meets vehicle authentication, vehicle privacy and vehicle traceability of Step 3 as defined in Section 7.1.2.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

In this step, the LBS provider first decrypts the ciphertext $cipher_1$ to get $Des||Add||TP||Sig$. If Sig is a valid group signature, then the LBS provider is sure that the request comes from a registered vehicle. Hence, vehicle authentication is satisfied. Furthermore, the KGC can recover the identity of the vehicle, so vehicle traceability is satisfied. As to vehicle privacy, since anyone can generate $Des||Add||TP$, it is easy to see that $Des||Add||TP$ may not help the LBS provider to trace a vehicle. It remains Sig for the LBS provider to trace a vehicle. However, the group signature with verifier-local revocation has the property that it is computationally hard for anyone but the trusted third party (KGC in our scheme) to decide whether two different signatures were issued by the same member. Hence, Sig cannot help the LBS provider to trace a vehicle.

7.3.2 Transmission overhead

In this section, we examine the transmission delay incurred by the security and privacy mechanism. We will only deal with the delay in Step 1, which has a relatively crucial bandwidth limitation[2].

From our LBS protocol, it is easy to see that the length of an LBS request is equal to the length of $C_3||TP||ID_{\mathcal{L}}||C_1||Des||Add||TP||Sig$ in Step 1. Excluding $Des||Add$[3], it remains to evaluate the length of $C_3||TP||ID_{\mathcal{L}}||C_1||TP||Sig$. According to [Bone01a] and [Naka05], the length of a point in $\mathbb{G}$ and the length of Sig are 171 bits (about 22 bytes) and 362 bytes respectively. In addition, the length of TP is 4 bytes and the length of $ID_{\mathcal{L}}$ is 20 bytes. Hence, the length of $C_3||TP||ID_{\mathcal{L}}||C_1||TP||Sig$ is about 434 bytes.

[2]For Step 2 and 3, since we assume RSUs are connected to LBS providers by a wired network, the delay in these steps is much smaller than that in Step 1.

[3]These data are required even without any security and privacy mechanism. It is clearer to evaluate the cryptographic overhead without considering these data.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

According to DSRC [DSRC], the minimal data rate in DSRC is 6 Mbps. Hence, we have that the maximal transmission delay caused by the security and privacy mechanism at Step 1 is $\frac{434\times 8}{6\times 1024\times 1024}$ s $\approx$ 0.55 ms. This delay is very low for vehicles in VANETs.

7.3.3 Computational overhead

This section discusses the computational overhead at each step in our protocol. In the sequel, we will only consider the costly operations (*i.e.* bilinear map and point exponentiation operations). According to the execution time results shown in [Jian09], the measured processing time[4] for one bilinear map operation is about 1.87 ms and the time for one point exponentiation operation is about 0.49 ms.

At the first step, we notice that all point exponentiation operations can be pre-computed off-line. Therefore, this step only needs to compute two bilinear map operations on-line. The time is about 3.74 ms.

At the second step, an RSU only needs to compute one bilinear map operation to decrypt the ciphertext $cipher_2$. The time is about 1.87 ms.

For the last step, the LBS provider needs to calculate 17 point exponentiation operations and 2 bilinear map operations. The total time is about 12.07 ms.

Therefore, the total computational overhead at all the steps is about 17.68 ms. This is affordable for vehicles wishing to access LBS.

[4]For a super singular curve of embedded degree $k = 6$ over $F_{3^{97}}$ with a C program on an Intel CoreTM 2 Duo 2.0GHz Linux machine.

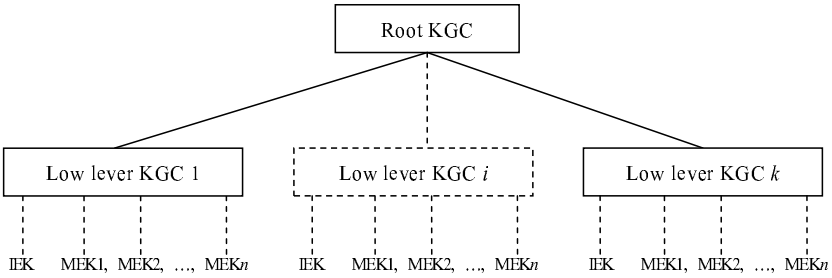

Figure 7.5: Hierarchical KGC and multi-issue Key

7.4 Hierarchical KGC and multi-issue key

In our basic system, we use a single KGC to generate private keys for RSUs and LBS providers, and issue member keys for vehicles. However, if there is a huge number of users in a VANET, the KGC may become a bottleneck: the KGC needs not only to generate private keys or member keys for a large number of users, but also to verify the identities of the users. Furthermore, as the number of vehicles in the revocation list grows, the performance of the system might decline. To let the system remain efficient even if a large number of vehicles are revoked, we introduce an approach referred to as hierarchical KGC and multi-issue key (HKMK). The idea of HKMK is illustrated in Figure 7.5.

In this approach, we use a two-level hierarchical KGC. A root KGC is used to issue certificates for low-level KGCs. As in our basic system, each low-level KGC has a single identity enrolment key (IEK) which is used to generate private keys for RSUs and LBS providers. However, unlike in our basic system, each low-level KGC has n different member enrolment keys (MEKs). When a vehicle joins the system, the low-level KGC randomly chooses one of its MEKs and generates a member key for this vehicle. In this way, vehicles in a domain are separated into n sub-groups and, when

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

a vehicle contacts an LBS provider for the LBS, the LBS provider can only learn that the vehicle belongs to a sub-group.

In what follows, we show how to set up the system parameters in the *System Setup* stage. We reformulate this stage into two sub-stages: *Root KGC Setup* and *Low-Level KGC Setup*. The description of each sub-stage comes as follows.

[Root KGC Setup]

At this stage, the root KGC initializes the system-wide parameters. It does the following:

1. Choose a cyclic group $\mathbb{G}$ and a cyclic multiplicative group $\mathbb{G}_T$ of the same order p, so that there exists a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, where $\mathbb{G}$ is generated by g.

2. Choose $u_0, u_1 \in \mathbb{G}$ and compute

$$\begin{cases} Y_1 = \hat{e}(u_0, g) \\ Y_2 = \hat{e}(u_1, g) \\ Y_3 = \hat{e}(g, g). \end{cases}$$

3. Choose a symmetric-key encryption scheme $\mathcal{E}_K(\cdot)/\mathcal{D}_K(\cdot)$.

4. Select cryptographic hash functions $H_0(\cdot) : \{0,1\}^* \longrightarrow \mathbb{G}$, $H_1(\cdot) : \{0,1\}^* \longrightarrow \mathbb{Z}_p^*$ and $H_2(\cdot) : \mathbb{G}_T \longrightarrow \{0,1\}^\lambda$.

5. Publish the system-wide parameters

$$\Psi = (\hat{e}, p, \mathbb{G}, \mathbb{G}_T, g, u_0, u_1, H_0, H_1, H_2, Y_1, Y_2, Y_3, \mathcal{E}_K(\cdot)/\mathcal{D}_K(\cdot)).$$

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Ψ is assumed to be pre-loaded in each low-level KGC, vehicle, RSU and LBS provider.

One may notice that the root KGC no longer needs to maintain a revocation list with the revocation tokens of the vehicles. Instead, the low-level KGCs will maintain their respective revocation lists.

[Low-Level KGC Setup]

After seeing the system-wide parameters, a low-level KGC generates its own parameters as follows:

1. Pick $\kappa \in \mathbb{Z}_p^*$ as its identity enrolment key (IEK) and n member enrolment keys (MEKs) $\rho_1, ..., \rho_n \in \mathbb{Z}_p^*$.
2. Compute $u_2 = g^{\kappa}$ and $u_{3i} = g^{\rho_i}, 1 \leq i \leq n$ as its master public key.
3. Compute $Y_{0i} = \hat{e}(u_0, u_{3i}), 1 \leq i \leq n$.
4. Publish the parameters as

$$\Omega = (u_2, u_{31}, ..., u_{3n}, Y_{01}, ..., Y_{0n}).$$

The low-level KGC also maintains n member lists $\mathsf{ML}_1, ..., \mathsf{ML}_n$ and revocation lists $\mathsf{RL}_1, ..., \mathsf{RL}_n$ corresponding to the n MEKs, respectively. To deal with the revocation problem more efficiently, similarly to our basic system, a low-level KGC chooses a threshold τ. If a vehicle $\mathcal{V}_i$ is compromised (we assume the member key of $\mathcal{V}_i$ is issued by using the j-th MEK, $1 \leq j \leq n$) and the number of vehicles in RL_j is not greater than τ, the low-level KGC first finds the revocation token of $\mathcal{V}_i$ in ML_j, then adds the revocation token to RL_j. Otherwise, the KGC updates its j-th MEK and corresponding public key u_{3j} and $Y_{0j} = \hat{e}(u_0, u_{3j})$, and re-issues member keys for all the vehicles in j-th sub-group.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

7.5 Summary

We have proposed a new location based service protocol that efficiently addresses the security and conditional privacy challenges inherent to offering LBSs in VANETs. In our system, both RSUs and LBS providers are identity-based, and a vehicle only needs a member key. With its member key, a vehicle can generate group signatures with verifier-local revocation. Those signatures can be validated by the LBS providers without violating the privacy of the vehicles. Furthermore, if an LBS request is found to be false, the key generation center can determine the identity of the vehicle. Our analysis shows that the security and privacy mechanisms proposed represent little extra overhead in a VANET, so that our scheme is a practical one.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Chapter 8

Conclusion

8.1 Concluding remarks

In this thesis, we have focused on providing security and privacy in VANETs. Several protocols were proposed to secure vehicular communications. Our first protocol (Chapter 4) is designed for mature VANETs, in which the RSUs are densely distributed. The second protocol (Chapter 5) is devised for VANETs in an early deployment stage, *i.e.* with few available RSUs, and it aims to process emergency announcements as soon as possible. The two protocols in Chapter 6 concentrate on signature aggregation/compression in VANETs, by noting that signatures might have to be stored for a long period for possible liability investigation. Our last protocol deals with value-added services in VANETs, and specifically it focuses on providing secure and privacy-preserving LBSs in vehicular networks.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

8.2 Future research

Some questions stay open for future research. One problem in the schemes for signature aggregation/compression in Chapter 6, in the PKI setting, is how to compress the public keys which have to be stored in the receiving vehicles; in the ID-based scenario, a problem is how to shorten VOA's public key, whose length is currently linear in the VANET size. Addressing these issues and improving the aggregate signatures will be very interesting to extensively deploy cryptographic authentication techniques in VANETs. The group signature schemes we used in our protocols all have a substantial signature length. They will cause heavy communication overhead for message relay and an expensive storage load for the purpose of supporting accident investigation. Therefore, designing short (especially aggregatable) group signature schemes which support fast batch verification is also regarded as a future challenge.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Our Published Contributions

[Chen09a] W. Chen, L. Zhang, B. Qin, Q. Wu and H. Zhang, "Certificateless One-Way Authenticated Two-Party Key Agreement Protocol", in *Fifth International Conference on Information Assurance and Security, IAS09*, pp. 483-486, 2009.

[Chen09b] W. Chen, B. Qin, Q. Wu, L. Zhang and H. Zhang, "ID-based Partially Blind Signatures: A Scalable Solution to Multi-Bank E-Cash", in *2009 International Conference on Signal Processing Systems, ICSPS 2009*, pp. 433-437, 2009.

[Zhan09a] L. Zhang and F. Zhang, "A New Certificateless Aggregate Signature Scheme", *Computer Communications*, vol. 32, no. 6, pp. 1079-1085, 2009.

[Zhan09b] L. Zhang and F. Zhang, "Certificateless Partially Blind Signatures", in *1st International Conference on Information Science and Engineering, ICISE2009*, pp. 2883-2886, 2009.

[Zhan09c] L. Zhang, Q. Wu and Bo Qin, "Identity-Based Verifiably Encrypted Signatures Without Random Oracles", in *The Provable Security Conference, ProvSec 2009*, LNCS 5848, pp. 76-89, 2009.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Zhan09d] L. Zhang, B. Qinm Q. Wu and Futai Zhang, "Novel Efficient Certificateless Aggregate Signatures", in *The 18th Symposium on Applied algebra, Algebraic algorithms, and Error Correcting Codes, AAECC 2009*, LNCS 5527, pp. 235-238, 2009.

[Zhan10a] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications", *IEEE Transactions on Vehicular Technology*, special issue on Cognitive Radios (to appear 2010).

[Zhan10b] L. Zhang, Q. Wu and B. Qin, "Authenticated Asymmetric Group Key Agreement Protocol and Its Application", in *IEEE International Conference on Communications, ICC 2010* (to appear 2010).

[Zhan10c] L. Zhang, F. Zhang, Q. Wu and J. Domingo-Ferrer, "Simulatable Certificateless Two-Party Authenticated Key Agreement Protocol", *Information Sciences*, vol. 180, no. 6, pp. 1020-1030, 2010.

[Zhan10d] L. Zhang, B. Qin, Q. Wu and F. Zhang, "Efficient Many-to-One Authentication with Certificateless Aggregate Signatures", *Computer Networks* (to appear 2010).

[Zhan10e] L. Zhang, Q. Wu, B. Qin and J. Domingo-Ferrer, "Identity-Based Authenticated Asymmetric Group Key Agreement Protocol", in *The 16th Annual International Computing and Combinatorics Conference, COCOON 2010*, LNCS (to appear 2010).

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Bibliography

[Abow97] G. Abowd, C. Atkeson, J. Hong, S. Long, R. Kooper, and M. Pinkerton, "CyberGuide: A Mobile Context-Aware Tour Guide", *ACM Wireless Networks*, vol. 3, no. 5, pp. 421-433, 1997.

[Ande96] R. Anderson and M. Kuhn, "Tamper resistance–a cautionary note", in *2nd Usenix Workshop on Electronic Commerce*, pp. 1-11, 1996.

[Bell93] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", in *ACM Conference on Computer and Communications Security, ACM CCCS 1993*, pp. 62-73, 1993.

[Bell98] M. Bellare, J. Garay and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures", in *Advances in Cryptology-Eurocrypt 1998*, LNCS 1403, pp. 236-250, 1998.

[Bell00] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E.V. Herreweghen and M. Waidner, "Design, implementation, and deployment of the iKP Secure Electronic Payment System", *IEEE Journal of Selected Areas in Communications*, vol. 18, no. 4, pp. 611-627, 2000.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Blau08] J. Blau, "Car talk", *IEEE Spectrum*, vol. 45, no. 10, pp. 16, 2008.

[Blum04] J. Blum and A. Eskandarian, "The threat of intelligent collisions", *IT Professional*, vol. 6, no. 1, pp. 24-29, 2004.

[Bold03] A. Boldyreva, "Threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman-group signature scheme", in *Public Key Cryptography, PKC 2003*, LNCS 2567, pp. 31-46, 2003.

[Bold07] A. Boldyreva, C. Gentry, A. O'Neill and D.H. Yum, "Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing", in *ACM Conference on Computer and Communications Security, ACM CCS 2007*, pp. 276-285, 2007.

[Bone01a] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the weil pairing", in *Advances in Cryptology-Asiacrypt 2001*, LNCS 2248, pp. 514-532, 2001.

[Bone01b] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in *Advances in Cryptology-CRYPTO 2001*, LNCS 2139, pp. 213-229, 2001.

[Bone03] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps", in *Advances in Cryptology-Eurocrypt 2003*, LNCS 2656, pp. 416-432, 2003.

[Bone04a] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation", in *ACM Conference on Computer and Communications Security, ACM CCS 2004*, pp. 168-177, 2004.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Bone04b] D. Boneh, X. Boyen and H. Shacham, "Short group signatures", in *Advances in Cryptology-CRYPTO 2004*, LNCS 3152, pp. 41-55, 2004.

[Boye03] X. Boyen, "Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography", in *Advances in Cryptology-CRYPTO 2003*, LNCS 2729, pp. 383-399, 2003.

[Car2car] Car 2 Car Communication Consortium.
`http://www.car-to-car.org/`

[Cala07] G. Calandriello, P. Papadimitratos, A. Lioy and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in VANET", in *ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2007*, pp. 19-28, 2007.

[Came07] J. Camenisch, S. Hohenberger and M. Pedersen, "Batch verification of short signatures", in *Advances in Cryptology-Eurocrypt 2007*, LNCS 4515, pp. 246-263, 2007.

[Cao06] T. Cao, D. Lin and R. Xue, "Security analysis of some batch verifying signatures from pairings", *International Journal of Network Security*, vol. 3, no. 2, pp. 112-117, 2006.

[Chau82] D. Chaum, "Blind signatures for untraceable payments", in *Advances in Cryptology-Crypto 1982*, Plenum Press, pp. 199-203, 1983.

[Chau91] D. Chaum and E. van Heijst, "Group signatures", in *Advances in Cryptology-Eurocrypt 1991*, LNCS 576, pp. 257-265, 1991.

[Chen05] X. Cheng, J. Liu and X. Wang, "Identity-based aggregate and verifiable encrypted signatures from bilinear pairing", in *International*

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Conference on Computational Science and its Applications, ICCSA 2005, LNCS 3483, pp. 1046-1054, 2005.

[Chen09] W. Chen, B. Qin, Q. Wu, L. Zhang and H. Zhang, "ID-based Partially Blind Signatures: A Scalable Solution to Multi-Bank E-Cash", in *2009 International Conference on Signal Processing Systems, ICSPS 2009*, pp. 433-437, 2009.

[Cheo06] J. Cheon, Y. Kim and H. Yoon, "A new id-based signature with batch verification", *Cryptology ePrint Archive*, Report 2004/131 2006. `http://eprint.iacr.org/2004/131.pdf`.

[Cheo07] J. Cheon and J. Yi, "Fast batch verification of multiple signatures", in *Public-Key Cryptography, PKC 2007*, LNCS 4450, pp. 442-457, 2007.

[Daza09] V. Daza, J. Domingo-Ferrer, F. Sebé and A. Viejo, "Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks", *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1876-1886, 2009.

[DSRC] Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ASTM E2213-03, Sep. 2003. `http://www.iteris.com/itsarch/html/standard/dsrc5ghz.htm`.

[Duri02] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Pérez, M. Singh and J.-M. Tang, "Framework for security and privacy in automotive telematics", in *2nd International Workshop on Mobile Commerce, WMC 2002*, pp. 25-32, September 2002.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[ERIZONWireless] ERIZONWireless. http://www.verizonwireless.com/.

[European] European Parliament. Legislative resolution on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 C6-0293/2005 2005/0182(COD)), 2005.

[Ferr09] A. Ferrara, M. Green, S. Hohenberger and M. Pedersen, "Practical short signature batch verification", in *RSA Cryptographers' Track, CT-RSA 2009*, LNCS 5473, pp. 309-324, 2009.

[Fons07] E. Fonseca, A. Festag, R. Baldessari and R. L. Aguiar, "Support of anonymity in VANETs - Putting pseudonymity into practice", in *IEEE Wireless Communications and Networking Conference, WCNC 2007*, pp. 3400-3405, 2007.

[Freu07] J. Freudiger, M. Raya and M. Feleghhazi, "Mix zones for location privacy in vehicular networks", in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems, WiN-ITS 2007*, 2007.

[Frey94] G. Frey and H.-G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, vol. 62, no. 206, pp. 865-874, 1994.

[Galb06] S. D. Galbraith, K. G. Paterson and N. P. Smart, "Pairings for cryptographers".
`http://eprint.iacr.org/2006/165.pdf`.

[Gent06] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures", in *Public Key Cryptography, PKC 2006*, LNCS 3958, pp. 257-273, 2006.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Gerl05] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker and C. Harsch, "Security architecture for vehicular communication", in *International Workshop on Intelligent Transportation-WIT,* Hamburg, Germany, Mar. 2005. http://www.network-on-wheels.de/downloads/wit07secarch.pdf.

[Goll02a] L. Gollan and C. Meinel, "Digital Signatures for Automobiles", Technical Report, Institut für Telematik e.V., Trier, 2002. http://www.telematik-institut.org/publikationen/technische_berichte/2002/Prep012002.pdf

[Goll02b] L. Gollan and C. Meinel, "Digital signatures for automobiles", in *Systemics. Cybernetics and Informatics, SCI 2002*, 2002. http://www.hpi.uni-potsdam.de/fileadmin/hpi/FG_ITS/papers/DigitalSignaturesAuto02.pdf.

[Goll10c] P. Golle, D. Greene and J. Staddon, "Detecting and correcting malicious data in VANETs", in *ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2004*, pp. 29-37, 2004.

[Grot07] J. Groth, "Fully anonymous group signatures without random oracles", in *Advances in Cryptology-Asiacrypt 2007*, LNCS 4833, pp. 164-180, 2007.

[Guo07] J. Guo, J. P. Baugh and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework", in *2007 Mobile Networking for Vehicular Environments*, pp. 103-108, 2007.

[Herr06] J. Herranz, "Deterministic identity-based signatures for partial aggregation", *The Computer Journal*, vol. 49, no. 3, pp. 322-330, 2006.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Hess06] F. Hess, N.P. Smart and F. Vercauteren, "The Eta pairing revisited", *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4595-4602, 2006.

[Huba04a] J. Hubaux, S. Ĉapkun and J. Luo, "The security and privacy of smart vehicles", *IEEE Security and Privacy*, vol. 2, no. 3, pp. 49-55, 2004.

[Huba04b] J.P. Hubaux, "The security and privacy of smart vehicles", *IEEE Security and Privacy*, vol. 2, no. 3, pp. 49-55, 2004.

[Jian09] Y. Jiang, M. Shi, X. Shen and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication trees", *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974-1983, 2009.

[Karg95] P. Karger and Y. Frankel, "Security and privacy threats to ITS", in *Second World Congress on Intelligent Transport Systems*, vol. 5, pp. 2452-2458, 1995.

[Koch96] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", in *Advances in Cryptology-CRYPTO 1996*, LNCS 1109, pp. 104-113, 1996.

[KVH] KVH Industries, Inc.
`http://www.kvh.com/`.

[Lee99] J.-H. Lee and H. Lee-Kwang, "Distributed and cooperative fuzzy controllers for traffic intersections group", *IEEE Transactions on Systems, Man and Cybernetics*, vol. 29, no. 2, pp. 263-271, 1999.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Lee07] S. Lee, G. Pan, J. Park, M. Gerla and S. Lu, "Secure incentives for commercial ad dissenmination in vehicular networks", in *ACM International Symposium on Mobile Ad Hoc Networking & Computing*, pp. 150-159, 2007.

[Li07] C. Li, G. Yang, D. Wong, X. Deng and S. Chow, "An efficient signcryption scheme with key privacy", in *European PKI Workshop, EuroPKI 2007*, LNCS 4582, pp. 78-93, 2007.

[Lin07] X. Lin, X. Sun, P. Ho and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications", *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, 2007.

[Lu08] R. Lu, X. Lin, H. Zhu, P. Ho and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications", in *IEEE INFOCOM 2008*, pp. 1229-1237, 2008.

[Lu06] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham and B. Waters, "Sequential aggregate signatures and multisignatures without random oracles", in *Advances in Cryptology-Eurocrypt 2006*, LNCS 4004, pp. 465-485, 2006.

[Lysy04] A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, "Sequential aggregate signatures from trapdoor permutations", in *Advances in Cryptology-Eurocrypt 2004*, LNCS 3027, pp. 514-532, 2004.

[Mastercard] Mastercard and Visa, *SET protocol specifications*, 1997. `http://www.setco.org/set_specifications.html`

[Matt09] B.J. Matt, "Identification of multiple invalid signatures in pairing based batched signatures", in *Public-Key Cryptography, PKC 2009*, LNCS 5443, pp. 337-356, 2009.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Mene93] A. Menezes, T. Okamoto and S.A. Vanstone, "Reducing elliptic curves logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639-1646, 1993.

[Msntv] Microsoft Corp.'s MSN TV.
`http://www.msntv.com/`.

[Miya01] A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE Transactions on Fundamentals*, vol. E84-A, no. 5, pp. 1234-123, 2001.

[Multiprecision] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIR-ACL).
`http://www.shamus.ie/`.

[Naka05] T. Nakanishi and N. Funabiki, "Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps", in *Advances in Cryptology-Asiacrypt 2005*, LNCS 3788, pp. 533-548, 2005.

[National] National ITS Architecture.
`http://www.iteris.com/itsarch/index.htm`

[NextBus] NextBus Inc., http://www.nextbus.com/, Jan. 2004.

[NOW] NOW: Network on Wheels.
`http://www.network-on-wheels.de/`.

[NS2] The Network Simulator - ns.
`http://nsnam.isi.edu/nsnam/index.php/MainPage`.

[Okam98] T. Okamoto, "A digital multisignature scheme using bijective public-key cryptosystems", *ACM Transactions on Computer Systems*, vol. 6,, no. 4, pp. 432-441, 1998.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Papa06] P. Papadimitratos, V. Gligor and J. Hubaux, "Securing vehicular communications - Assumptions, requirements, and principles", in *Workshop on Embedded Security in Cars, ESCAR 2006*, pp. 5-14, 2006.

[Papa07] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung and M. Raya, "Architecture for secure and private vehicular communications", in *International Conference on ITS Telecommunications*, pp. 1-6, 2007.

[Parn05] B. Parno and A. Perrig, "Challenges in securing vehicular networks", in *Workshop on Hot Topics in Networks, HotNets-IV 2005*, 2005.
`http://conferences.sigcomm.org/hotnets/2005/papers/parno.pdf`.

[Pate06] K. Paterson and J. Schuldt, "Efficient identity-based signatures secure in the standard model", in *Information Security and Privacy, ACISP 2006*, LNCS 4058, pp. 207-222, 2006.

[Picc06] F. Picconi, N. Ravi, M. Gruteser and L. Iftode, "Probabilistic validation of aggregated data in vehicular ad hoc networks", in *The Third ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2006*, pp. 76-85, 2006.

[Pool09] N. Poolsappasit and I. Ray, "Towards achieving personalized privacy for location-based services", *Transactions on Data Privacy*, vol. 2, no. 1, pp. 77-99, 2009.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Qin09] B. Qin, Q. Wu, W. Susilo and Y. Mu, "Publicly verifiable privacy-preserving group decryption", in *The 5th China International Conference on Information Security and Cryptology, Inscrypt 2008*, LNCS 5487, pp. 84-95, 2009.

[Raya05] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks", in *ACM Workshop on Security of Ad hoc and Sensor Networks, SASN 2005*, pp. 11-21, 2005.

[Raya06] M. Raya, A. Aziz and J.-P. Hubaux, "Efficient secure aggregation in VANETs", in *The 3rd International Workshop on Vehicular Ad hoc Networks, VANET 2006*, pp. 67-75, 2006.

[Raya07] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007.

[Reed98] J. Reed, K. Krizman, B. Woerner, and T. Rappaport, "Challenges and Progress in Meeting the E-911 Requirement for Location Service", *IEEE Personal Communications Magazine*, vol. 5, no. 3, pp. 30-37, 1998.

[Saha04] A.K. Saha and D.B. Johnso, "Modeling mobility for vehicular ad hoc networks", in *ACM International Workshop on Vehicular Ad Hoc Networks, VANET 2004*, pp. 91-92, 2004.

[Samp05] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura and K. Sezaki, "CARAVAN: Providing location privacy for VANET", in *Embedded Security in Cars, ESCAR 2005*, 2005. `http://www.ee.washington.edu/research/nsl/papers/ESCAR-05.pdf`.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Samp07] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET", *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569-1589, 2007.

[Scot07] M. Scott, "Efficient implementation of cryptographic pairings". `http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscott-samos07.pdf`.

[Secure] Secure Vehicle Communication. `http://www.sevecom.org/`.

[Sham79] A. Shamir, "How to share a secret", *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[Sham84] A. Shamir, "Identity based cryptosystems and signature schemes", in *Advances in Cryptology-CRYPTO 1984*, LNCS 196, pp. 47-53, 1984.

[Sham01] A. Shamir and Y. Tauman, "Improved online/offline signature schemes", in *Advances in Cryptology-Crypto 2001*, LNCS 2139, pp. 355-367, 2001.

[Shin08] H. Shin, V. Atluri, J. Vaidya. "A profile anonymization model for privacy in a personalized location based service environment, in *The Ninth International Conference on Mobile Data Management*, pp. 73-80. IEEE Computer Society, 2008.

[Sola08a] A. Solanas, J. Domingo-Ferrer and A. Martínez-Ballesté, "Location privacy in location-based services: beyond TTP-based schemes", in *The 1st International Workshop on Privacy in Location-Based Applications, PiLBA 2008*, 2008.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Sola08b] A. Solanas and A. Martínez-Ballesté, "A TTP-free protocol for location privacy in location-based services", *Computer Communications*, vol. 31, no. 6, pp. 1181-1191, 2008.

[Sprint] http://www.sprint.com.

[Stan09] F. Standaert, T. Malkin and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks", in *Advances in Cryptology-Eurocrypt 2009*, LNCS 5479, pp. 443-461, 2009.

[Tell08] J. Téllez-Isaac, J. Sierra-Cámara, S. Zeadally and J. Torres-Márquez, "A Secure vehicle to roadside communication payment protocol in vehicular ad hoc networks", *Computer Communications*, vol. 31, no. 10, pp. 2478-2484, 2008.

[USDe] U.S. Department of Transportation, National highway traffic safety administration, Vehicle Safety Communications Project, Final Report. Appendix H: WAVE/DSRC Security, April 2006.

[Viej09] A. Viejo, F. Sebé and J. Domingo-Ferrer, "Aggregation of trustworthy announcement messages in vehicular ad hoc networks", in *IEEE 69th Vehicular Technology Conference, VTC2009-Spring*, 2009. `http://crises-deim.urv.cat/webCrises/publications/bcpi/Aggregation_VTCconf.pdf`.

[Wase08] A. Wasef, Y. Jiang and X. Shen, "ECMV: Efficient certificate management scheme for vehicular networks", in *IEEE GLOBECOM 2008*, pp. 1-5, 2008.

[Wase09] A. Wasef and X. Shen, "ASIC: Aggregate signatures and certificates verification scheme for vehicular networks". `http://www.engine.lib.uwaterloo.ca`.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[WAVE] IEEE trial-use standard for wireless access in vehicular environments (WAVE), IEEE Std 1609.2-2006, 2006.
`http://ieeexplore.ieee.org/servlet/opac?punumber=11000`.

[Wei05] V. K. Wei, T. H. Yuen and F. Zhang, "Group signature where group manager, members and open authority are identity-based", in *Information Security and Privacy, ACISP 2005*, LNCS 3574, pp. 468-480, 2005.

[Wu10] Q. Wu, J. Domingo-Ferrer and U. González-Nicolás, "Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559-573, 2010.

[Xu05] J. Xu, Z. Zhang and D. Feng, "ID-based aggregate signatures from bilinear pairings", in *Cryptology and Network Security, CANS 2005*, LNCS 3810, pp. 110-119, 2005.

[Yen95] S.M. Yen and C.S. Laih, "Improved digital signature suitable for batch verification", *IEEE Transactions on Computers*, vol. 44, no. 7, pp. 957-959, 1995.

[Yoon05] H. Yoon, J. H. Cheon and Y. Kim, "Batch verifications with ID-based signatures", in *Information Security and Cryptology, ICISC 2004*, LNCS 3506, pp. 233-248, 2005.

[Zark02] M. Zarki, S. Mehrotra, G. Tsudik and N. Venkatasubramanian, "Security issues in a future vehicular network", in *European Wireless*, 2002.
`http://www.ics.uci.edu/~dsm/papers/sec001.pdf`.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Zhan08a] C. Zhang, X. Lin, R. Lu and P. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks", in *IEEE International Conference on Communications, ICC 2008*, pp. 19-23, 2008.

[Zhan08b] C. Zhang, R. Lu, X. Lin, P. Ho and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks", in *IEEE INFOCOM 2008*, pp. 246-250, 2008.

[Zhan09a] L. Zhang, B. Qin, Q. Wu and F. Zhang, "Novel efficient certificateless aggregate signatures", in *The 18th Symposium on Applied algebra, Algebraic algorithms, and Error Correcting Codes, AAECC 2009*, LNCS 5527, pp. 235-238, 2009.

[Zhan09b] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme", *Computer Communications*, vol. 32, no. 6, pp. 1079-1085, 2009.

[Zhan09c] L. Zhang and F. Zhang, "Certificateless Partially Blind Signatures", in *1st International Conference on Information Science and Engineering, ICISE2009*, pp. 2883-2886, 2009.

[Zhan10a] L. Zhang, F. Zhang, Q. Wu and J. Domingo-Ferrer, "Simulatable Certificateless Two-Party Authenticated Key Agreement Protocol", *Information Sciences*, vol. 180, no. 6, pp. 1020-1030, 2010.

[Zhan10b] L. Zhang, B. Qin, Q. Wu and F. Zhang, "Efficient Many-to-One Authentication with Certificateless Aggregate Signatures", *Computer Networks*, (to appear).

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

[Zhen97] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost(encryption)", in *Advances in Cryptology-CRYPTO 1997*, LNCS 1294, pp. 165-179, 1997.

[Zhu08] H. Zhu, X. Lin, R. Lu, P. Ho and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks", in *IEEE International Conference on Communications, ICC 2008*, pp. 1436-1440, 2008.

UNIVERSITAT ROVIRA I VIRGILI
RESEARCH ON SECURITY AND PRIVACY IN VEHICULAR AD HOC NETWORKS
Lei Zhang
ISBN:978-84-693-8865-5/DL:T.1942-2010

Lei Zhang

June 2010