Secure and Privacy-Preserving Vehicular Communications

by

Xiaodong Lin

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2008

©Xiaodong Lin, 2008

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

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

Abstract

Road safety has been drawing increasing attention in the public, and has been subject to extensive efforts from both industry and academia in mitigating the impact of traffic accidents. Recent advances in wireless technology promise new approaches to facilitating road safety and traffic management, where each vehicle (or referred to as On-board unit (OBU)) is allowed to communicate with each other as well as with Roadside units (RSUs), which are located in some critical sections of the road, such as a traffic light, an intersection, and a stop sign. With the OBUs and RSUs, a self-organized network, called Vehicular Ad Hoc Network (VANET), can thus be formed. Unfortunately, VANETs have faced various security threats and privacy concerns, which would jeopardize the public safety and become the main barrier to the acceptance of such a new technology. Hence, addressing security and privacy issues is a prerequisite for a market-ready VANET. Although many studies have recently addressed a significant amount of efforts in solving the related problems, few of the studies has taken the scalability issues into consideration. When the traffic density is getting large, a vehicle may become unable to verify the authenticity of the messages sent by its neighbors in a timely manner, which may result in message loss so that public safety may be at risk. Communication overhead is another issue that has not been well addressed in previously reported studies. Many efforts have been made in recent years in achieving efficient broadcast source authentication and data integrity by using fast symmetric cryptography. However, the dynamic nature of VANETs makes it very challenging in the applicability of these symmetric cryptography-based protocols.

In this research, we propose a novel Secure and Efficient RSU-aided Privacy Preservation Protocol, called $SERP^3$, in order to achieve efficient secure and privacy-preserving Inter-Vehicle Communications (IVCs). With the commitments of one-way key chains distributed to vehicles by RSUs, a vehicle can effectively authenticate any received message from vehicles nearby even in the presence of frequent change of its neighborship. Compared with previously reported public key infrastructure (PKI)-based packet authentication protocols for security

and privacy, the proposed protocol not only retains the security and privacy preservation properties, but also has less packet loss ratio and lower communication overhead, especially when the road traffic is heavy. Therefore, the protocol solves the scalability and communication overhead issues, while maintaining acceptable packet latency. However, RSU may not exist in some situations, for example, in the early stage deployment phase of VANET, where unfortunately, $SERP^3$ is not suitable. Thus, we propose a complementary Efficient and Cooperative Message Validation Protocol, called ECMVP, where each vehicle probabilistically validates a certain percentage of its received messages based on its own computing capacity and then reports any invalid messages detected by it.

Since the ultimate goal of designing VANET is to develop vehicle safety/non-safety related applications to improve road safety and facilitate traffic management, two vehicle applications are further proposed in the research to exploit the advantages of vehicular communications. First, a novel vehicle safety application for achieving a secure road traffic control system in VANETs is developed. The proposed application helps circumvent vehicles safely and securely through the areas in any abnormal situation, such as a car crash scene, while ensuring the security and privacy of the drivers from various threats. It not only enhances traveler safety but also minimizes capacity restrictions due to any unusual situation. Second, the dissertation investigates a novel mobile payment system for highway toll collection by way of vehicular communications, which addresses all the issues in the currently existing toll collection technologies.

Acknowledgments

Finishing my Ph.D. dissertation would be impossible without the help, advice and support of people. There is no any word that I can use to express my feelings and appreciation to them. It is also impossible to list here all those individuals whom I am deeply indebted. Needless to say that my Ph.D. co-advisors, Dr. Xuemin (Sherman) Shen and Dr. Pin-Han Ho, played major roles. I would like to express my gratitude to Dr. Shen and Dr. Ho for their understanding, constructive advices, encouragement and personal guidance. They not only help me to develop the academic skills, but also guide me to strive for excellence. I would also like to thank Prof. Wenjing Lou for serving as my dissertation external examiner and sharing her invaluable insight on wireless networking and security with me. I would also like to extend my appreciation to the other members of my examing committee, Prof. Ajit Singh, Prof. Sagar Naik, and Prof. Xinzhi Liu, for the time and efforts to read my dissertation. In spite of their busy schedules, all have been readily available for advice, reading, or simply a word of encouragement. Further, my deep thanks to Prof. Weidong Tian for serving as the delegated dissertation committee member.

I would like to thank all the members in the Broadband Communications Research (BBCR) Group for continued support and warm working atmosphere. It is indeed a great honor to work with so many great talents during my Ph.D. study at the University of Waterloo. Special thanks go to Dr. Rongxing Lu, Mr. Chenxi Zhang, Mrs. Xiaoting Sun and Mr. Haojin Zhu for day-and-night discussion and continuous support throughout my graduate study.

Thanks to the administrative and technical supporting staffs, Wendy Boles, Karen Schooley, Annette Dietrich, Lisa Hendel, Wendy Stoneman, Deborah Perchaluk, Lisa Szepaniak, Sandra Rivers, Mary McColl, Anne Jenson, Paul Ludwig and Philip Regier.

Thanks to the ECE (Electrical and Computer Engineering) GSA (Graduate Student Association) council members, Fariborz Rahimi and Mehrdad Hosseini Zadeh for working with me to organize and promote social events for ECE graduate students. Thanks to Prof. Paul A.S. Ward, Prof. Sagar Naik and Prof. Gordon B. Agnew for sharing their teaching experiences with me.

Grateful acknowledgement is made for financial support from the Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral, the Provincial Centre of Excellence Communications and Information Technology Ontario (CITO), Ontario, Canada. Thanks to the University of Waterloo for numerous scholarships.

Finally, my special thanks go to my wife, Fei Yang, for the loving support and patience she has for me to fulfil my career goals.

To my dear forever beloved grandmother Mrs. Xiulin Li who raised me up

Contents

List of Tables

List of Figures

List of Abbreviations

ABS	Anti-lock braking system
CWBS	Collision warning with brake support
CRL	Certificate revocation list
DoS	Denial of service
DSRC	Dedicated Short Range Communication
EBL	Extended brake light
ECC	Elliptic curve cryptography
ETC	Electronic toll collection
FCC	Federal Communications Commission
HIPAA	Health insurance portability and accountability act
IBC	Identity-based cryptography
ITS	Intelligent Transportation Systems
IVC	Inter-Vehicle Communication
LPR	License plate recognition
MAC	Message authentication code
MTO	Ministry of Transportation
OBU	On-Board unit
PKI	Public key infrastructure

RSU	Roadside unit
SUV	Sport utility vehicle
TPD	Tamper-proof device
V2I	Vehicle-to-infrastructure
V2V	Vehicle-to-vehicle
VANET	Vehicular Ad Hoc Network
VSC	Vehicle Safety Communications
VSCC	Vehicle Safety Communications (VSC) Consortium
USDOT	United States Department of Transportation
WAVE	Wireless Access in Vehicular Environment

Chapter 1

Introduction

1.1 Background

Impaired driving, traffic congestion, and treacherous driving conditions have caused numerous accidents every year all over the world, leading to great suffering to people in different ways such as great anguish, fatal injuries and horrendous losses of human lives. There were nearly 6,420,000 auto accidents in the United States in 2005 where 2.9 million people were injured and 42,636 people killed, which cause a financial loss of more than 230 billion dollars. By statistics, about five people die every hour in vehicle crashes in the United States, that is one death every 12 minutes [1]. Under such a circumstance, how to improve driving safety has been drawing increasing attention in the public and has been subject to extensive efforts from both industry and academia in mitigating the impact of traffic accidents and injuries. For example, car manufacturers have made great efforts to improve the safety of their vehicles by developing "passive" vehicle safety systems, such as seat belts, air bag systems and crumple zones, which look to minimize post-crash driver and passenger injury, as well as by accommodating "active" vehicle safety systems that explore pre-collision accident avoidance, such as Anti-lock Braking System (ABS) brakes, blind-spot safety, roll stability control, active steering systems,

collision warning with brake support (CWBS), Lane Departure Warning System and Mazda Pre-crash Safety System [2]. Although the aforementioned safety technologies have led to enormous improvements on driving safety over the last few decades, we still witness tremendous loss on the roads. Hence, it is crucial to explore the new techniques to improve road safety.

Over the last twenty years, the miraculous evolution of wireless technology has imposed a major impact on the revolution of human's lifestyle by providing the best ever convenience and flexibility in accessing the Internet services and various types of personal communication applications. Recently, technologies built on 802.11p and IEEE 1609 standards, 5.9 GHz Dedicated Short Range Communications (DSRC) protocols [3], are proposed to support advanced vehicle safety applications through effective, reliable, and secure vehicle-to-vehicle (V2V) (also known as Inter-Vehicle Communication (IVC)) and vehicle-to-infrastructure (V2I) communications, which are also known as Vehicle Safety Communications (VSC) technologies. U.S. Department of Transportation (USDOT) works with seven automotive manufacturers - BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VW - to form the Vehicle Safety Communications (VSC) Consortium (VSCC) to establish the VSC project to evaluate vehicle safety applications enabled or enhanced by external vehicle communications [4]. For example, if a possible red light violation is detected at an intersection, the potential violator will receive a warning to slow down to avoid unintentional red light violations. Meanwhile, a warning on the running red light event will be given to the other drivers at the intersection thereby minimizing the possibility of collision.

1.2 DSRC and VANET

1.2.1 DSRC

Dedicated Short Range Communications (DSRC) is one of short-range wireless protocols, which is specifically designed for V2V and V2I communications to enhance the safety and the productivity of the transportation system, which is also referred to Intelligent Transportation System (ITS). Originally, DSRC is proposed to work in the 915 MHz band, and US Federal Communications Commission (FCC) later allocated 75 MHZ of spectrum at 5.9 GHz for DSRC in 1999. Similar activities also undergo in Japan and Europe, where 5.8 GHz band is used for DSRC instead. The DSRC radio technology is a variant of the IEEE 802.11a technology [5], which provides high data transfer rates of up to 27 Mb/s over a range of 1km while maintaining low overhead in the DSRC spectrum. Recently, both industry and academia have been extensively working on standardization of DSRC. One of the activities is done by the IEEE P1609 Working Group, which is currently working on the IEEE 802.11p standard for both PHY and MAC layer of DSRC, as well as applications and management services over DSRC, which are also known as Wireless Access in Vehicular Environments (WAVE). Furthermore, VSC adopts IEEE 1609 standards to develop many DSRC/WAVE applications, which can be categorized into the following two classes according to different aspects of their design premises and abilities.

- Vehicle safety-related applications: which are used to improve road safety. For example, currently, drivers can only see the brake light of vehicles ahead of them; and the brake light system can only demonstrate whether the vehicle is braking, but cannot indicate the level of deceleration. When there is an emergency braking, drivers may not see the break lights of any other vehicles but the one in front of them, especially, when visibility is poor beyond the car in front of them (in fog), or in heavy traffic when everyone is so close or behind bigger vehicles like

minivans, trucks, and Sport Utility Vehicles (SUVs). Under such a circumstance, rear-end collisions could happen with a much larger chance. To countermeasure the situation, V2V communication can serve to extend the range of brake light signals for the drivers and as well indicate the level of deceleration (or referred to as Extended Brake lights (EBL)) [4]. Through the V2V communication, the hard braking information of a vehicle is disseminated in a timely fashion so that the other vehicles can be alerted.

- Vehicle non-safety-related applications: which are used to facilitate traffic management and infotainment dissemination for drivers and passengers. For example, in the modern transportation systems, traffic lights take an important role in automatically performing traffic control and management in urban areas, which not only enhance the driver safety but also facilitate smooth multiplexing at the intersections. Hence, much attention has been put to make traffic light controllers more intelligent, where collecting traffic related information plays an important role in traffic flow control. Currently, this has been done by equipping the traffic lights with sensing devices such as electromagnetic wires (loops), which are embedded in street pavement. However, deploying sensors in pavement at an intersection could be very expensive and difficult to maintain. In addition, the sensors can become inaccurate and fail to regularly function as time goes by. However, V2I communication can be used to effectively collect traffic information. Through V2I communication, an RSU at an intersection can probe the traffic load in all directions of the intersection, and then intelligently control the corresponding traffic light according to the dynamic traffic load.

1.2.2 VANET

Nowadays, car manufactories and telecommunication industries have been gearing up to equip each car with the technology that allows drivers and passengers to communicate

with each other as well as with a roadside infrastructure that may be located in some critical sections of the road, such as at every traffic light or any intersection or stop sign, in order to improve the driving experience and make driving safer. For example, Microsoft Corp.'s MSN TV and KVH Industries, Inc. have introduced an automotive vehicle Internet access system called TracNet, which can bring the Internet service to any in-car video screens. It also turns the entire vehicle into an IEEE 802.11-based Wi-Fi hotspot, so passengers can use their wireless-enabled laptops to go online like they are home or in the office. Furthermore, by using those equipped communication devices, also known as On-Board Units (OBUs), vehicles can communicate with each other as well as with the Roadside units (RSUs) located in the critical points of the road. As shown in Fig. 1.1, a self-organized network can be formed by connecting the vehicles and RSUs, which is called Vehicular Ad Hoc Network (VANET), and the RSUs are further connected to the backbone network via the high speed network connections. An increasing interest has been raised recently on the applications through V2V and V2I communications, aiming to improve driving safety and traffic management while providing drivers and passengers with Internet access. It is estimated that the market for vehicular communications will reach to multi-billions dollars by 2012.

In VANETs, RSUs can provide assistance in finding the facilities such as restaurants and gas stations, and broadcast traffic-related messages such as "maximum curve turning speed" notifications to give drivers a heads up. For example, a vehicle can communicate to a traffic light through V2I communications, and traffic light can indicate to the vehicle when turning to yellow or red. This can be served as an advance-warning sign to the drivers, and will be very helpful to the drivers when they are driving during winter weather conditions or in an unfamiliar area, especially when facing a wide angle of road curve ahead of a traffic light. This could reduce the occurrence of red light running with a disaster circumstance. Through V2V communications, on the other hand, the drivers can get a better awareness of what's going on in their driving environment

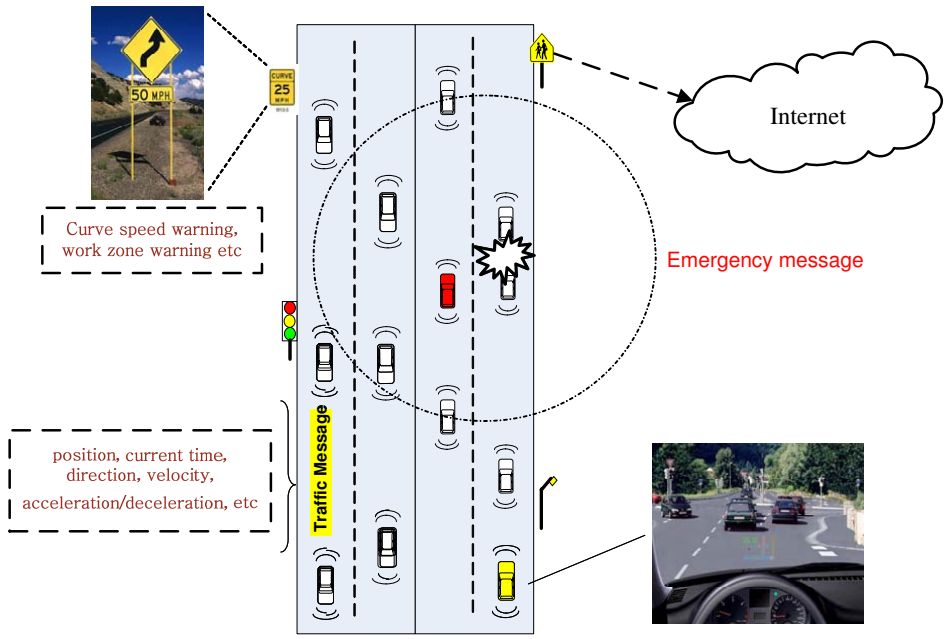


Figure 1.1: Vehicular ad hoc network

and take early actions to respond to an abnormal situation. For achieving this, an OBU regularly broadcasts routine traffic-related messages with the information of position, current time, driving direction, speed, brake status, steering angle, turn signal, acceleration/deceleration, traffic conditions, and traffic events. In addition, emergency messages can be generated and sent by OBUs in case of emergent braking, traffic jam, or any accident, etc. For example, as shown in Fig. 1.2, whenever there is an accident on a highway, several lanes can be blocked. Drivers can experience a long delay. However, the delay can be mitigated if drivers are informed in advance so that they can follow detour route or change lane to avoid a traffic jam.

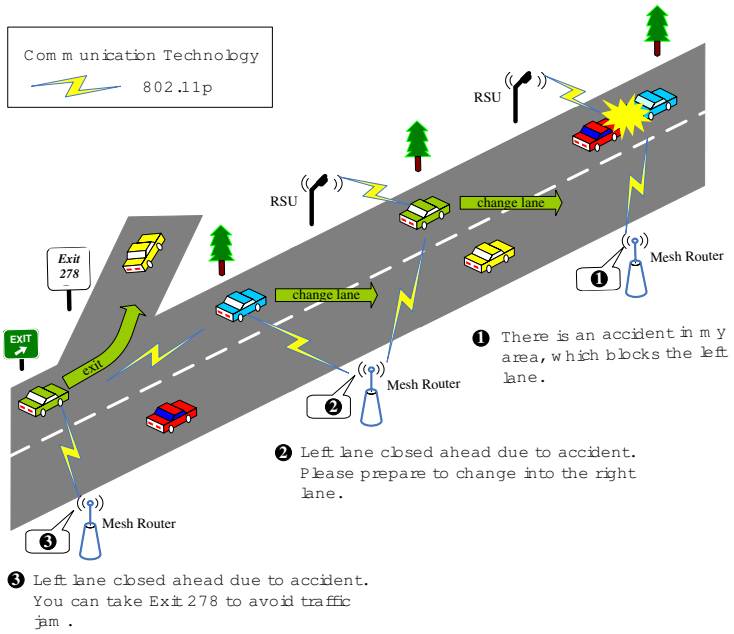


Figure 1.2: An example of road emergency response operation under VANET

1.3 Research Motivations and Objectives

1.3.1 Motivations

The creation of VANETs is obviously a great plus to the road driving safety and traffic management. However, the design of VANETs comes with a set of newly emerged challenges, especially in the aspects of security and privacy. As a special implementation of mobile ad hoc networks (MANETs), VANETs inherit all the known and unknown security weaknesses. Any malicious behavior of users, such as a modification and replay on the disseminated messages, could be fatal to other users. In addition, the issues on VANET security become more challenging due to the unique features of the networks, such as high mobility and an extremely large amount of network entities (i.e., the vehicles). Furthermore, conditional privacy preservation must be achieved in the sense that the user-related privacy information, including the driver's name,

the license plate, speed, position, and traveling routes along with their relationship, has to be protected; while the authorities should be able to reveal the identities of message senders in the event of traffic disputes, such as a crime/car accident scene investigation. Hence, addressing security and privacy issues is a prerequisite for any vehicle applications based on VANETs. To sum up the above, it is obviously a critical task to develop a suite of carefully designed security mechanisms for achieving security and conditional privacy preservation in a VANET. Until recently, however, security and privacy issues of VANETs have been subject to little attention, which has formed a major barrier that prevents many car manufacturers from employing the state-of-the-art wireless communication devices.

Security Threats

There are several possible security attacks in VANETs, which are listed as follows:

- Bogus information attack: The adversary may send fake messages to meet a specific purpose. For example, one may send a fake approaching emergency vehicle warning in order to push over the others such that it can manipulate to get a better traffic condition.

- Unauthorized preemption attack: An RSU could be used to control a traffic light when any emergent situation occurs. Similar to the bogus information attack, the adversary may illegally interrupt a traffic light through the RSU in order to meet some specific purposes [6].

- Message replay attack: The adversary replays the valid messages sent by a legitimate user some time before in order to disturb the traffic.

- Message modification attack: A message is altered during or after transmission. The adversary may wish to change the source or content of the message in terms

of the position and/or time information that had been sent and saved in its device to escape from the consequence of a criminal/car accident event.

- Impersonation attack: The adversary may pretend to be another vehicle or even an RSU to fool the others.
- RSU replication attack: An RSU may be compromised such that the adversary can relocate the compromised RSU to launch any malicious attack, such as broadcasting fake traffic information.
- Denial of service (DoS) attack: The adversary sends irrelevant bulk messages to take up the channels and consume the computational resources of the other nodes, such as RF interference or jamming or layer 2 packet flooding [7].

Privacy Threats

Since a VANET is on an open shared medium, which allows illegal collection and processing of information easy to happen. After the adversary intercepts a significant amount of messages in a certain region, the adversary may trace a vehicle in terms of its physical position and moving patterns simply through information analysis. Since drivers concern the leakage of the aforementioned sensitive information to the public, resolving the concern becomes one of the major issues in the design of a modern VANET.

- Personal information leakage: If information transmitted over a VANET is not protected, an adversary can easily collect the information by sniffing the network and discover some user-related sensitive information, such as a driver's name, address, license. The personal identification information leakage could result in identity theft, which may disrupt a person's life.

- Location privacy: After an adversary intercepts a significant amount of messages in a certain region, the adversary may be able to trace a vehicle in terms of its physical position and moving patterns simply through information analysis.

Since the topic on DoS attacks in wireless communication networks has been extensively investigated [8–11], in this study, we will focus on the security and privacy issues which are not related to the DoS attack.

Traceability

Traceability is another very crucial issue in VANETs. It is very common to have an emergency or a dispute on our roads, and it is always the road authority's desire and enthusiasm to find someone who may be able to provide valuable information about the incident. Hence, the authority should be able to reveal the real identities of the message senders when needed[1].

1.3.2 Objectives

The objective of this research is to develop a set of efficient secure and privacy-preserving protocols to countermeasure and mitigate the aforementioned security and privacy threats. Further, the protocols should ensure that road authorities can reveal the real identities of the message senders in order to guard the truth when there is any dispute or need to track down the drivers.

The study also develops two vehicle applications, which are as follows:

- Develop a novel vehicle safety application, secure VANET-based road traffic control system, to help to circumvent vehicles safely and securely through an area of an abnormal situation.

[1]In this thesis, we term the co-existed privacy and identity traceability as conditional privacy.

- Develop a novel mobile payment system for highway toll collection through vehicular communications, which addresses all the issues in the currently existing toll collection technologies.

1.4 Research Contributions

This research focuses on developing a suite of interoperable approaches to tackle the most critical problems in the efforts of achieving security guarantee and privacy preservation for VANETs. In addition, this study also aims at developing value-added services in VANETs, vehicle applications. Specifically, the main contributions of this research lie in:

- A security infrastructure for VANETs is introduced, where the concept of **ePermit** is defined which serves as a proof of an authorized driver to drive the vehicle and to activate the security system based on proxy signature;

- An efficient approach in distributing the commitments of one-way key chains to vehicles by RSUs is proposed for achieving efficient V2V communications and ensuring effective message authentication. It solves the main barrier to the applicability of symmetric cryptography-based protocols in vehicular networks. Further, a complementary cooperative message validation protocol is introduced to deal with the situations where RSUs may not exist in VANETs.

- Two vehicle applications are developed to explore the advantages of vehicular communications. First, a secure VANET-based road traffic control system is proposed to help to circumvent vehicles safely and securely through an area of an abnormal situation, while ensuring the security and privacy of the users from various threats. It not only enhances traveler safety but also minimizes capacity restrictions due to any abnormal situation. Second, a novel mobile payment

system for highway toll collection through vehicular communication is proposed to address all the issues existed in the current traditional toll collection technologies.

1.5 Outline of the Thesis

The organization of the remainder of the thesis is as follows. Chapter 2 provides a survey on state-of-the-art research on security and privacy preservation in VANETs. Chapter 3 presents a Secure and Efficient RSU-aided Privacy-Preserving Protocol ($SERP^3$). Chapter 4 presents a complementary Efficient and Cooperative Message Validation Protocol ($ECMVP$) for some situations where RSUs may not exist in VANETs. Chapter 5 presents a novel vehicle safety application, secure VANET-based road traffic control system. In Chapter 6, a novel mobile payment system for highway toll collection is presented. Finally, conclusions and future research work are described in Chapter 7.

Chapter 2

Related Work

Securing V2V and V2I communications is mandatory in VANETs, and has drawn tremendous attention from both industry and academia. Over the past a few years, a number of initiatives have been launched. The Vehicle Safety Communications (VSC) project [4], which was initiated by US DOT in 2002, aims to evaluate the feasibility of supporting vehicle safety/non-safety-related applications through telecommunication technologies, such as the DSRC standard [3]. The VSC project investigates the security issues associated with VSC and identifies four major security goals for a VSC system: message integrity/origin authentication, correctness, privacy, and robustness under attack. In addition, the project discusses possible solutions for the aforementioned security goals. The VSC project proposes a dual authentication structure in which a list of short-lived anonymous certificates is taken to guarantee the privacy of OBUs and ensure the security, where the short-lived certificates are discarded once after being used. It is worth noting that a pseudonym is used in any anonymous certificate instead of the real identity of the vehicle, which protect the privacy of the vehicle. In addition, the classic hierarchical public key infrastructure (PKI) is presented for the purpose of ensuring the security of RSUs and public safety OBUs since RSUs and public safety OBUs do not have any issue of privacy. The scheme can provide a higher level of

privacy preservation and security assurance because the certificates are blindly signed by the Certificate Authority (CA) in order to deal with any possible insider attack. An insider attack could be simply launched by the CA which abuses its authority by mishandling the driver information. In order to achieve traceability, a linkage is devised for the escrow authorities to associate each blindly signed anonymous certificate with a single vehicle. All the compromised and expired vehicles have to be revoked by putting anonymous certificates belonging to those vehicles into the certificate revocation list (CRL). The disadvantage of this scheme is that the CRL may grow quickly such that it takes a long time to check through the whole CRL to see if a given certificate is valid or not. Another disadvantage lies in the fact that for achieving traceability, a unique electronic identity is assigned to each vehicle by which the identity of the vehicle owner can be inspected by the polices and authorities in case of any disputes. Although this scheme can effectively meet the conditional anonymity requirement, it is far from efficient and can hardly become a scalable and reliable approach because the ID management authority has to keep all the anonymous certificates for the vehicles in the administrative region. Once a malicious message is identified, the authority has to exhaustedly search in a very large database to find the identity related to the compromised anonymous certificate.

Similar activities are underway in Europe. The European Car-2-Car communication consortium [12], which is backed by General Motors, Audi, BMW, Fiat, Honda, Renault, etc, has been formed to work on V2V technologies to help to make driving safer and improve driving experience. A prerequisite for the successful deployment of vehicular communications is to ensure that the vehicular communication is secure and the driver privacy is protected. Secure Vehicular Communication (SeVeCom) project [13], which is part of the eSafety initiative [14], the Information Society and Media initiative [15], and the Sixth Framework Programme of the European Commission [16], is then funded in Europe to identify the variety of security and privacy threats facing

vehicular communications, define security requirements for vehicular communications, and investigate the cryptographic primitives which are suitable to the VC environment.

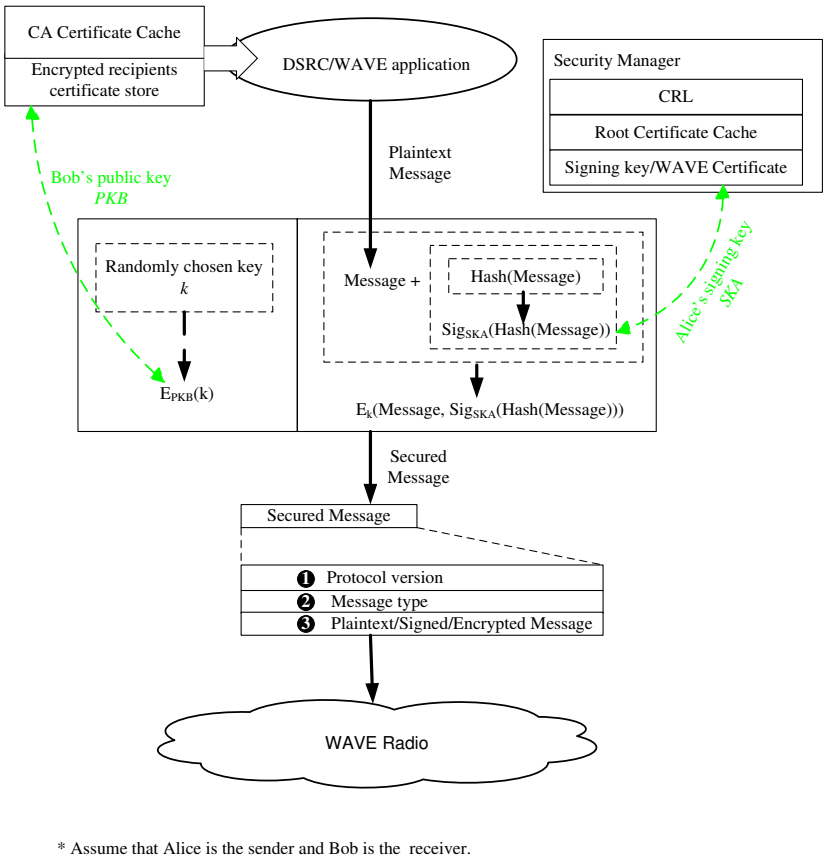


Figure 2.1: IEEE Std 1609.2 security services framework for creating and exchanging WAVE message between WAVE devices

Meanwhile, international standardizing bodies have addressed a lot of efforts in standardizing V2V communication technologies. The IEEE 1609 WAVE communication standards, which are also known as Dedicated Short Range Communications (DSRC) protocols, have emerged recently to enhance the 802.11 to support wireless communications among vehicles for the roadside infrastructure [5]. The IEEE 1609.2 standard addresses the issues of securing WAVE messages against eavesdropping, spoof-

ing, and other attacks. The components of the IEEE Std 1609.2 security infrastructure are shown in Fig. 2.1, and are based on industry standards for PKI, including the support for Elliptic curve cryptography (ECC) [17], WAVE certificate formats, and hybrid encryption methods, in order to provide secure services for WAVE communications. The security infrastructure is also responsible for the administrative functions, which are necessary to support the core security functions, such as certificate revocation. Note that due to some unexpected reasons, for example, a private key corresponding to a public key specified in the certificate is identified as compromised, certificate revocation is essential to any security system based on PKI, which has not been addressed in the current IEEE Std 1609.2 by considering the unique features of vehicular networks. In addition, IEEE 1609.2 standard does not define driver identification and privacy protection, and has left a lot of open issues.

In traditional PKI architecture, the most commonly adopted certificate revocation scheme is through CRL, which is a list of revoked certificates stored in central repositories prepared in CAs. Based on such centralized architecture, alternative solutions to CRL could be by way of a Certificate Revocation System (CRS), Certificate Revocation Tree (CRT), and Online Certificate Status Protocol (OCSP) [18], etc. The common requirement for these schemes is the high availability of the centralized CAs, where frequent data transmission with the OBUs for obtaining timely revocation information may cause significant overhead. Thus, with the high-speed mobility and extremely large amount of network entities in VANETs, the centralized CRL architecture may cause scalability problems. To tackle the problem, Raya et al. [19] proposed three certificate revocation protocols for VANETs, namely Revocation using Compressed Certificate Revocation Lists (RC2RL), Revocation of the Tamper-Proof Device (RTPD), and Distributed Revocation Protocol (DRP). RC2RL uses a compression technique to reduce the overhead of the distribution of the CRL. Instead of checking the status of a certificate, RTPD removes revoked certificates from their corresponding vehicles' certificate

stores by introducing a tamper-proof device as a vehicle key and certificate management tool. In this case, the vehicle possessing the revoked certificates is informed of the certification revocation incident, by which the tamper-proof device automatically removes those revoked certificates. Different from RC2RL and RTPD, a distributed certificate revocation mechanism is implemented in DRP to determine the status of a certificate. In DRP, each vehicle is equipped with an attacker detection system, which enables a vehicle to identify any compromised peer. When a compromised or malicious vehicle is detected and located, its neighbors can work together to temporally revoke the compromised one.

Securing VANETs has been subject to extensive research efforts in recent years, and has been well recognized as a prerequisite for the emerging applications such as vehicle safety-related services, and vehicle non-safety-related services [4]. To address the issues of security and conditional privacy in VANETs, three categories of solutions have been introduced. In the first category, each vehicle is securely equipped with a large number of short-life anonymous key pairs (probably 43,800 pairs), hereafter anonymous credentials [20]. Then, each vehicle randomly selects one of its anonymous credentials and uses the corresponding private key to sign the launched messages. The other vehicles authenticate the sender of the messages by using the public key of the sender. In addition, instead of taking any real identity information of the vehicles, these anonymous credentials are generated by taking the pseudo IDs of the vehicles in order to achieve privacy. Finally, the whole list of anonymous credentials correspond to a unique real identity, which should be kept by the authorities in order for the police to verify the real-world identities of the vehicles. In the second category, group signature and Identity-based signature techniques are adopted not only to guarantee the requirements of security and privacy, but also to provide desired traceability of each vehicle [21]. Finally, an efficient conditional privacy preservation (ECPP) protocol is introduced by the way of generating on-the-fly short-time anonymous key pairs between vehicles and

RSUs, which can provide fast anonymous authentication and privacy tracking while minimizing the required storage for short-time anonymous key pairs [22].

Unfortunately, the aforementioned solutions of updating pseudonyms are ineffective to protect location privacy and prevent tracking in VANETs. In other words, unlinkability cannot be guaranteed due to the fact that it is trivial to link an old pseudonym with a new pseudonym when vehicles constantly broadcast routine traffic information include their location and speed and driving directions, but without any type of mix. Even worse, if the adversary could link someone to the OBU's destinations, e.g., an office and a home, user anonymity cannot be achieved as well. To cope with this location privacy issue, Sampigethaya et al. proposed a location privacy scheme for VANETs called CARAVAN in which a vehicle remains silent for a randomly chosen short period of time after it enters a certain area of the network [23]. Freudiger et al. [24] introduced a solution by creating cryptographic mix-zones at some critical points on the roads, in which all traffic-related messages broadcast by the vehicles are encrypted and protected, and the vehicles also change their pseudonyms. Therefore, the sensitive information such as vehicle position information, which could lead to the violation of location privacy, is no longer visible to external attackers. Furthermore, a vehicular mix-network is built by combining all mix-zones to enhance location privacy in VANETs. Hence, the location privacy can be achieved.

The ultimate goal of building vehicular communication network is to develop various vehicle applications which could improve road safety and driving experience via vehicular communication. As applications built on VANETs, vehicle applications inherit all the known and unknown security weaknesses that are associated with VANETs, and could further be subject to many application-specific security and privacy threats. However, only few attention has been paid to security in vehicle applications. In [25], Rahman et al. proposed a secure architecture for VANET-based automated crash reporting application called Autocore after identifying several application-specific se-

curity and privacy threats. By introducing a concept of Road-worthiness certificate, a vehicle can be effectively authenticated and then obtain a list of anonymous credentials from regional authorities via RSUs. Afterwards, those anonymous credentials can be used to protect the broadcast messages and as well ensure the privacy of the OBUs since those anonymous credentials are blindly signed by the authorities. Furthermore, different from any previously reported studies, a decentralized architecture has been introduced to achieve the conditional privacy of the OBUs, which prevents a single point of failure.

Chapter 3

Secure and Efficient RSU-aided Privacy-Preserving Protocol

3.1 Introduction

In recent years, protocols have been developed to ensure secure and privacy-preserving communications over the vehicular communications network. In any of the previously reported protocols, a vehicle sender signs each message and broadcasts it, while each receiver verifies the received message using the corresponding public key. With asymmetric algorithms, the protocols will certainly induce heavy signature and authentication overhead, which make them not scalable when the traffic load is high, which, unfortunately, could be the situation commonly seen in metropolitan-area transportation. According to DSRC [3], a vehicle sends each message with a time interval from 100ms to 300ms. In the case that 50 to 120 cars are within the communication range of a vehicle, the vehicle needs to verify up to $1,200$ messages per second, which will obviously lead to a high computation burden and communication overhead. As shown in Table 3.1, none of traditional digital signature algorithms can achieve the desired verification speed and communication overhead.

Table 3.1: Verification speed and signature overhead of digital signature schemes

Digital signature scheme	RSA (2048 bits)	DSA (2048 bits)	ECDSA (224 bits)
Verification speed (verifications/s)	1370	62	258
Signature (bits)	2048	4096	448
Public key certificate* (bytes)	125	125	125

† We evaluate the verification speed and signature overhead of digital signature schemes on an Intel Pentium 4 3.0 GHz machine with 1GB RAM running Fedora Core 4 based on cryptographic library MIRACL (http://www.shamus.ie/).

* The size of a signing certificate for an OBU is 125 bytes [5].

To avoid the heavy signature and authentication overhead caused by asymmetric cryptography, significant efforts have been made in recent years in achieving efficient broadcast source authentication and data integrity by using fast symmetric cryptography [26–29], where TESLA [29] is among the most promising ones. However, due to the dynamic nature of VANETs, the use of a symmetric cryptography-based scheme may cause some other problems [5]. The main challenge lies in how to efficiently distribute commitments of one-way key chains to a highly dynamic group in VANETs in order for vehicles within the transmission range to freely authenticate each other. Motivated by the possibly advantages in taking symmetric cryptography, this chapter introduces a novel secure and efficient RSU-aided privacy-preserving protocol for VANETs. The major contributions of the chapter lies in the following two aspects: 1) a security infrastructure for VANET is introduced, where the concept of **ePermit** is defined which serves as a proof of an authorized driver to drive the vehicle and to activate the security system based on proxy signature; and 2) an efficient approach in distributing commitments of one-way key chains to vehicles by RSUs is proposed for achieving efficient IVCs and ensuring effective message authentication.

The remainder of the chapter is organized as follows. In Section 3.2, preliminaries are presented. In Section 3.3, a secure and efficient RSU-aided privacy-preserving protocol is introduced. Section 3.4 discusses the security and performance of the proposed protocol. Finally, we give the summary in Section 3.5.

3.2 Preliminaries

3.2.1 One-Way Key Chain

One-way hash chain was first proposed in [30] for secure password authentication, which quickly became an important cryptographic primitive in many other applications, such as micropayment systems [31], secure data forwarding in wireless ad hoc networks [32], and stream data authentication [33]. A one-way hash chain is repeated applications of a secure one-way hash function $H(x)$ to a randomly selected seed S, which has the following properties:

- $H(x)$ can take a message of arbitrary-length input and produce a message digest of a fixed-length output;
- Given x, it is easy to compute $y = H(x)$. However, it is hard to compute $x = H^{-1}(y)$ for a given y.
- Given x, it is computationally infeasible to find $x^{'} \neq x$ such that $H(x^{'}) = H(x)$;
- It is computationally infeasible to find any two pair x and $x^{'}$ such that $x^{'} \neq x$ and $H(x^{'}) = H(x)$.

The application of the hash function on S for $n-1$ times yields results denoted as $h_1, h_2, \cdots, h_n$, respectively, where $h_{i-1} = H(h_i)$, $h_n = S$, $1 < i \leq n$, and h_1 is called the *commitment* to the chain $h_1, h_2, \cdots, h_n$. Similarly, each chain element commits to all the subsequent elements in the chain shown in Fig. 3.1. Then, the holder of the

hash chain can release the chain elements one after another in an opposite order of that the chain to be generated. In this way, any hash chain element can be kept unrevealed before it is released, and upon receiving a chain element, its authenticity can be easily validated with a simple hash operation.

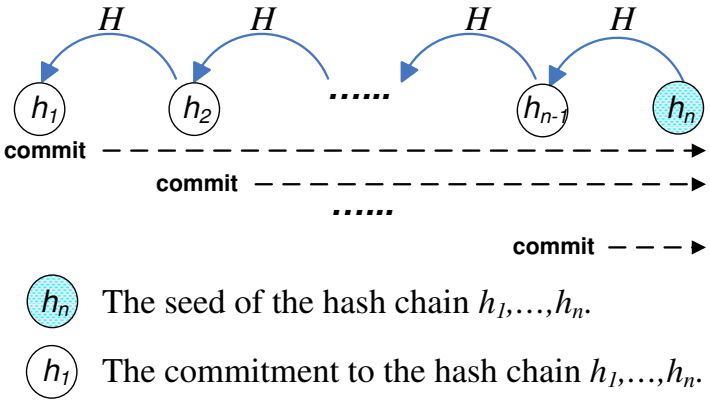


Figure 3.1: One-way hash chain

One-way hash chain can always be used to reduce the authentication load of a series of messages. For example, in TESLA, the chain elements are used as secret keys to compute message authentication codes (MACs) of the messages. Further, time is slotted and synchronized between senders and receivers, and each chain element corresponds to a specific time slot. By using the delayed secret key disclosure technique, the authenticity of a message can be guaranteed by verifying the MAC after the authenticity of the released key is checked against the relationship between it and any previously received genuine chain elements since any previously received chain element is a commitment to it. In this case, the chain is referred to as one-way key chain, denoted as $KC(n, h_1, h_n)$, where n is the length of the key chain, h_1 is the commitment to the chain, h_n is the seed of the chain.

3.2.2 Bilinear Pairing and ID-based Cryptography

Bilinear pairing can solve some previously well recognized unsolvable problems, such as *ID-based cryptography* (IBC) [34]. IBC is a public-key cryptosystem where any string can be used to derive a valid public key such as user names, email addresses, IP addresses, host or node names. Compared with conventional public key cryptosystems, IBC simplifies the certificate management since the public key of a user could be any of its publicly known identity. Another advantage is that they can save communication bandwidth compared with traditional schemes such as RSA [35] and ElGamal [36] because pairing-based schemes feature a relatively small signature overhead due to the usage of bilinear pairing in the design of signature schemes and/or security protocols.

As the preliminary of the proposed protocol, bilinear pairing is briefly reviewed as follows.

let $\mathbb{G}_1$ be a cyclic additive group and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q. We assume that the discrete logarithm problems in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard. A bilinear pairing is a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ which satisfies the following three properties:

- Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, where $P, Q \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q^*$.
- Non-degenerate: There exists $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.
- Computability: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

According to [34], the modified Weil or Tate pairing associated to supersingular elliptic curves can create such bilinear pairings.

Definition 1 (Bilinear Parameter Generator) *A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and outputs a*

5-tuple $(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P)$ *as the bilinear parameters, including a prime number* q *with* $|q| = k$*, two cyclic groups* $\mathbb{G}_1$*,* $\mathbb{G}_2$ *of the same order* q*, an admissible bilinear map* $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ *and a generator* P *of* $\mathbb{G}_1$*.*

3.2.3 Proxy Signature

The concept of proxy signature was first introduced in [37, 38]. As a variation of the standard digital signature, a proxy signature is very useful when a user (called original signer) tries to delegate her/his signing right to other user (called proxy signer). Once such a delegation is performed, the proxy signer can then sign on behalf of the original signer. Upon receiving a proxy signature, anyone can check its validity and will be convinced by the original signer's agreement on the signed message if the validation is positive. Recently, proxy signature schemes have been adopted in a number of applications, including electronic commerce and distributed shared objected systems [39, 40].

Based on the delegation type in different applications, they can be classified as *full delegation*, *partial delegation* and *delegation by warrant*. With a full delegation scheme, the original signer's private key is directly given to the proxy signer so that the proxy signer can have the same signing capability as the original signer, and the signatures generated by the original or the proxy signers are undistinguishable. Therefore, full delegation scheme is impractical and insecure in practice. In a partial delegation scheme, the original signer distributes a proxy secret key (different from the original signer's private key) to the proxy signer. Hence, the proxy signatures generated by the proxy secret key are different from the original signer's signatures. However, the messages that a proxy signer could sign are not limited, which could result in the risk of abuse of a delegated authority. With a delegation by warrant scheme, the weaknesses in the previous two schemes are removed by a warrant that specifies what kind of message to be delegated. The warrant is created by the original signer, which keeps the related

delegation information including the identity of the original signer and proxy signer, as well as the restrictions on the message that the proxy signer is allowed to sign [41–43].

3.3 Secure and Efficient RSU-aided Privacy-Preserving Protocol

The proposed secure and efficient RSU-aided privacy-preserving protocol called $SERP^3$ consists of the following five phases: system initialization phase, pseudo identity and private key generation phase, anonymous mutual authentication phase, one-way key chain commitment distribution phase between OBUs and RSUs, the OBU safety message signing and verification phase. For the sake of presentation, the notations in this chapter are listed in Table 3.2.

3.3.1 Threat Model

By taking the advantage that RSUs are not subject to any privacy issue, an elaborated solution based on ID-based signature was proposed to address the security issues existed in RSUs [21]. In this chapter, we will focus on the security and privacy issues related to each vehicle, which are described in Section 1.3.1.

3.3.2 System Model

Inspired by the fact that only the authorized drivers with all required documents, for example, insurance policy, can drive a car, the proposed protocol is embedded with eight entities in the system, including car manufacturer, car sellers, vehicle owners, the Ministry of Transportation (MTO), MTO's authorized safety inspection/emission test stations, insurance companies, vehicle owners' authorized drivers, and police road safety enforcement authority, as shown in Fig. 3.2.

Table 3.2: Notations

Notation	Descriptions
PK_{MTO}:	The public key of the MTO
SK_{MTO}:	The private key of the MTO
PK_{owner}:	The public key of the owner
SK_{owner}:	The private key of the owner
$\text{Cert}_{\text{owner}}$:	The certificate of the owner signed by the MTO
$\text{rid}_{\text{owner}}$:	The real identity of the vehicle owner
$PK_{\text{insurance}}$:	The public key of the insurance company
$SK_{\text{insurance}}$:	The private key of the insurance company
$\text{Cert}_{\text{insurance}}$:	The certificate of the insurance company signed by the MTO
PK_{safety}:	The public key of the safety inspection station
SK_{safety}:	The private key of the safety inspection station
PSK_{safety}:	The proxy signing key of the safety inspection station athorized by the MTO
$\text{Cert}_{\text{safety}}$:	The certificate of the safety inspection station signed by the MTO
$\text{Warrant}_{\text{safety}}$:	A proxy warrant containing delegation between the safety inspection station and the MTO, type of information authorized to sign, and expiration date.
s:	The private master key of the TA
P_{pub}:	The public key of the TA
rid:	The real identity of the vehicle
pid:	The pseudo identity of the vehicle
$\mathcal{M}_i$:	A message sent by the vehicle V_i
$h(.)$:	A one-way hash function such that SHA-1
$H_0(.)$:	A MapToPoint hash [58] function such as $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$\|\|$:	Message concatenation operation, which appends several messages together in a special format
$\lceil\ \rceil$:	The ceiling function

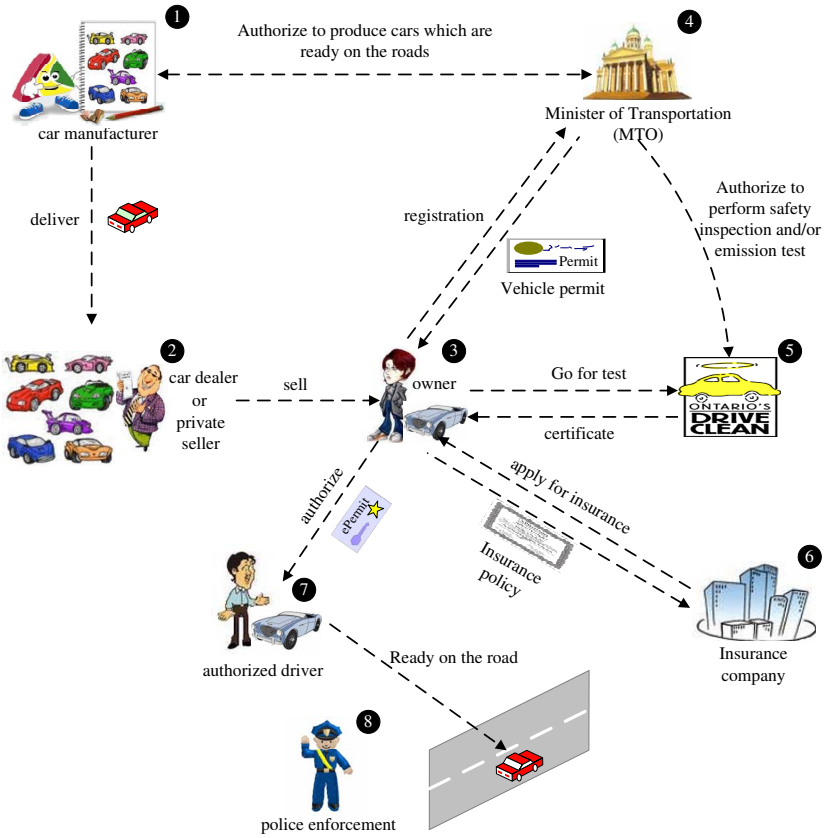


Figure 3.2: Procedure for vehicle's road readiness

First, all car manufacturers need to meet a series of different requirements set by the government who governs a region, and let their cars overcome stringent regulatory standards in order to sell the cars in that region. Afterwards, the public key and the related information of Ministry of Transportation, which serves as the representative of the government, will be preloaded to a *tamper-proof device* (TPD) of each vehicle by the car manufacturers. Then, the vehicle will be delivered to a car dealer, and be sold to a vehicle owner. To make the vehicles legitimate in the public usage, the vehicles have to pass some tests before registered with the MTO, such as emission test and safety inspection. Afterwards, the test station will issue a vehicle safety inspection

and/or emission test pass certificate to the vehicle owner. However, depending on regulations, those tests may be waived for brand new vehicles and vehicles with model years less than certain years old, e.g., 3 years. Therefore, the car manufacturers are the default authorized safety inspection and/or emission test station as well, and the brand new cars will be equipped with a vehicle safety inspection and/or emission test pass certificate. Here, an authorized safety inspection and/or emission test station serves as a delegate to sign certificates by using proxy signature on behalf of MTO.

Second, the vehicle owner needs to register the purchased vehicle with MTO by submitting all necessary information, such as Vehicle Identification Number (VIN), vehicle safety inspection certificate, and emission test pass certificate. It is worth noting that every vehicle has a unique VIN. MTO then loads the owner information into the TPD of the vehicle including the real identity of the owner. Also, the vehicle owner needs to apply for appropriate car insurance. For instance, if the owner wants to have a secondary driver for her/his car, the owner needs to buy insurance for herself/himself and as well the secondary driver. An evidence of insured is issued by the insurance company to the owner. Finally, the owner can authorize any allowed person to drive the car by issuing an **ePermit** to her/him, but the allowed driver should match the insured person listed in the insurance policy.

Third, the vehicle owner and other authorized drivers if applicable can drive the car on the road by using holding **ePermit** to authenticate with the TPD and activate it if passed, which will be detailed later. An **ePermit** has the following structure shown in Figure 3.3. Finally, the police can enforce the road readiness of vehicles by checking whether a vehicle on the road broadcasts authentic routine traffic-related message.

The considered road system architecture is mainly composed of the immobile RSUs at the roadside and the mobile OBUs equipped on the moving vehicles, as shown in Fig. 3.4. The RSUs and OBUs are dynamically interconnected with each other to form a VAENT, and those RSUs are further connected to the Internet backbone via some

ePermit			
Part I. Ownership proof	VIN	$\text{rid}_{\text{owner}}$	$\text{ExpirationDate}_{\text{owner}}$
	$\text{Sign}_{\text{SK}_{\text{MTO}}}(\text{VIN}, \text{rid}_{\text{owner}}, \text{ExpirationDate}_{\text{owner}})$		
Part II. An evidence of insured	VIN	Listofinsureddrivers	$\text{ExpirationDate}_{\text{insurance}}$
	$\text{Sign}_{\text{SK}_{\text{insurance}}}(\text{VIN}, \text{Listofinsureddrivers}, \text{ExpirationDate}_{\text{insurance}})$		
	$\text{Cert}_{\text{insurance}}$		
Part III. Safety inspection	VIN	Pass/Fail	$\text{ExpirationDate}_{\text{safety}}$
	$\text{PSign}_{(\text{PSK}_{\text{safety}}+\text{SK}_{\text{safety}})}(\text{VIN}, \text{Pass/Fail}, \text{ExpirationDate}_{\text{safety}})$		
	$\text{Cert}_{\text{safety}}$		
	$\text{Warrant}_{\text{safety}}$		
Part IV. Authorization	VIN	Authorized driver ID rid	$\text{ExpirationDate}_{\text{permit}}$
	$\text{Sign}_{\text{SK}_{\text{owner}}}(\text{VIN}, \text{Authorized driver ID rid}, \text{ExpirationDate}_{\text{permit}})$		
	$\text{Cert}_{\text{owner}}$		

Figure 3.3: The structure of **ePermit**

high-speed links. In this chapter, we assume that each road intersection is equipped with one RSU so that the road system can be viewed as a network interconnected by RSUs. In addition, an RSU is subject to no power constraint and there is no energy limit for vehicles. The vehicle's communication device is actively powered for any computation and communication task. As shown in Fig. 3.5, the vehicles are equipped with various sensors, e.g., reliable positioning system like GPS, and all the vehicles are loosely synchronized, e.g., equipped with a highly accurate atomic clock or through a central satellite. The output of those sensors become input for some vehicle applications, e.g., rear end collision warning, which analyze these data and format findings accordingly [44].

Furthermore, each vehicle is equipped with a *tamper-proof device* (TPD) to store cryptographic key, data, and code, which is secure against any compromise attempt in the way that an attacker cannot extract any data stored in the device. The TPD is composed of four modules: an authentication module which enables user authentication by way of the OBU, a pseudo identity generation module which generates random

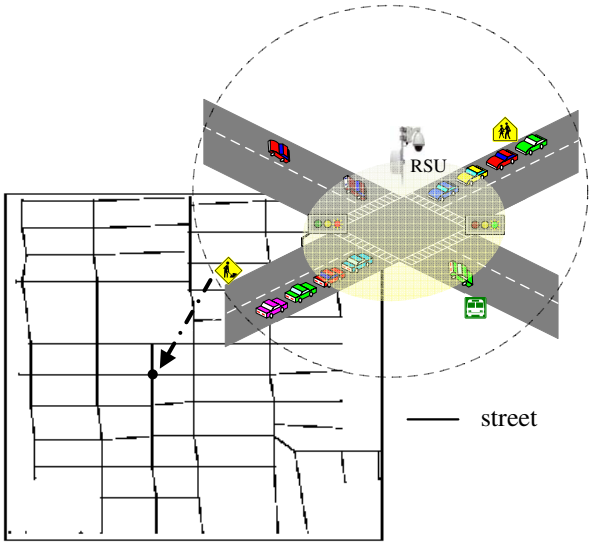


Figure 3.4: Road system architecture

pseudo identity, a private key generation module which calculates the corresponding private key of a pseudo identity, and an event recorder which records any data launched from and received by the vehicle as shown in Fig. 3.5. The four modules will be further discussed in the next section.

The driver needs to authenticate his credentials, i.e., **ePermit**, with his TPD. The TPD needs to validate the permit by checking through ownership proof, the evidence of insured, safety inspection status, and legitimation of the driver. After successful authentication, the TPD is enabled to periodically generate short-time anonymous key pairs, which have two usages. Firstly, those anonymous key pairs can be used to request a limited-time one-way key chain from an RSU, and the chain element is the secret key to compute a MAC of data from various installed vehicle applications, which is similar to TESLA [29]. Secondly, those short-time anonymous key pairs can also be used to cryptographically process data directly when the vehicles are in rural and suburban areas without RSUs. Afterwards, the result will be broadcast to the vehicle's neighboring vehicles.

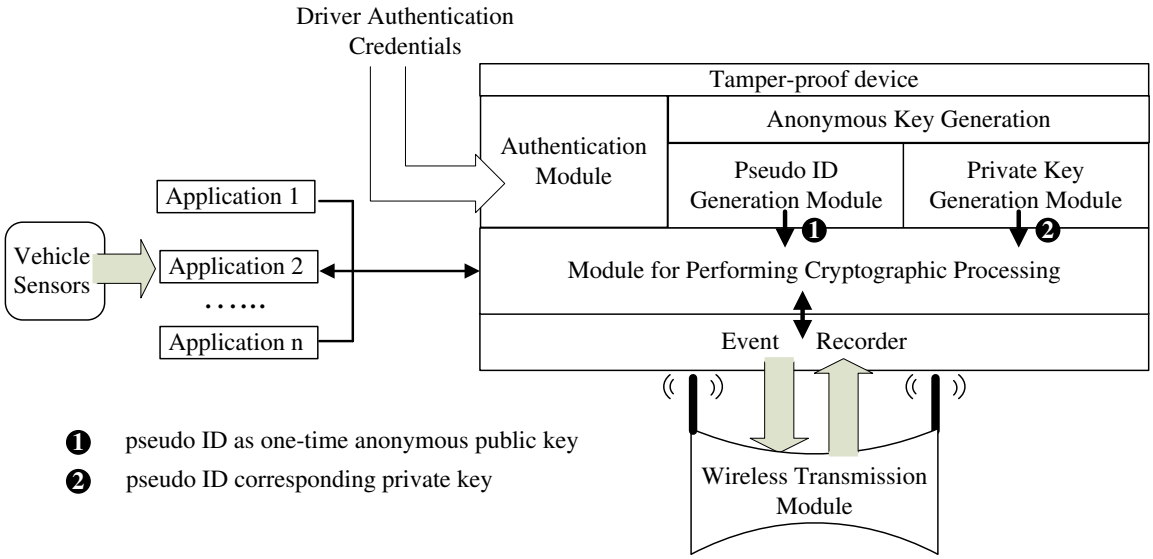


Figure 3.5: OBU architecture

Furthermore, in order to ensure both security and privacy in vehicular communication networks, we need to consider various attacks that might be mounted. In this study, we consider the highest security scenario where there exists a passive global attacker who is able to eavesdrop on any message transmitted over the VANETs.

3.3.3 System Initialization Phase

Suppose that there exists an offline *trust authority* (TA) which is in charge of checking the vehicle's identity and pre-distributing the private master key of the TA. Prior to the network deployment, the TA sets up the system parameters for each RSU and OBU as follows.

- Given the security parameter k, a 5-tuple bilinear parameter $(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P)$ is generated by running the bilinear parameter generator $\mathcal{G}en(k)$.
- The TA randomly chooses two secure primes p_0, q_0 such that $p_0 \equiv q_0 \equiv 3 \bmod 4$ and $s \in \mathbb{Z}_q^*$ as its *master key*, and computes $n_0 = p_0 \cdot q_0$ and $P_{pub} = sP \in \mathbb{G}_1$ as the

corresponding public keys. Let $H_0(.)$ be a MapToPoint hash [58] function such as $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_1$. Then, the public parameters are $(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_0, n_0)$.

- The tamper-proof device of each vehicle and each RSU is preloaded with the public parameters $(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub}, H_0, n_0)$ and the *master key* (s, p_0, q_0) of the TA. Each RSU has an ID id_r, which may include the name of the RSU, the authorized geographical region to operate, and the authorized message type. The TA computes $SR_{RSU} = sH_0(id_r)$ as the RSU's private key. Then this private key of the RSU is stored in the RSU's tamper-proof device as well.

- To activate the tamper-proof device, the driver has to present a valid **ePermit**. Hence, an attacker cannot take advantages of the tamper-proof device even if the vehicle is stolen.

Each vehicle maintains a key chain commitment table for facilitating the packet source authentication, whose format of each entry is shown as follows.

Source	Index	c	$Lifetime$

where the first field records a packet source's pseudo ID; the second field records the index of the time interval when the last key chain element is received successfully; the third field records the last successfully received key chain element; and the last field $Lifetime$ serves as a timer controlling how long the entry is active. If the timer hits 0, the entry is expired and removed from the vehicle's cache table.

3.3.4 Pseudo Identity and Private Key Generation Phase

The driver first needs to use her/his possessing **ePermit** to activate the TPD, where the authentication module of the TPD works as an access control mechanism. If the **ePermit** successfully passes the verification of the authentication module, the driver's real ID *rid* is delivered to the pseudo identity generation module. Otherwise, the

TPD denies providing services for the vehicle. Obviously, the authentication module enhances the security of the TPD since a malicious attacker cannot take advantage of it even though the TPD is physically held by the attacker if the attacker does not have any valid authentication credential.

The pseudo identity generation module periodically generates random pseudo identities from the authenticated *rid*, which serves as public keys of the OBU, and as well pass those keys to the private key generation module, which generates the corresponding private key by using Identity-based cryptography [34], which is shown in Algorthm 1.

Finally, a vehicle can obtain a list of pseudo identities pid_i along with the corresponding private keys sk_i, where $i = 1, 2, 3, ...$

3.3.5 Anonymous Mutual Authentication Phase

In this phase, a vehicle authenticates itself to an RSU and the RSU authenticates itself to the vehicle in such a way that both parties are assured of the others' legitimacy but the vehicle stays anonymous whenever the vehicle is within the transmission range of the RSU. Then, the RSU distributes one or more one-way key chains to the vehicle. The vehicle can take the one-way key chains to obtain the MACs that will be attached to the safety messages. In addition, a set of commitments of one-way key chains are sent to the vehicle, which will help the vehicle to perform source authentication and ensure data integrity of the received safety messages after the vehicle leaves the current RSU and before it reaches the next RSU.

Let the RSU r advertise its presence by periodically broadcasting beacons containing the RSU's ID id_r. As soon as a vehicle newly enters the transmission range of the RSU, the vehicle initiates anonymous mutual authentication and executes a one-way key chain commitment distribution protocol with the RSU as illustrated in Fig. 3.6:

Step 1. An OBU with pseudo-id *pid* first gets the RSU's identity information id_r from the RSU's beacon, computes $h_o = H_0(pid)$, $h_r = H_0(id_r)$, and uses its private key

Algorithm 1: Anonymous key pairs generation algorithm

Data: Real identity rid

Result: Pseudo-id pid and the private key sk

begin

The TPD first runs the following steps:

▷ choose a random number r with the same length as rid, that is $|r| = |rid|$ and set pid as

$$\begin{cases} pid_p \equiv r \oplus rid \bmod p_0 \\ pid_q \equiv r \bmod q_0 \end{cases} \tag{3.1}$$

▷ based on the Chinese Remainder Theorem, compute the pseudo-id pid as

$$pid \equiv pid_p \cdot c_p + pid_q \cdot c_q \bmod n_0 \tag{3.2}$$

where $c_p = q_0 \cdot (q_0^{-1} \bmod p_0)$ and $c_q = p_0 \cdot (p_0^{-1} \bmod q_0)$.

▷ compute the hash value $H_0(pid)$ and the private key

$$sk = sH_0(pid) \in \mathbb{G}_1 \tag{3.3}$$

The TPD returns (pid, sk) to the module for performing cryptographic processing.

end

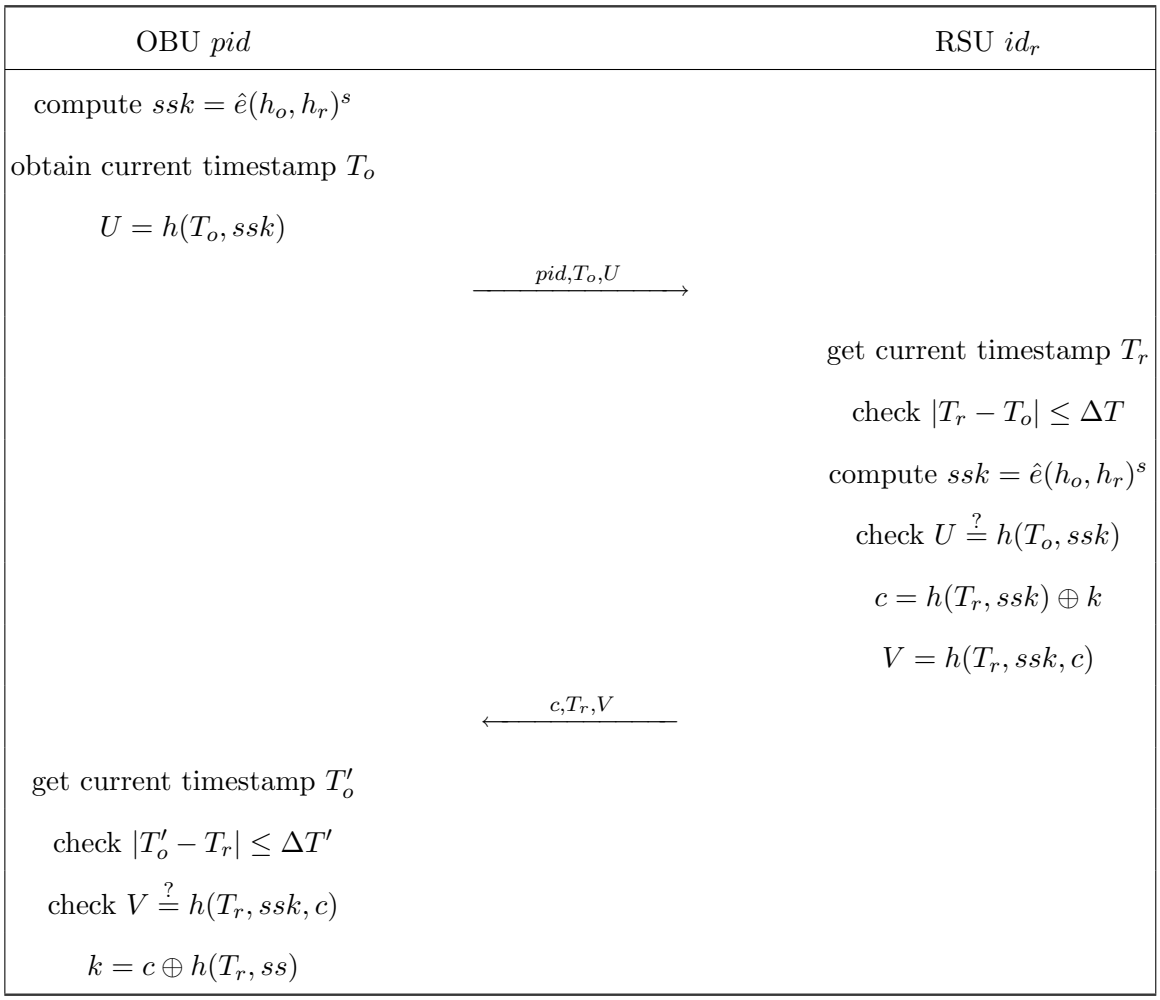


Figure 3.6: Anonymous mutual authentication between OBU and RSU

$sk = sH_0(pid) = s \cdot h_o$ to compute their static shared key ssk,

$$ssk = \hat{e}(sk, h_r) = \hat{e}(s \cdot h_o, h_r) = \hat{e}(h_o, h_r)^s \tag{3.4}$$

Then, the OBU gets the current timestamp T_o, computes

$$U = h(T_o, ssk) \tag{3.5}$$

and sends (pid, T_o, U) to the RSU.

Step 2. After receiving the OBU's request (pid, T_o, U), the RSU first gains the current timestamp T_r, and checks whether $|T_r - T_o| \leq \Delta T$, where ΔT is the expected legal time interval for transmission delay. If it does not hold, the RSU will reject the OBU's request. Else, the RSU will continue running the following procedures:

- Compute $h_o = H_0(pid)$, $h_r = H_0(id_r)$, and use private key $sk = sH_0(id_r)$ to derive the static shared key ssk as

$$ssk = \hat{e}(h_o, sk) = \hat{e}(h_o, s \cdot h_r) = \hat{e}(h_o, h_r)^s \tag{3.6}$$

- Check whether or not

$$U = h(T_o, ssk) \tag{3.7}$$

  If it holds, the OBU with pseudo-id pid is anonymously authenticated; otherwise rejected.

- Randomly choose a session key k. To distribute the session key k to the OBU, c and V are computed as follows:

$$c = h(T_r, ssk) \oplus k \tag{3.8}$$

$$V = h(T_r, ssk, c) \tag{3.9}$$

- Send (c, T_r, V) back to the OBU.

Step 3. On receiving the RSU's response (c, T_r, V), the OBU first gains the current timestamp T_o', and checks whether $|T_o' - T_r| \leq \Delta T'$, where $\Delta T'$ is another expected legal time interval for transmission delay. The OBU then performs the following procedures to obtain the session key k:

- Compute

$$V^{'} = h(T_r, ssk, c) \tag{3.10}$$

  Check whether or not

$$V = V^{'} \tag{3.11}$$

  If it does hold, the RSU with identity id_r is authenticated;

- Compute

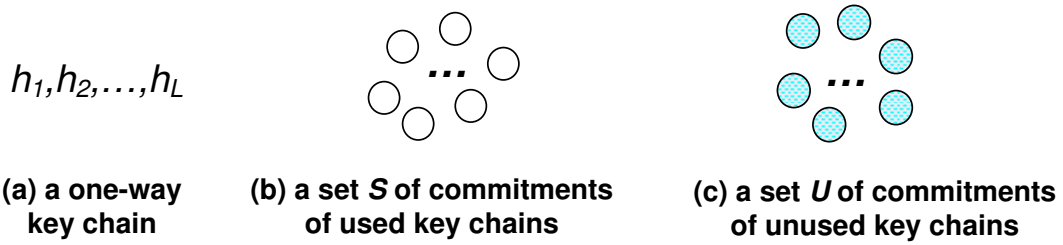
$$k = h(T_r, ssk) \oplus c \tag{3.12}$$

In the end, when the above three steps are executed normally, the anonymous mutual authentication between the RSU and the OBU completes, and the OBU also obtains the session key k from the RSU.

Inspired by the fact that a majority of vehicles run in a certain area everyday and communicate with the same RSUs, the aforementioned authentication process can further be speed up by pre-computing ssk at OBUs.

3.3.6 One-way Key Chain Commitment Distribution Phase Between OBUs and RSUs

In this phase, the RSU will securely distribute the three parts of information to the newly authenticated entering vehicle by using its sharing secret key k with the entering vehicle, which is shown as follows.



Stands for a commitment of a key chain that has been assigned to a vehicle passing through the intersection

Stands for a commitment of a key chain that will be assigned to a vehicle entering the intersection later.

Figure 3.7: One-way key chain commitment distribution between OBU and RSU

1. The first part is a one-way key chain with a specific length L shown in Fig. 3.7 (a). The vehicle, after obtaining the whole key chain, will broadcast safety messages by attaching each of them with a short MAC tag according the one-way key chain;

2. The second part is a set $\mathcal{S}$ of the commitments of one-way key chains that have been assigned to the passing vehicles. With such a mechanism, any newly entered vehicle will be able to authenticate the safety messages from the other vehicles previously passing through the intersection within a time window. Those vehicles can authenticate each other on the way to an adjacent RSU since they have the commitments corresponding to the key chains assigned to those vehicles;

3. The last part is a set $\mathcal{U}$ of the commitments of one-way key chains that will be assigned to the vehicles entering the intersection later. In this case, any newly entered vehicle will be able to authenticate the safety messages from the vehicles entering the intersection later and coming to pass it since it holds the commitments corresponding to the key chains assigned to those vehicles in advance. Also, it ensures that any newly entered vehicle will be authenticatable by all the vehi-

cles that passed through the intersection before and still are on the way to the next adjacent intersection since they hold the commitment corresponding to the key chain assigned to the newly entered vehicle in advance.

It is worth noting that every key chain commitment is associated with a unique pseudo ID, which is sent to the entering vehicle by the RSU as well.

The size Y of the set $\mathcal{U}$ of the commitments of one-way key chains will be discussed later. A key chain maintained in the RSU will become expired and erased after it is used up by its assigned vehicle, and in this case, new key chains will be generated to replace the old and expired ones, which can be assigned to an entering vehicle later.

$$\underset{\Downarrow}{\mathcal{P}_1[L,K]}
\begin{bmatrix}
T_1 & h_1^1 & h_1^2 & \cdots & h_1^{K-1} & h_1^K \\
\cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\
T_N & h_N^1 & h_N^2 & \cdots & h_N^{K-1} & h_N^K \\
 & \cdot & \cdot & \cdots & \cdot & \cdot \\
 & \cdot & \cdot & \cdots & \cdot & \cdot \\
 & \cdot & \cdot & \cdots & \cdot & \cdot \\
 & h_L^1 & h_L^2 & \cdots & h_L^{K-1} & h_L^K
\end{bmatrix}
\qquad
\underset{\Downarrow}{\mathcal{P}_2[L,K]}
\begin{bmatrix}
T_{N+1} & h_1^{K+1} & h_1^{K+2} & \cdots & h_1^{2K-1} & h_1^{2K} \\
\cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\
T_{2N} & h_N^{K+1} & h_N^{K+2} & \cdots & h_N^{2K-1} & h_N^{2K} \\
 & \cdot & \cdot & \cdots & \cdot & \cdot \\
 & \cdot & \cdot & \cdots & \cdot & \cdot \\
 & \cdot & \cdot & \cdots & \cdot & \cdot \\
 & h_L^{K+1} & h_L^{K+2} & \cdots & h_L^{2K-1} & h_L^{2K}
\end{bmatrix}
\cdots\cdots$$

Figure 3.8: One-way key chain pool

Note that in order to defend replay attack, the proposed protocol loosely synchronizes each vehicle by having time slotted with a fixed interval denoted as Δt. Thus, during a specific time slot, a vehicle has to create a MAC using a correct key chain

element for launching the safety messages, such that the safety messages can be successfully authenticated by the other vehicles.

With the proposed IVC authentication mechanism, the value of Y determines the maximum number of vehicles that can communicate with a vehicle passing through the intersection before the vehicle reaches another adjacent intersection[1]; while the value L determines how long a vehicle can use the assigned key chain to launch tagged messages. Note that once a vehicle cannot reach the next RSU and be newly assigned a key chain before running out of the whole key chain, it has to switch back to the conventional PKI-based authentication, which is subject to more communication and computation overhead.

Let t_i denote the starting time of the i_{th} time slot, and T_i denote the i_{th} time slot $[t_i, t_{i+1})$. The OBU key chain assignment procedure is detailed as follows.

Each RSU has a pool of one-way key chains divided into a number of sub-pools $\mathcal{P}_i[L, K]$ with L rows and K columns, where $i = 1, 2, 3, \cdots$, which is shown in Fig. 3.8, where $h_1^j = h(h_2^j)$, $h_{i-1}^j = h(h_i^j)$, $h_L^j = S^j$, $j \geq 1$, h_1^j is called the *commitment* to the chain, and $h_L^j = S^j$ is the randomly selected seed of the chain, L is the length of the chain. Each sub-pool is responsible for N time intervals. Further, the RSU will generate a pseudo ID $PVID_j$ for each chain $KC(L, h_1^j, S^j)$ by using Algorithm 1 with its identity id_r. How to determine the parameters L, K and Y will be discussed in Section 3.3.8.

In the following descriptions, any vehicle which finishes association and anonymous mutual authentication with the RSU in T_i is considered entering the RSU in T_i. Let vehicle V_1 enter the RSU in T_1. For simple exemplification, we take $L = 7$, $K = 8$,

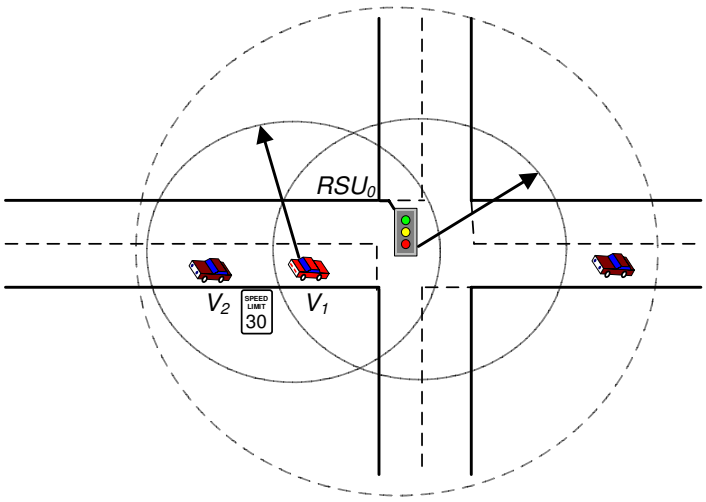
[1]For simplicity, we assume that all the vehicles, which enter the intersection after a vehicle, communicate with the vehicle before the vehicle enters another adjacent intersection.

$N = 3$ and $Y = 4$ in the following descriptions.

$$\begin{bmatrix} h_1^1 & h_1^2 & \cdots & h_1^5 \\ \vdots & & & \\ \vdots & & & \\ \vdots & & & \\ h_7^1 & & & \end{bmatrix},$$

i.e., $KC(7, h_1^1, h_7^1)$, $\mathcal{U} = \{h_1^1\}$ and $\mathcal{S} = \{h_1^2, \cdots, h_1^5\}$, as well as their corresponding pseudo IDs $PVID_i$, $1 \leq i \leq 5$, are sent to vehicle V_1, where the size of $\mathcal{S}$ is $Y = 4$. It is worth noting that the size of $\mathcal{S}$ is always kept unchanged. Without loss of generality, we take $\mathcal{M}$ to denote all the information which will be sent to V_1 by the RSU, which is detailed in the next paragraph. The information exchange between the RSU and V_1 is demonstrated as follows.

The RSU prepares $\mathcal{M} = \{E_k(KC(7, h_1^1, h_7^1)), \mathcal{U}, \mathcal{S}, PVID_1, \cdots, PVID_5\}$, where $E_k(m)$ means the encryption of message m by using any implicit secure symmetric encryption algorithm, i.e., DES [45], under the key of k, and generates a *message authentication code* (MAC) on $\mathcal{M}||T$ as $MAC_k(\mathcal{M}||T)$, where T is the time when the RSU broadcasts the information, which is used to defeat replay attack, and k is the shared secret key between the RSU and V_1. Also, the RSU uses its private key to sign $\mathcal{M}$ as $\sigma = Sign_{SK_{RSU}}(\mathcal{M}||T)$ by any ID-based signature scheme where SK_{RSU} is the corresponding private key of id_r. With the ID-based signature scheme, the workload of certificate management can be significantly reduced, and the public key update and revocation operations can be largely simplified. Among all the known ID-based signature schemes, the provably-secure ID-based signature scheme given in [46] is adopted in the study since the length of the signature is significantly reduced due to the use of bilinear pairing. The scheme is also among the most efficient ones in terms of the complexity of signature verification, which takes only 1 pairing computation. Afterwards, the RSU broadcasts $\mathcal{P} = \langle \mathcal{M}, T, MAC_k(\mathcal{M}||T), \sigma, id_r \rangle$.



* Solid circle stands for normal transmission range, and dotted circle stands for extended transmission range.

Figure 3.9: Extended intersection

Upon receiving $\mathcal{P}$, V_1 uses its shared secret key k to verify $MAC_k(\mathcal{M}||T)$ from the RSU[2]. It drops $\mathcal{P}$ if the authentication fails. Otherwise, it continues as follows. V_1 decrypts $E_k(KC(7, h_1^1, h_7^1))$ for the assigned key chain. Afterwards, V_1 stores the received commitments in its local key commitment table along with the corresponding pseudo IDs $PVID_i$. Then, V_1 can use assigned key chain $KC(7, h_1^1, h_7^1)$ to secure its launched messages, which will be described in the next subsection. It is worth noting that a vehicle, e.g., V_2 in Fig. 3.9, is within the transmission range of V_1, but it cannot authenticate the messages from V_1 since V_2 has not reached the RSU to obtain the commitment of V_1's key chain. To further solve this problem, we have the RSU to broadcast $\mathcal{P}$ with a higher radiation power in order to cover at least twice of the transmission range of a vehicle; then, as shown in Fig. 3.9, V_2 can receive $\mathcal{P}$ and authenticate any message from V_1[3].

Subsequently, the similar procedure occurs to the vehicles entering the intersection later except receiving a different key chain, $\mathcal{S}, \mathcal{U}$ and their corresponding pseudo IDs. Suppose V_2 enters in the RSU in T_2, RSU will construct a key chain $KC(6, h_2^2, h_7^2)$ shown as follows.

$$\begin{bmatrix} h_2^1 & h_2^2 & h_2^3 & \cdots & h_2^6 \\ & \vdots & & & \\ & \vdots & & & \\ & \vdots & & & \\ & h_7^2 & & & \end{bmatrix}$$

In this case, $\mathcal{P}$ contains $KC(6, h_2^2, h_7^2)$, $\mathcal{U} = \{h_2^1, h_2^2\}$, $\mathcal{S} = \{h_2^3, \cdots, h_2^6\}$ along with their corresponding pseudo IDs $PVID_i$, $1 \leq i \leq 6$, which will be sent to V_2.

[2]Whenever receiving any packet, the receiver first checks if the timestamp found in packet is reasonable, and if so, continue. Otherwise, the receiver drops the packet since the receiver could be subject to replay attack.

[3]V_2 ensures the authenticity of $\mathcal{P}$ by verifying RSU's signature σ.

In the case that multiple vehicles, e.g., V_3 and V_4, enter the RSU within a single time slot T_3, the RSU will create a key chain $KC(5, h_3^3, h_7^3)$ shown as follows.

$$\begin{bmatrix} h_3^1 & h_3^2 & h_3^3 & h_3^4 & \cdots & h_3^7 \\ & & \vdots & & & \\ & & \vdots & & & \\ & & \vdots & & & \\ & & h_7^3 & & & \end{bmatrix}$$

In this case, $\mathcal{P}$ contains $KC(5, h_3^3, h_7^3)$, $\mathcal{U} = \{h_3^1, h_3^2, h_3^3\}$ and $\mathcal{S} = \{h_3^4, \cdots, h_3^7\}$ along with their corresponding pseudo IDs $PVID_i$, $1 \leq i \leq 7$, which will be sent to V_3.

On the other hand, the RSU will create a key chain $KC(5, h_3^4, h_7^4)$ shown as follows, where $\mathcal{P}$ contains $KC(5, h_3^4, h_7^4)$, $\mathcal{U} = \{h_3^1, h_3^2, h_3^3, h_3^4\}$ and $\mathcal{S} = \{h_3^5, \cdots, h_3^8\}$ along with their corresponding pseudo IDs $PVID_i$, $1 \leq i \leq 8$, which will be sent to V_4.

$$\begin{bmatrix} h_3^1 & h_3^2 & h_3^3 & h_3^4 & h_3^5 & \cdots & h_3^8 \\ & & & \vdots & & & \\ & & & \vdots & & & \\ & & & \vdots & & & \\ & & & h_7^4 & & & \end{bmatrix}$$

Next, we suppose that V_5 enters the RSU at T_4. The RSU will create a key chain $KC(7, h_1^9, h_7^9)$ from the second sub-pool $\mathcal{P}_2[7, 8]$ shown as follows, where $\mathcal{P}$ contains $KC(7, h_1^9, h_7^9)$, $\mathcal{U} = \{h_4^1, h_4^2, h_4^3, h_4^4, h_1^9\}$ and $\mathcal{S} = \{h_1^{10}, \cdots, h_1^{13}\}$ along with their corresponding pseudo IDs $PVID_i$, $1 \leq i \leq 4$ and $9 \leq i \leq 13$, which will be sent to V_5.

$$\begin{bmatrix} h_4^1 & h_4^2 & h_4^3 & h_4^4 \end{bmatrix} \quad \begin{bmatrix} h_1^9 & h_1^{10} & h_1^{11} & h_1^{12} & h_1^{13} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ h_7^9 & & & & \end{bmatrix}$$

It is worth noting that in order to enable IVC between the vehicles arriving at T_1, T_2, T_3 and the ones at T_4, T_5, T_6, the following condition must be satisfied:

$$\begin{cases} h_4^i = h_1^{i+4}, i = 5, 6, 7, 8 \\ PVID_i = PVID_{i+4}, i = 5, 6, 7, 8 \end{cases} \tag{3.13}$$

This condition can be easily achieved by generating a longer key chain for each vehicle at the expense of more storage and higher computation required in RSUs.

3.3.7 Message Signing and Verification

Suppose vehicle V_1 periodically broadcasts routine traffic related safety messages denoted as $M_1, M_2, ..., M_k$, and M_i is encapsulated in packet P_i, $1 \leq i \leq k$. Further, let packets be launched one after another with a fixed interval of 300 ms. The packet authentication process is shown in Fig. 3.10:

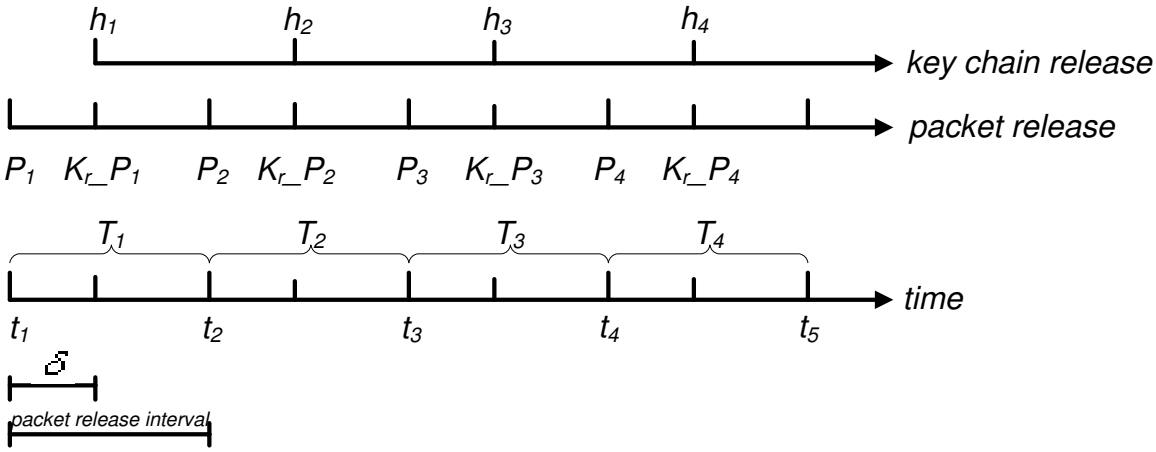


Figure 3.10: Relationship between a key chain and the corresponding packets

In this chapter, two categories of packets, namely data packets and key release

packet (KRP), are defined, and are denoted as P_i and kr_P_i, respectively. A vehicle periodically launches a KRP by a fixed time δ after the previous data packet is released.

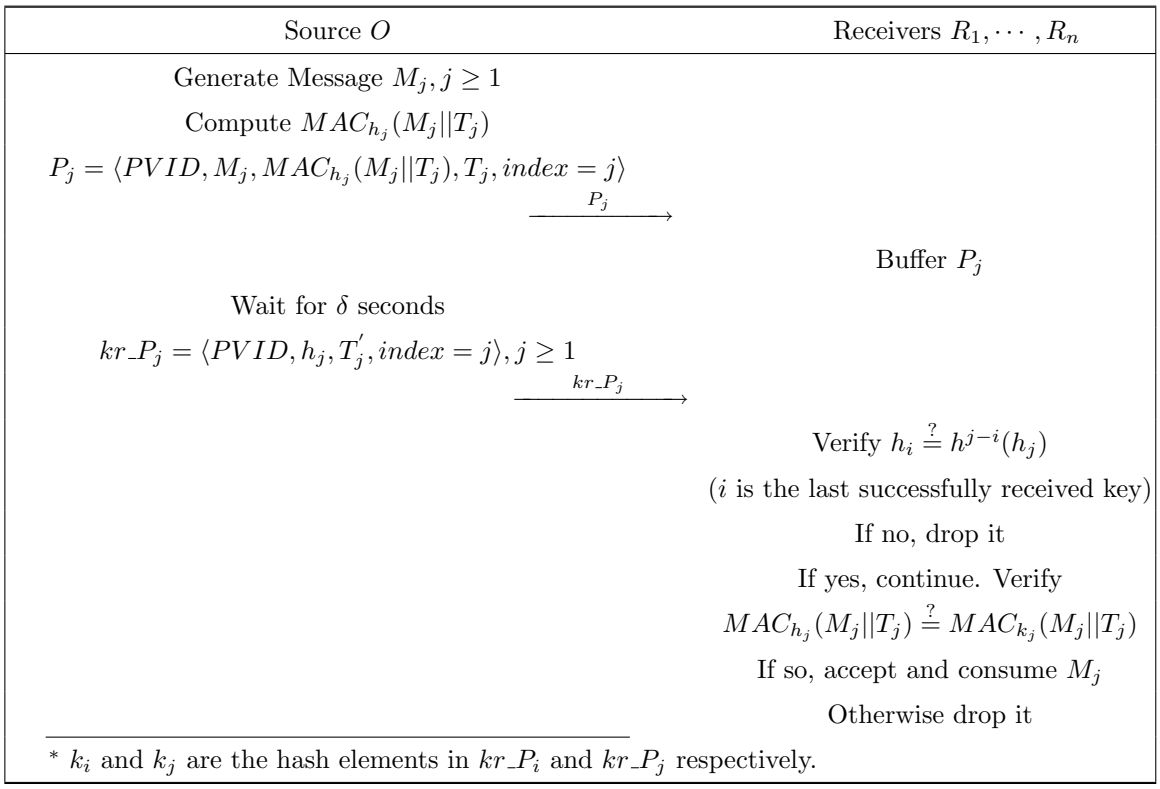


Figure 3.11: The proposed security protocol

The proposed security scheme is illustrated in Fig. 3.11. For an arbitrary sender O, it generates the MAC tags of the messages using h_j as the encryption keys, where $1 \leq j \leq n$. Therefore, the data packet to be sent has the following format:

$$P_j = \langle PVID, M_j, MAC_{h_j}(M_j||T_j), T_j, index = j \rangle, \ j \geq 1 \tag{3.14}$$

where M_j is the safety message, $PVID$ is the pseudo ID of vehicle O; T_j is the time when the sender sends the data packet, which is used to defeat replay attack.

Then, the sender O prepares the key release packet, which has the following format:

$$kr\_P_j = \langle PVID, h_j, T_j^{'}, index = j \rangle, \ j \geq 1, \tag{3.15}$$

where h_j is used to generate the MAC tag for message M_j, $T_j^{'} = T_j$.

Delayed authentication is performed in the sense that when receiving data packet P_j, $j \geq 1$, the receivers simply put the received messages in the buffer without trying to verify them. As soon as the next key release packet kr_P_j arrives, the receivers start to verify the previous data packet. At first, the receivers check the legitimacy of the received key chain element, which can be done by checking if the following equation holds:

$$h^{j-index}(h_j) = c \tag{3.16}$$

where h_j is included in the key release packet kr_P_j, and c and $index$ are from the entry corresponding to $PVID$, which is found in its local key commitment table. If the Eq. 3.16 does not hold, the packet kr_P_j is dropped along with data packet P_j; otherwise, the receivers start to validate the data packet P_j by checking if

$$MAC_{k_j}(M_j||T_j) = MAC_{h_j}(M_j||T_j), \tag{3.17}$$

where M_j, T_j and $MAC_{h_j}(M_j||T_j)$ are the previously buffered values of the data packet P_j, k_j is the key chain element in kr_P_j. If the verification succeeds, P_j is accepted and consumed by the application layer, and then, in the entry corresponding to $PVID$, the receivers update the second and third fields with $index$ and h_j along with a new timer for the last field; otherwise, P_j is dropped.

In summary, the proposed protocol can achieve the same guarantee on the message integrity, anonymity, and authenticity as the traditional PKI-based protocols, while taking much less computation and communication overhead in the IVC authentication since only hash function and MAC operations are required. In spite of the anonymity assurance, the scheme can well achieve conditional traceability for the authorities in case of any traffic dispute. The conditional anonymity is due to the fact that all the accepted messages are uniquely tied to an anonymous pseudo ID created by an RSU, while this pseudo ID can be further tied to an anonymous pseudo ID of its sender. Thus,

by checking these two unique anonymous pseudo IDs, the authorities can trace the unique real world identity of the message sender as that can be done in the traditional PKI-based protocols, which will be detailed in Section 3.4.1.

3.3.8 Parameters Selection

Determine the parameter L

Without loss of generality, one RSU is allocated at an intersection, and each intersection has four adjacent intersections. As exemplified in Fig. 3.12, RSU_0 is next to the intersections where RSU_i is located, for $i = 1, 2, 3, 4$. Further, each street is two way road with two lanes; and each vehicle periodically broadcasts its routine safety messages within each time interval ΔT, which is 300 ms.

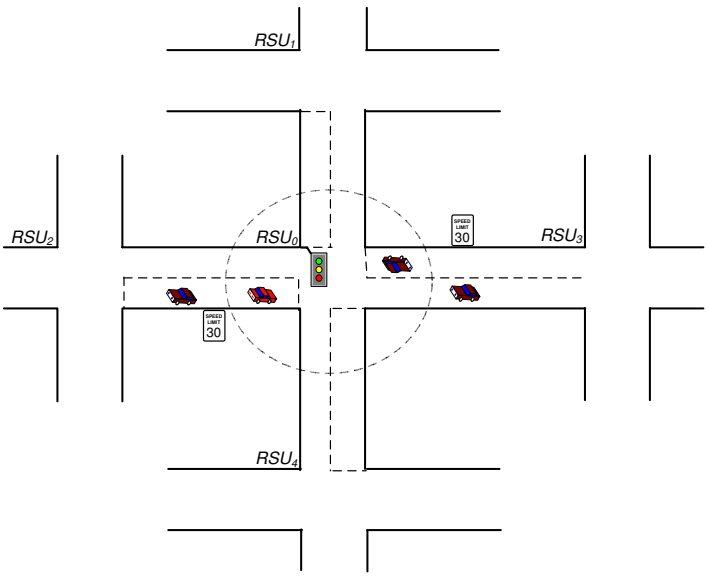


Figure 3.12: Considered road architecture

The length L of each key chain can be determined

$$L = \lceil r_{max}/0.3 \rceil + N \tag{3.18}$$

where N is the number of time intervals that each key chain sub-pool is responsible for, $r_i = \frac{l_i}{vi}$, $i = 1, 2, 3, 4$, $r_{max} = \max\{r_1, r_2, r_3, r_4\}$. l_i and v_i are the length and speed limit of the street from the intersection to its adjacent intersections, respectively.

Parameter Selection for Y

The value of Y determines the maximum number of vehicles that can communicate with a vehicle passing through the intersection before the vehicle reaches another adjacent intersection. Suppose vehicle arrivals at an intersection follow a Poisson distribution, that is:

$$P\{X = n\} = \frac{\lambda^n}{n!} e^{-\lambda}, n = 0, 1, 2, \cdots, \lambda > 0 \tag{3.19}$$

where X is the number of entering vehicles to the RSU within a time interval, λ is the expected number of entering vehicles to the RSU during an interval.

Based on the road architecture in Fig. 3.12, vehicles can arrive at an intersection simultaneously from different directions. Hence, we have the total number no of the vehicles entering the intersection after a vehicle, which entered the intersection before, and before the vehicle enters another adjacent intersection.

$$no = 4 \sum_{n=1}^{\lceil r_{max}/0.3 \rceil} nP\{X = n\} \tag{3.20}$$

For simplicity, all the vehicles, which enter the intersection after a vehicle, communicate with the vehicle before the vehicle enters another intersection. Therefore, the parameter Y can be

$$Y = \lceil no \rceil \tag{3.21}$$

Parameter Selection for K

K is defined as the sum of Y and the number of total key chains needed for vehicles which are expected to enter the intersection during N time intervals. Hence, we have

$$K = \lceil 4 \sum_{n=1}^{N} nP\{X = n\} \rceil + Y \tag{3.22}$$

3.3.9 Discussions

Security Requirement and Key Disclosure Delay δ

To defend the message forgery attack, the key disclosure delay should be longer than the time for a message to travel from the source to all the recipients within its transmission range. If any receiver r can receive the released key before the original data packet arrives at another receiver, e.g., $\overline{r}$, receiver r who holds the key can forge a message by generating a valid MAC tag to this message and sending the tagged message to $\overline{r}$. This situation can be avoided by properly choosing the key disclosure delay δ. In the vehicular communications with IEEE 802.11p, since the longest transmission range is about 1000 m [3], δ should be slightly greater than the time duration for a message to travel for 1000 m in the wireless channel. In [4], the communication latency is identified as about 10 ms. In our protocol, therefore, δ is set to be 80 ms which is about 8 times of the communication latency for resolving the aforementioned concerns. Note that before performing the normal message authentication process, a receiver has to check the validity of the message by being aware of which time interval that the message belongs to and whether the corresponding key has been released already. If it is not true, the message is dropped without further processing.

Resilience to Message Loss

Inherent from TESLA, our protocol is packet loss tolerant. In other words, no action will be taken when a data packet is lost. If the KRP kr_P_i is lost, the legitimacy

of the previous message can still be verified upon receiving kr_P_j with $j > i$. The broken key chain can be reconnected by applying the hash function $h(x)$ $j - i$ times and obtaining $h_i = h^{j-i}(h_j)$. Also, the receiver checks if $h(h_i) = h_{i-1}$, where h_{i-1} is the last successfully received key. If so, the newly arrived key value h_j is acceptable. However, if multiple continuous packets are lost such that the time to wait for the new KRP is longer than the maximum tolerable message delay, M_j is neglected. In this case, the subsequent messages can still be authenticated when new data packets arrive.

Time Synchronization

Similar to TESLA, the security offered by the proposed protocol heavily relies on loose time synchronization among the vehicles, which can easily be achieved by some time synchronization protocols [29, 47, 48]. Currently, there are two methods to synchronize the senders and the receivers, namely *direct time synchronization* and *indirect time synchronization*, respectively [49]. By considering the high mobility of vehicles in VANETs and the loose time synchronization requirement, our protocol performs a direct synchronization between the RSU and each entering vehicle, while taking indirect time synchronization where all the vehicles in a group are synchronized the external time reference given by the RSU. In specific, when a vehicle enters an RSU, it will be synchronized with the RSU first, and then the vehicle will be given a time reference for slotting time domain. On the other hand, the enumeration of the time slots will be performed through the local clock of the vehicle. Since the residential time for a vehicle is expected to be no more than a few tens minutes, the accuracy of the clock will not be a concern.

3.4 Performance Analysis

3.4.1 Security Analysis

In this subsection, the security of the proposed protocol is analyzed.

- *Data source (or origin) authentication*: In the application scenario considered in the study, data source (or origin) authentication is the assurance for the receivers that received messages originated from a legitimate sender that is claimed to be, but the identity of the sender is unknown to the receivers. In the proposed protocol, a sender, which is also known as the leader (or the header) of a group, always broadcasts a data packet first, which contains a routine traffic-related message and its MAC as well as a pseudo ID of the sender. Then, the key used to calculate the MAC of the message is released in a key release packet after a fixed delay, which is pe-determined to be larger than the maximum transmission delay. Upon reception of the key release packet, the message recipients use the key from the received key release packet to verify data authenticity by recomputing the MAC using the same algorithm and comparing it with the one from previously received data packet.

  In order to forge a packet, the attacker needs to either guess the correct key or generate fake data packet with a MAC obtained from a fake key. The former one is a brute-force attack or an exhaustive key search, which simply does not work if the MAC algorithm is secure, such as MD5 and SHA-1. The latter fails due to the use of a one-way key chain in the proposed protocol, where the chain element serves as the secret keys for computing the MACs of data packets in the opposite order of that a key chain has been generated. If a receiver receives the fake key, the receiver can easily identify that the key is incorrect by checking the relationship between this key and previously successfully received keys (also known as the key commitment of the currently received key) in the key chain. Definitely, it results

in verification failure of the received key. The security depends on the secure characteristics of one-way hash function used to generate one-way key chain.

- *Data Integrity:* Integrity prevents the unauthorized modification of messages in transit. The integrity of considered applications is violated when the correctness and appropriateness of the content of message is modified, destroyed or deleted. Data integrity is assured that the messages from a sender is protected by either using an ID-based signature scheme or TESLA-based self-authenticating one-way chains, which are assigned by an RSU along the roads, as the key to compute the MACs over the original messages.

- *Data source privacy:* The privacy of the data source is well protected because each vehicle is using random pseudo ID to broadcast a message by either using an ID-based signature scheme or TESLA-based self-authenticating one-way chains.

- *Traceability:* We assume that each local government region has its own data center, which periodically collects ID pairs from the RSUs in its domain. An ID pair is composed of two components: one is a vehicle's pseduo ID pid, and another is a dynamic pseduo ID PVID, which is assigned to the vehicles by the RSUs. When the authorities have to reveal the real identities of the message senders, the authorities firstly find the real ID of the RSU by using PVID,

$$(PVID \bmod q_0) \oplus (PVID \bmod p_0) \tag{3.23}$$

  Then, the authorities contact the local government region, which will look up in its database for the *pid* and sends the *pid* back to the authorities. Afterwards, the authorities can reveal the real identities of the message senders as follows.

$$(pid \bmod q_0) \oplus (pid \bmod p_0) \tag{3.24}$$

- *Replay attack resilience:* With a replay attack, an adversary simply replays the intercepted message, which is originally launched by a legitimate user in order

to trick the receivers into believing that they are receiving the message from the legitimate user. Obviously, this attack does not work because a timestamp is embedded into each packet to verify its freshness.

3.4.2 Efficiency Analysis

In this subsection, simulation is conducted to verify the efficiency of the proposed security protocol using ns-2 [50]. We are interested in the system performance concerning with the average *Packet Delay* (PD) and average *Packet Loss Ratio* (PLR), which is further compared with several traditional public key based security protocols [19, 21]. The communication overhead is also investigated for the proposed protocol. For the PLR, we only consider the packet loss caused by security mechanisms instead of lossy wireless channels. The road system considered in the study is the traffic scenario on a straight bi-directional six lane city road, where the vehicles are moving with a speed fluctuation uniformly distributed in a range of ± 5 km/hr centered at the road speed limit that ranges from 5-30 m/s. An intersection is located every 600 meters along the road, where one RSU is installed at each intersection. Other simulation parameters are listed in Table 3.3.

We first simulate the message transmission delay through the wireless channel. Because most of the transmission delay is incurred by wireless channel contention, which means the longest transmission time happens when the density of the traffic is the highest, we simulate the crowded traffic scenario the communication range and inter-vehicle distance as 300 m and 5 m, respectively. The result of the simulation shows the longest transmission delay is around 6.467 ms. Hence, the key disclosure delay δ in the later experiments is conservatively set as 80 ms, which is much larger than the actual delay. Thus, the absolute security can be ensured. We then run two sets of simulations. The first set of simulations investigates the impact of the vehicle moving speed to PLR and PD, whereas the second investigates the impact of vehicle density

Table 3.3: Simulation configuration

simulation area	$3000m \times 50m$
Communication range	300 m
Simulation time	100 s
Channel bandwidth	6 Mbs
Pause time	0 s
Payload for OBU message	200 bytes
Group key verification delay	10.7 ms
ECDSA-224 signing delay	2.92 ms
ECDSA-224 verification delay	3.87 ms

on the two performance metrics. The delay induced by any cryptographic operation in the simulation is automatically taken as delay in the ns-2 simulation according to the measurement of those algorithms based on cryptographic library MIRACL [51].

Impact of Vehicle Moving Speed

In the first set of simulations, v (i.e., the average speed of the vehicles) is changed from 5m/s $\sim$ 30m/s (18km/hr $\sim$ 108km/hr). The initial inter-vehicle distance is 30 meters. The simulation results on PD and PLR are shown in Figs. 3.13 and 3.14. It can be seen that the speed variation does not affect the PD and PLR. According to [4], the maximum allowable message latency is around 100ms to meet the human beings' reaction. Thus, all these protocols can meet this requirement. On the other hand, for PLR, $SERP^3$ yields much lower packet loss ratio compared with that of PKI-based protocols under this normal vehicle density.

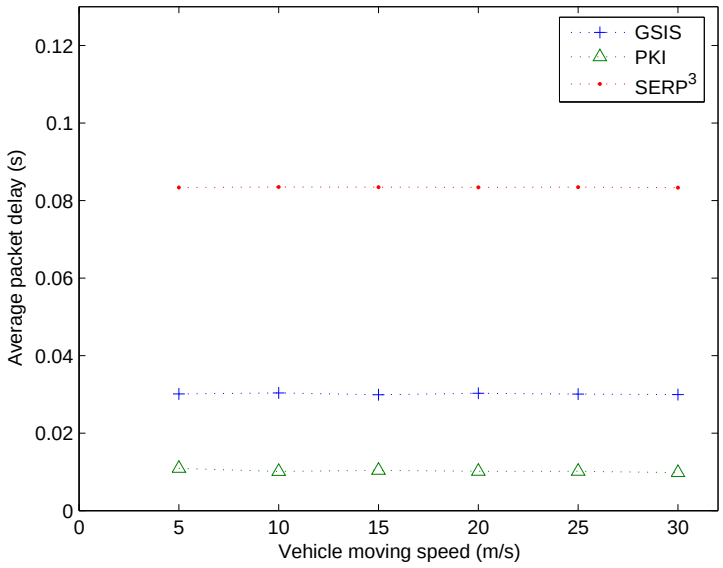


Figure 3.13: Relationship of PD and vehicle moving speed

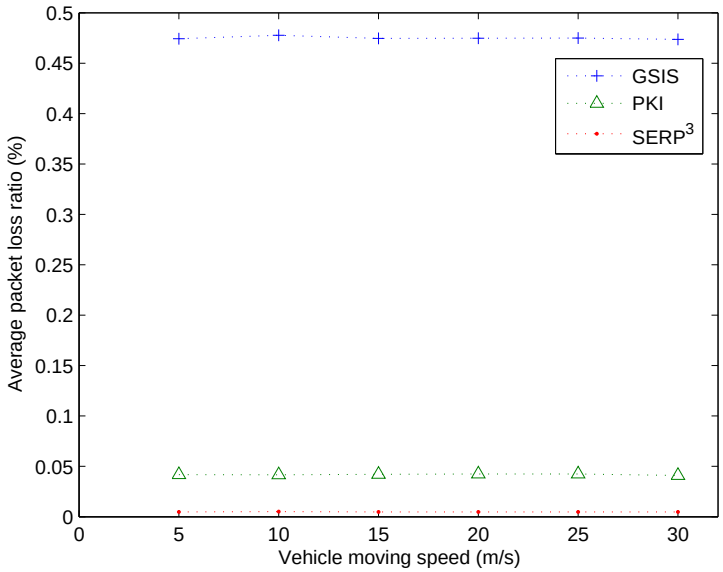


Figure 3.14: Relationship of PLR and vehicle moving speed

Impact of Vehicle Density

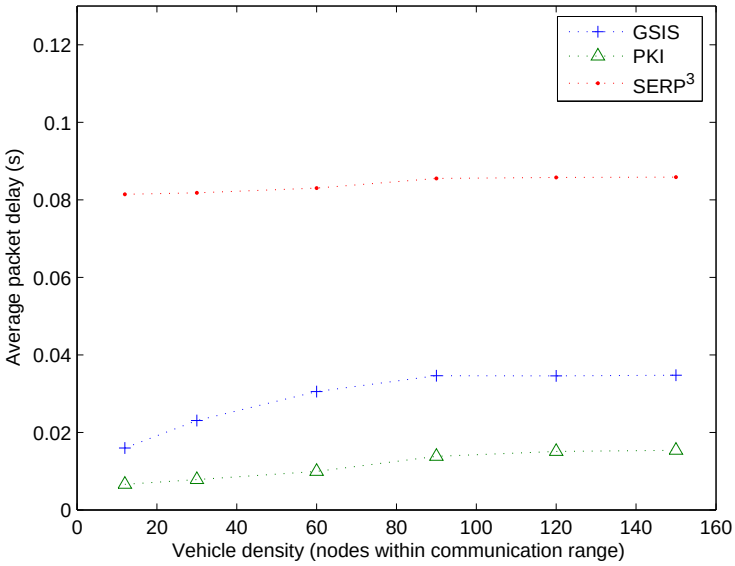


Figure 3.15: Relationship of PD and vehicle density

In the second set of simulations, the impact of vehicle density on PD and PLR is studied. From Fig. 3.15, it can be seen that $SERP^3$ has higher but acceptable packet delay than PKI-based protocols. In addition, the packet delay for all the protocols does not vary much with the increase of the vehicle density. From Fig. 3.16, the traditional public key based protocols suffer from a much higher packet loss ratio when the vehicle density is larger, which makes them not scalable in practical scenario. On the other hand, the proposed $SERP^3$ protocol maintains stable PLR and is not affected by the increase of the vehicle density.

Communication overhead

Next, the communication overhead is investigated for the proposed protocol. We assume that ECDSA-224 is adopted for PKI-based scheme and the size of a signing

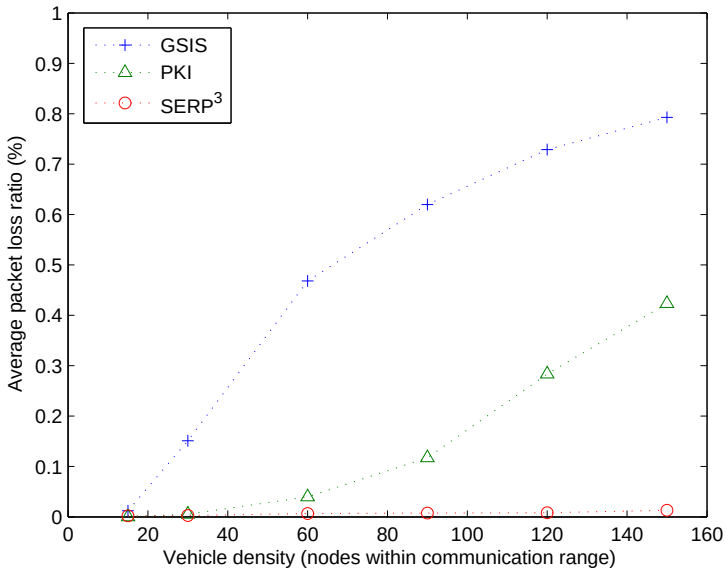


Figure 3.16: Relationship of PLR and vehicle density

certificate for an OBU is 125 bytes [5]. Further, suppose that MAC algorithm adopted in $SERP^3$ is constructed from MD5, which is a widely used cryptographic hash function with a 128-bit hash value. For PKI-based scheme, the communication overhead includes the following two components: (1) the digital signature and (2) public key certificate. For the proposed symmetric-key cryptography based protocol, the communication overhead comes from the following three components: (1) message authentication code, (2) pseudo identity, and (3) key release packet. Fig. 3.17 shows the comparison of communication overhead for PKI-based scheme, GSIS, and the proposed protocol. It is observed that the proposed protocol has the least overhead compared to the other two protocols.

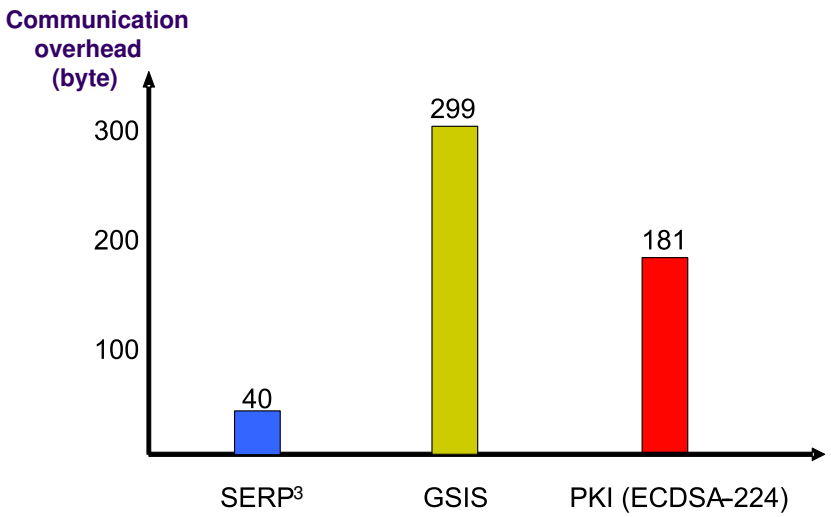


Figure 3.17: The comparison of communication overhead

3.5 Summary

In this chapter, we have introduced a security infrastructure for VANET in which a concept of **ePermit** is defined to serve as a proof of an authorized driver to drive the vehicle and to activate the security system based on proxy signature. Furthermore, we have proposed a novel $SERP^3$ security protocol for achieving efficient and secure inter-vehicular communications. With the symmetric key based scheme and delayed authentication, the packet loss ratio can be significantly reduced without much increasing the packet delay. We have conducted extensive analysis and simulation to verify the proposed protocol, which demonstrated that the proposed protocol cannot only meet the various security requirements and the driver's conditional privacy requirement, but also achieve high efficiency in terms of packet overhead and computation latency.

Chapter 4

Efficient and Cooperative Message Validation Protocol

4.1 Introduction

In the previous chapter, we introduced $SERP^3$, a secure and efficient RSU-aided privacy-preserving protocol. However, RSU may not exist in some situations, for example, in rural areas or in the early stage deployment phase of VANET, where unfortunately, $SERP^3$ is not suitable. In this chapter, we solve the problem from a different perspective by letting vehicles cooperatively verify messages. We propose a complementary Efficient and Cooperative Message Validation Protocol, called ECMVP, where each vehicle probabilistically validates a certain percentage of its received messages based on its own computing capacity and then reports any invalid messages detected by it.

Computing power is a precious asset for each individual vehicle. Besides for message validation, it also can be used for many purposes, such as infotainment dissemination for drivers and passengers including listening to mp3. The higher the vehicles' verification probability is, the higher the computing cost is. However, a vehicle also wants to detect any invalid message because it could be at risk if it consumes an invalid message.

Therefore, as for a vehicle cooperative message validation protocol, it is desired to find the minimum verification probability needed for each vehicle to assure adequate chance and find his comfort level to detect any invalid message.

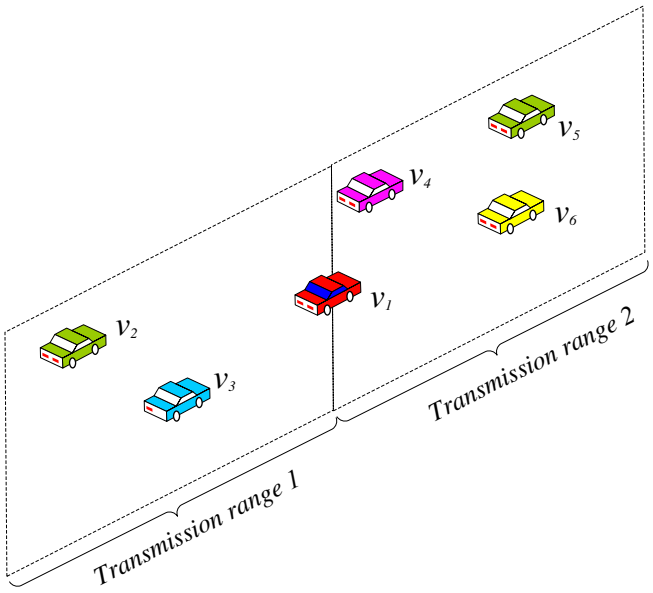


Figure 4.1: A group of vehicles which are divided by v_1 into two regions

However, there exists a reliability issue with regard to reporting mechanism used above. To illustrate the problem, as shown in Fig. 4.1, an example of vehicular network is used where two transmission ranges are defined and it is assumed that there exists a malicious vehicle v_1. One transmission range, Transmission 1, covers vehicles behind v_1, and another one, Transmission 2, covers vehicles ahead of v_1. We assume that v_1 sends out a bogus message. Upon receiving the bogus message, v_5 verifies the message and discovers that it is invalid. Then, v_5 broadcasts an accusation to alert the other nearby vehicles. However, since v_2 and v_3 are not in the transmission range of v_5, v_2 and v_3 will miss the accusation from v_5. Therefore, in order to ensure that vehicle v_2 and v_3 also receive an accusation, in this case that there should at least two vehicles that validate v_1's message, where the two vehicles are in the Transmission range 1 and

2, respectively.

The remainder of the chapter is organized as follows. In Section 4.2, we present the basic idea behind cooperative probabilistic message validation. Then, a detail reliability analysis is presented in Section 4.3. Afterwards, we discuss a solution to misbehavior resilience in Section 4.4. Finally, we give the summary in Section 4.5.

4.2 Probabilistic Verification

Without loss of generality, a PKI (Public Key Infrastructure)-based secure and privacy-preserving framework is built for vehicular communications, where each vehicle maintains a large set of public/private key pairs and their corresponding anonymous public-key certificates including pseudonyms as their identities [20]. We assume that vehicles are homogeneous and have the same computing power. Also, each vehicle can only process up to N received message per second based on its computing power. As we mentioned before, under some circumstances of high traffic density, for example, traffic jams are common on the road, a vehicle may not be able to validate its received messages fast enough if PKI is used to ensure security and privacy preservation, which results in the loss of message. Instead of letting vehicles validate all their received messages, vehicles validate any received message with a probability p. Also, for achieving the aforementioned cooperative probabilistic message validation mechanism, every vehicle maintains one table, as shown in the following, consisting of received messages but unverified and a timer which controls how long the corresponding message needs to wait before it can be consumed by the receiver. If the timer hits 0, the entry will be removed and the corresponding stored message will be consumed by the vehicle. However, if a message is accused bogus before timeout, it will be discarded and removed from the table.

Received message	Timer

Data: V_i received a message M_j and its corresponding signature σ_j from V_j
Result: *True* if σ_j is valid; *False* if σ_j is invalid

for *each vehicle* V_i *that received* $\langle M_j, \sigma_j \rangle$ **do**
  V_i chooses either 1 with probability p or 0 with probability $1 - p$;
  if V_i *chose 1* **then**
    V_i verifies σ_j;
    if σ_j *is valid* **then**
      V_i keeps silence;
      return *True*;
    else
      V_i one-hop broadcasts an accusation $\langle ID_{M_j}, \sigma_i \rangle$;
      return *False*;
    end
  else
    V_i waits Δt ms for other vehicles' accusations, which tell whether σ_j is valid or not;
    if *there no such accusation* **then**
      return *True*;
    else
      V_i received such an accusation from V_k;
      V_i verifies σ_j;
      if σ_j *is indeed invalid* **then**
        return *False*;
      else
        return *True*;
      end
    end
  end
end

Algorithm 2: Probabilistic Verification Algorithm

The details of cooperative probabilistic message validation are shown in Alg. 2. In Alg. 1, V_i, V_j, V_k are three vehicles that can one-hop communicate with each other, where $i, j, k = 1, \ldots, n$ and $i \neq j \neq k$. When V_i receives a message $\langle M_j, \sigma_j \rangle$ sent by V_j where σ_j is the signature of V_j on the message M_j, V_i determines whether to verify the signature σ_j with probability p (we name p the *verification probability*). If V_i determines to verify σ_j, and σ_j is proved to be valid, V_i keeps silence and consumes M_j. On the other hand, if V_i verifies σ_j and discovers that σ_j is invalid, V_i informs other neighbors that $\langle M_j, \sigma_j \rangle$ is an invalid message by one-hop broadcasting an accusation $\langle ID_{M_j}, \sigma_i \rangle$, where ID_{M_j} is used to uniquely identify the message $\langle M_j, \sigma_j \rangle$, for example, a hash value of $\langle M_j, \sigma_j \rangle$, and σ_i is the signature signed by V_i on ID_{M_j}. Otherwise, if V_i determines not to verify σ_j, V_i waits a predefined Δt ms for other neighbors' accusations on this message. If V_i receives an invalidity accusation $\langle ID_{M_j}, \sigma_k \rangle$ from V_k within Δt, V_i knows that $\langle M_j, \sigma_j \rangle$ may be invalid. To ensure $\langle M_j, \sigma_j \rangle$'s invalidity, V_i verifies $\langle M_j, \sigma_j \rangle$ by itself. If V_i does not receive any accusation from other neighbors within Δt, V_i treats $\langle M_j, \sigma_j \rangle$ as a valid message by default. It is worth noting that Δt should be greater than the total time of verifying two signatures and the transmission delay between two vehicles.

4.3 Reliability Analysis

This section discusses how to guarantee that the invalidity accusation of a specific message M_i will always be received by all neighboring vehicles of the malicious sender. Intuitively, at least one vehicle should work as the candidate to verify the message M_i, namely the probability that there exists at least one vehicle, which will verify M_i, is as close to 1 as possible. However, from the communication range's point of view, only one vehicle that verifies a message is not enough. For example, in Fig. 4.1, suppose that V_3 and V_4 are V_1's neighbors. V_1 sends a bogus message and V_3 determines to verify it while V_4 not. Since V_4 is not in the communication range of V_3, it cannot receive the

accusation from V_3. Therefore, without loss of generality, there should exist at least two vehicles verifying a message sent by a vehicle, say V. One vehicle should physically be in front of V, while the other should be behind V.

Let n be the total number of neighboring vehicles of V (or referred to as traffic load), i be the number of neighbors in front of V, $n-i$ be the number of neighbors behind V. Notice that the value of n can be known by each vehicle because each vehicle periodically broadcasts its traffic related information (e.g., a pseudo identity and a position) every 300 ms. Suppose that V's neighbors are uniformly distributed around V and each vehicle's position is independent. Let A_i be the event that there are i vehicles in front of V and $n-i$ vehicles behind V. Let B be the event that there are two vehicles that will verify a message sent by V, one of which is in front of V and the other is behind V. Then $\Pr\{B\}$ can be represented as a function of n and p.

$$\begin{aligned}\Pr\{B\} &= \sum_{i=0}^{n} \Pr\{B|A_i\} \cdot \Pr\{A_i\} \\ &= 1 + (1-p)^n - 2 \cdot (1 - \frac{p}{2})^n\end{aligned} \tag{4.1}$$

where $\Pr\{B|A_i\} = (1-(1-p)^i) \cdot (1-(1-p)^{n-i})$, and $(1-p)^i$ is the probability that none of i vehicles in front of V will verify a message sent by V, $1-(1-p)^i$ is the probability that there is at least one vehicle that will verify the message, and $1-(1-p)^{n-i}$ is the probability that there is at least one vehicle behind V that will verify the message, respectively; $\Pr\{A_i\} = \frac{\binom{n}{i}}{\sum_{l=0}^{n}\binom{n}{l}} = \binom{n}{i}(\frac{1}{2})^n$. Our objective is to make $\Pr\{B\}$ as close to 1 as possible with minimum p. In other words, each vehicle aims to use a minimum computing resource while makes sure that any invalid message can still be detected.

Fig. 4.2 shows the relationship among $\Pr\{B\}$, p, and n. It can be seen that $\Pr\{B\}$ increases as either p or n increases. The increasing gradient is rather sharp. $\Pr\{B\}$ quickly approaches to 1 even if p is a small value when traffic load is large (e.g., $\Pr\{B\} = 99.98\%$ when $p = 15\%, n = 120$). Moreover, we can conclude from Fig. 4.2 that when $\Pr\{B\}$ is fixed, p is inversely proportional to n. In particular, when n is

large, p should be small, and vice versa. Our objective is to change p to make $\Pr\{B\}$ approach to 1 as much as possible. On the other hand, under the condition that $\Pr\{B\}$ has sufficiently approached to 1, we try to make p as small as possible because a small value of p implies that a vehicle can potentially save processor (e.g., CPU) resources and can further verify more messages when the traffic load becomes larger.

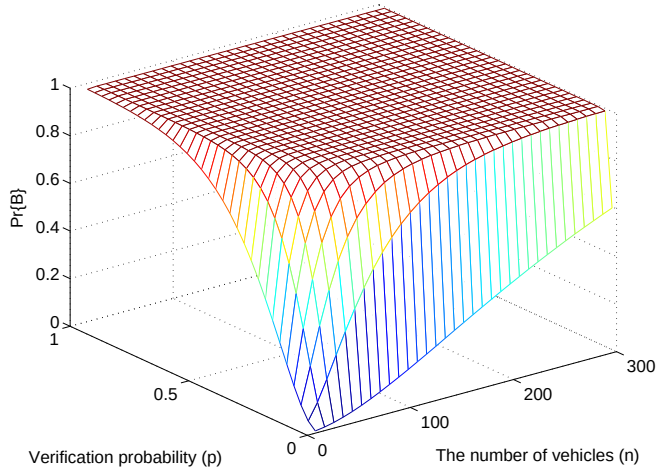


Figure 4.2: Pr{B} vs. traffic load and verification probability

In order for each vehicle to choose an appropriate p under different values of n, we use the parameter $k = n \cdot p$ to leverage the inversely proportional relationship between p and n. Notice that k presents the average number of signatures that a vehicle verifies every 300 ms because n is the total number of neighbors each of which sends a message every 300 ms, and p is the verification probability. If we can find a suitable k, then the corresponding p can be determined. Based on Eq. 4.1, we can obtain the relationship between $\Pr\{B\}$ and n in terms of different k as shown in Fig. 4.3. From Fig. 4.3(d), we can see that $\Pr\{B\}$ with $k = 25$ is sufficiently close to 1 no matter how large n is. Therefore, we conclude that in ECMVP we can set k as a constant value, i.e., 25. Since k is fixed, p can be computed as k/n (that is, $25/n$). In other words, we can change p according to n. For example, a vehicle V having 50 neighbors receives a message M_i,

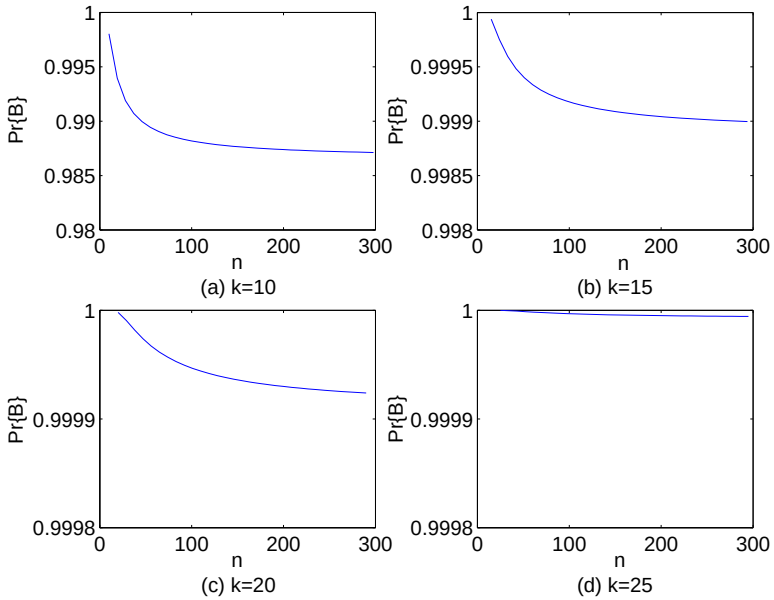


Figure 4.3: Pr{B} vs. traffic load

and V will verify M_i with the probability of 25/50. Notice that V knows the number of its neighbors. In case that n is less than 25, let p be equal to 100%. It is worth noting that k cannot be larger than the vehicle V's verification capability, which is the maximum number of verifications that the vehicle V can process.

4.4 Misbehavior Resilience

Misbehavior or selfish behavior is an inherent attack in cooperative networks. In our scheme, there are two kinds of misbehaviors: 1) some vehicles do not verify any signature and instead they just wait for other honest nodes' accusations; 2) some vehicles verify signatures but they do not send any accusation to other vehicles. Previously related studies have addressed misbehavior issues. Zhang *et al.* in [52] introduce a credit based scheme that encourages nodes forwarding packets in mobile ad hoc net-

works. Zhang *et al.* in [53] employ a tamper-proof device in vehicular sensor networks, and the tamper-proof device can trustworthily generate pseudo random identities for a vehicle. Although these schemes can prevent misbehavior, the overhead is high (such as credit management in [52]).

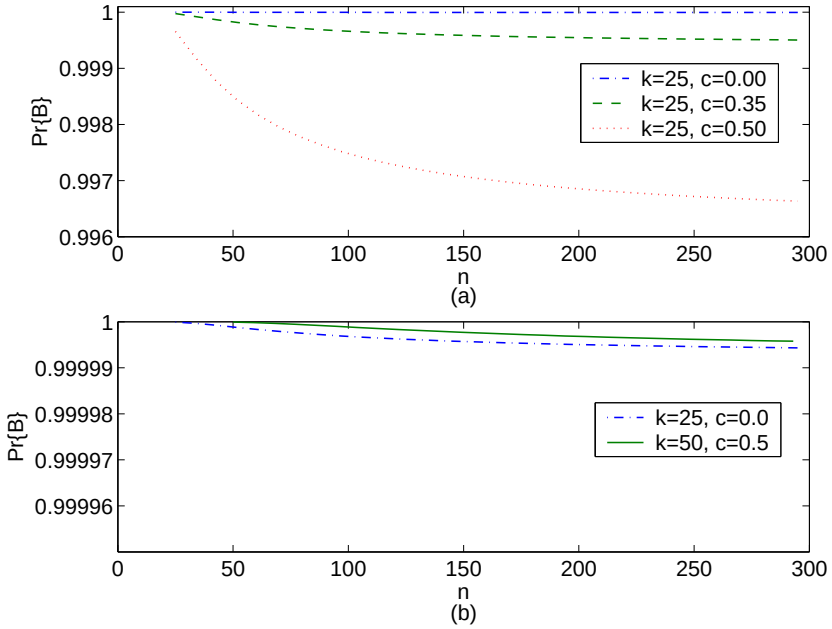


Figure 4.4: Pr{B} vs. traffic load given different k and c

Based on ECMVP, we can increase the value of k (and the corresponding p) to eliminate the effect caused by misbehaving vehicles. Assume that the total percentage of misbehaving vehicles in VANETs is not more than 50%, which is similar to that in [54–56]. This assumption is reasonable because in reality misbehaving vehicles make up only a small portion of the total vehicles. Let c represent the percentage of misbehaving vehicles in vehicular networks. In this case, if a vehicle has n neighbors, there would exist $(1-c)\cdot n$ vehicles that apply ECMVP and $c\cdot n$ misbehaving vehicles. As such, based on Eq. 4.1, $\Pr\{B\}$ equals $1+(1-p)^{(1-c)\cdot n}-2\cdot(1-p/2)^{(1-c)\cdot n}$. Fig. 4.4(a) shows that $\Pr\{B\}$ decreases as c increases. The ideal result is to keep $\Pr\{B\}$ as the

case where $k = 25, c = 0.0$ (as shown Fig. 4.3(d)). Our solution is to increase the parameter k, i.e., let $k = 50$. Fig. 4.4(b) indicates that the $\Pr\{B\}$ with $k = 50, c = 0.5$ approximates the $\Pr\{B\}$ with $k = 25, c = 0.0$. Therefore, ECMVP with $k = 50$ can effectively eliminate the negative effects of misbehaving vehicles but with the cost of increasing computational cost.

4.5 Summary

In this chapter, we have proposed a protocol complementary to $SERP^3$ to address the situation where RSU doesn't exist in VANET, which is possible in the early stage deployment phase of VANET. The proposed protocol not only retains the security and privacy preservation properties inherited from PKI-based solutions, but also solves the scalability issue.

Chapter 5

Secure VANET-based Road Traffic Control System

5.1 Introduction

In the previously chapters, we have introduced a security architecture as well as a secure and efficient RSU-aided privacy-preserving protocol for vehicular communications. The ultimate goal of vehicular communication network is to develop vehicle safety/non-safety related applications to improve road safety and facilitate traffic management and infotainment dissemination for drivers and passengers. In next two chapters, we will propose two vehicle applications to exploit advantages of vehicular communications while taking those application specific threats into consideration.

It is a commonly used approach by installing a temporary traffic sign to assist road traffic control so as to direct vehicular and pedestrian traffic to circumvent an accident scene or road disruption area. For example, when there is a car accident on the highway, it is necessary for the road authorities to have warning signs posted to warn drivers to take caution when they are approaching. Nevertheless, even though there is a warning sign ahead, it could still not be completely solving since some drivers

may ignore the warning sign due to many reasons such as bad weather. In addition, when there is an unexpected event on the roads, road authorities may not be notified in time to set up the warning signs. The time span between the occurrence of the accident event and the installation of warning signs becomes the most dangerous to the public, in which the subsequent vehicles could easily be affected and led into danger. This problem is worsened due to the fact that many car accidents may not be reported in a timely fashion. Thus, it will be with utmost importance to have a temporary emergency sign available at the scene as early as when the incidents occurs even before the road authorities are notified. Hence, it becomes a very challenging task for achieving dynamic and light-weigh traffic control in the efforts of how to rapidly and accurately disseminate road conditions information to the subsequent traffic, particularly to those drivers within the affected geographic area.

Recent advances in wireless technology promise a new approach to facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers, such as Approaching Emergency Vehicle Warning [4]. An increasing interest has been raised recently on the applications of roadside-to-vehicle communications (RVC) and Inter-vehicle communications (IVC), aiming to improve the driving safety and traffic management while providing drivers and passengers with Internet access at the same time. One of the main challenges in launching VANETs into practical roadside traffic control systems is on how to identify and defend malicious abuses, security attacks, and privacy violations. Thus, this chapter introduces a Secure VANET-based Road Traffic Control System, or called SVRTCS, in order to circumvent vehicles safely through the areas with abnormal situations while ensuring the security and privacy of the users from various threats. The proposed scheme not only enhances traveler safety but also minimizes capacity restrictions due to any unusual situation. The major advantages of our system lie in the following three aspects: 1) the proposed system can achieve secure road traffic control by way of VANETs; 2) the system contains a wrong-way driving

warning system to identify wrong-way driving by way of vehicular communication and multilayer perceptron (MLP) network technologies. The wrong-way driving warning system is devised to predict the possible future direction of a vehicle and then warn the driver about potential wrong way driving to prevent possible head-on collisions; and 3) the proposed system introduces a new implementation of RSUs, namely *temporary RSUs* (**tRSUs**). An **tRSU** is automatically formed by a vehicle involved in an abnormal situation, such as car accident, to serve as temporary RSU to improve the safety around the scene of the accident.

The remainder of the chapter is organized as follows. As a preliminary of the proposed scheme, multilayer perceptron classifier is presented in Section 5.2. In Section 5.3, the considered system model is presented along with a number of severe security and privacy threats in the application scenario. In Section 5.4, the proposed secure VANET-based road traffic control system is presented, and the security and efficiency of the proposed mechanism are analyzed and discussed in section 5.5. Finally, Section 5.6 summarizes the chapter.

5.2 Multilayer Perceptron Classifier

As a fundamental enabling technique of the proposed system, the preliminary knowledge about multilayer perceptron classifier is briefly introduced in this section.

An artificial neural network is initially inspired by the human brain and attempts to electronically simulate the human brain's ability to achieve the corresponding functions. Neurons, as basic elements in a neural network, work in unison. Each neuron that receives signals transferred from its frontward-neighbor neurons combines all information together, performs a general nonlinear activation operation, such as sigmoid transfer function, and then delivers the result to its backward-neighbor neurons. The link connecting two neurons is given a weight, which signifies how closely two neural connect. All weights can converge on a steady value after the neural network is

trained. Thus, a neural network in which neurons are appropriately interconnected along with weights can achieve an "intelligent" mission, such as pattern classification, clustering/categorization, function approximation, prediction/forecasting, optimization, content-addressable memory [62].

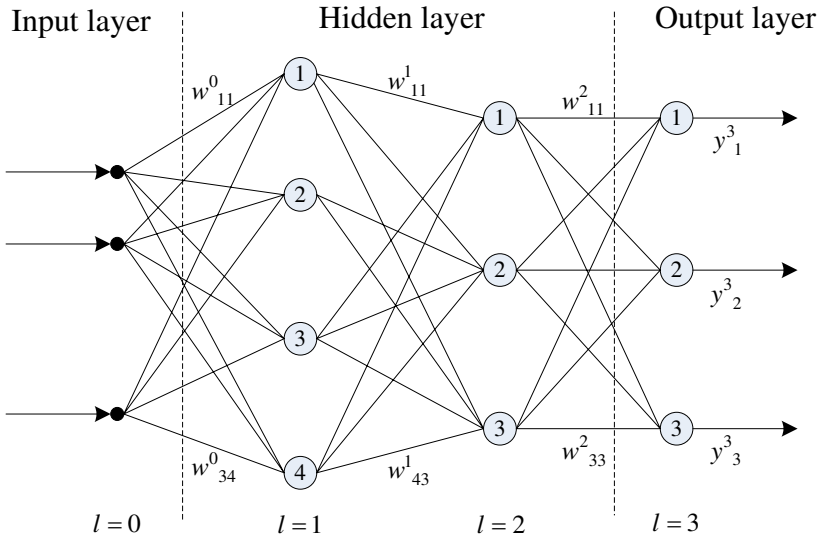


Figure 5.1: A three-layer perceptron network

Multilayer Perceptron (MLP) neural network, as the most popular neural network, is widely used for pattern classification today, and can find arbitrarily complex decision boundaries and represent any Boolean function [65]. Given enough neurons and appropriate layers, an MLP can efficiently approximate any desired function and achieve a great accuracy. The MLP network consists of multiple layers, including the input layer, hidden layer (which contains one or more sub-layers), and an output layer, as shown in Fig. 5.1. The number of neurons of an input layer is determined by the number of dimensions of input data space. The number of sub-layers of a hidden layer and neurons in each sub-layer depends on the complexity of classification. Roughly speaking, the more sub-layers and neurons the hidden layer has, the more accurate the result of the classifications is. However, as the number of neurons increases, the time consumed on

training the network increases as well. Thus, in most cases, a tradeoff is required. For classification purpose, the number of neurons of an output layer is equal to the number of classes, and each neuron stands for each class. There are two phases needed for an MLP as a classifier, a classification phase and a training phase.

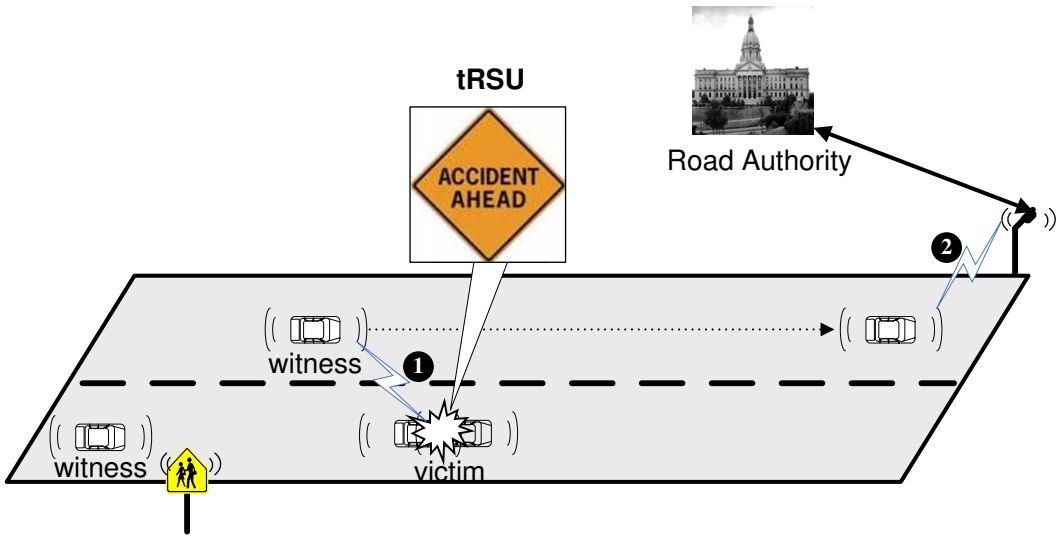
The objective of a training phase is to tune the weight of each link in the network by way of a large number of input training samples and their corresponding desired outputs, so that these weights can well contribute to a good classification result. Compared with the classification process, the training process is relatively complicated. The most typical training algorithm is the back-propagation algorithm [65]. The algorithm is used to calculate the gradient of the error of the network. Through the learning process, the errors propagate backwards from output layer to input layer, and the weights of the network are modified to minimize any error that might happen next time. In the classification phase, from the input layer to the output layer, each neuron sums up all data coming from the neuron of the previous intermediate neighbor layer. Before summation, each data is multiplied by a weight, which is obtained from a training process. At the output layer, the neuron having the largest summation value indicates that the input data belongs to the neuron (class).

5.3 System Model

In this section, we introduce the system model considered in this chapter, followed by a detailed illustration of several identified severe attacks against the system. Then, we propose a VANET-based secure road traffic control system.

5.3.1 System Overview

As shown in Fig. 5.2, when an incident happens, the cars involved in the incident automatically form an **tRSU** based on a trigger event, such as turning on the emergency



❶ A witness detects a car accident, and supports accident victims to evolve into a temporary RSU (**tRSU**).

❷ report to road authority over car accident.

Figure 5.2: Road traffic control at a car accident scene

lights and trig of the airbag. Also, we assume there does not exist any RSU within the transmission range of the accident scene. Otherwise, this RSU will automatically become an "accident ahead" warning RSU, which alerts any approaching drivers to the hazard. After the **tRSU** are formed by the vehicles involved in the accident, all the vehicles approaching the scene will receive the warning message from the **tRSU** and take some proper actions.

The above mechanism is straightforward and expected to effectively mitigate the potential danger caused by the roadside accident events. However, this may suffer from some malicious attacks, such as fake RSU attack. With such an attack, the adversary may set up a malicious **tRSU** to fool other drivers by providing a fake accident ahead message to the others such that it can manipulate to get a better traffic condition. Inspired by the fact that a network is insecure if the majority of nodes become malicious, we assume that k is an oracle number, and any set of k drivers supports one **tRSU**, the **tRSU** will be taken as authentic RSU and then will be trusted by all the other drivers. Hence, the initiator(s) should get enough supports from other drivers in order to evolve into a trusted **tRSU**. Therefore, if an approaching driver witnesses the accident, he/she should support the accident victims to evolve into a trusted **tRSU** by sending a support message. Afterwards, the witness may phone the road authorities straight away and help the casualties. If the witness chooses to continue traveling, the car accident will be reported automatically to the road authorities when the witness approaches the first RSU that he/she meets along the road.

5.3.2 Threat Models

As a special implementation of mobile ad hoc networks (MANETs), a VANET inherits all the known and unknown security weaknesses that are associated with MANETs, and could be subject to many security threats. In this section, we mainly discuss a number of application-specific security and privacy threats. A whole and compre-

hensive description of general security and privacy threats in VANETs is available in Section 1.3.1.

Privacy Threats

- Personal information protection: The personal information of drivers involved in an accident shall be protected unless the information is legally required or permitted.

Security Threats

- Bogus road control message attack: The adversary may put up a fake or illegal **tRSU** to send fake road control messages to meet a specific purpose. For example, one may send a fake road closed message to the others so as to get a better traffic condition.
- Sybil attack: In the application scenario considered in the study, the sybil attack is the one in which an adversary generates a large number of pseudonymous entities and use them to help a fake **tRSU** to evolve into a trusted **tRSU**.

5.4 Secure VANET-based Road Traffic Control System

The proposed secure VANET-based road traffic control system is composed of three components: system initialization, **tRSU**s formation, and wrong-way warning.

5.4.1 System Initialization

Given a security parameter k, a 5-tuple $(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P)$ is generated by running $\mathcal{G}en(k)$. The Ministry of Transportation (MTO) acts as a trusted authority (TA) and chooses

two random numbers $s_1, s_2 \in \mathbb{Z}_q^*$ as the *master* private keys. Then, the TA computes the corresponding public keys $P_{pub1} = s_1 P$ and $P_{pub2} = s_2 P$. Let f, h, H be three secure cryptographic hash functions, where $f : \mathbb{G}_1 \rightarrow \mathbb{Z}_q^*$, $h : \{0,1\}^* \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$, and $H : \mathbb{G}_1 \times \mathbb{Z}_q^* \rightarrow \mathbb{G}_1$. Then, the system parameters are **params**$=(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, P_{pub1}, P_{pub2}, f, h, H)$.

Further, in the system, each vehicle is assumed to be preloaded with a tamper-proof device, which is a device such that an attacker cannot extract any data stored in the device [19, 61]. When a vehicle registers itself to the TA, the TA will assign a unique identity $ID \in \mathbb{Z}_q^*$ and a password *pwd* to the vehicle. Also, the TA will inject the tamper-proof device with $\langle ID, pwd \rangle$, **params**$=(q, \mathbb{G}, \mathbb{G}_T, \hat{e}, P, P_{pub1}, P_{pub2}, f, h, H)$ and *master* private key (s_1, s_2). The password *pwd* is required in the authentication process by the tamper-proof device. Thus, an attacker cannot take advantage of the tamper-proof device even if the vehicle is stolen.

Then, in order to achieve privacy preservation, each vehicle uses the tamper-proof device to generate the pseudo-identity based key. Fig. 5.3 gives the flowchart of key generation, and the detailed steps are listed as follows.

Step 1. When the vehicle inputs its identity ID and password *pwd*, the tamper-proof device first authenticates the inputs. If the authentication passes, the tamper-proof device proceeds the next step; otherwise returns $\perp$ and terminates the procedure.

Step 2. The tamper-proof device generates a random number $r \in \mathbb{Z}_q^*$, and computes the pseudo-identity $PID = (PID_1, PID_2)$, where

$$\begin{cases} PID_1 = rP \in \mathbb{G}_1 \\ PID_2 = ID \cdot f(rP_{pub_1}) \bmod q \end{cases} \tag{5.1}$$

Step 3. The tamper-proof device then generates the corresponding one-time identity-based private key $SK = (SK_1, SK_2)$, where

$$\begin{cases} SK_1 = s_1 \cdot PID_1 \in \mathbb{G}_1 \\ SK_2 = s_2 \cdot H(PID_1, PID_2) \in \mathbb{G}_1 \end{cases} \tag{5.2}$$

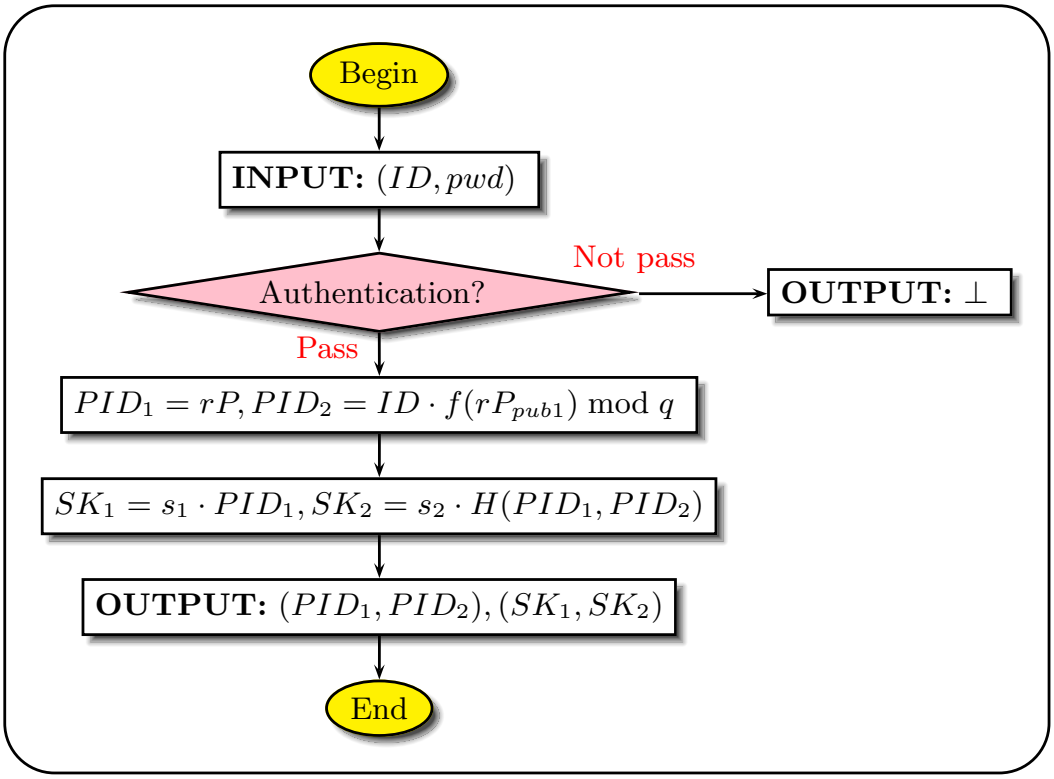


Figure 5.3: Pseudo-identity based key generation in tamper-proof device.

Step 4. The tamper-proof device outputs the pseudo-identity $PID = (PID_1, PID_2)$ and the corresponding private key $SK = (SK_1, SK_2)$ to the vehicle.

Note that the pseudo-identity PID and the private key SK can be generated offline. In other words, a vehicle can first obtain a list of pseudo-identities and the corresponding private keys, then no delay will be caused at the vehicle side due to this process.

5.4.2 tRSU Formation

When a traffic accident occurs shown in Fig. 5.2, any vehicle involved in the accident with a pseudo-identity $PID^i = (PID_1^i, PID_2^i)$ will use the private key $SK^i = (SK_1^i, SK_2^i)$ to sign the warning message m as

$$\sigma_i = SK_1^i + h(m, PID_2^i) \cdot SK_2^i \in \mathbb{G}_1 \tag{5.3}$$

and then sends out the signed warning message with the following format

Payload Head	Payload	Signature
PID^i (84 bytes)	m (200 bytes)	σ_i (64 bytes)

After receiving the warning message, other vehicles can check its validity by the following equation,

$$\hat{e}(\sigma_i, P) = \hat{e}(PID_1^i, P_{pub1}) \cdot \hat{e}(h(m, PID_2^i) \cdot H(PID_1^i, PID_2^i), P_{pub2}) \tag{5.4}$$

If it holds, the warning message can be convinced. Otherwise, the warning message will be filtered out. Since

$$\begin{aligned}
&\hat{e}(\sigma_i, P) \\
=&\hat{e}(SK_1^i + h(m, PID_2^i) \cdot SK_2^i, P) \\
=&\hat{e}(SK_1^i, P) \cdot \hat{e}(h(m, PID_2^i) \cdot SK_2^i, P) \\
=&\hat{e}(s_1 \cdot PID_1^i, P) \cdot \hat{e}(h(m, PID_2^i) \cdot s_2 \cdot H(PID_1^i, PID_2^i), P) \\
=&\hat{e}(PID_1^i, P_{pub1}) \cdot \hat{e}(h(m, PID_2^i) \cdot H(PID_1^i, PID_2^i), P_{pub2})
\end{aligned} \tag{5.5}$$

At the beginning, this **tRSU** is not fully trusted by other approaching vehicles. However, it is expected that even the **tRSU** is not fully trusted yet, other drivers will still approach carefully by responding to the warning. Hence, to enhance the trustiness of car accident warning message broadcast by an **tRSU**, some passing-by vehicles will use their private keys to sign the same warning message m after they witness the incident. For example, the vehicle with a pseudo-identity PID^j will send the valid $\langle PID^j||m||\sigma_j\rangle$ to the initiator(s).

After a while, suppose the initiator(s) holds n signed warning messages $\langle PID^1||m||\sigma_1\rangle$, $\cdots$, $\langle PID^n||m||\sigma_n\rangle$, $n \geq 1$. We assume that n is an oracle number that is accepted by every driver, and any set of n drivers are unlikely becoming malicious. Given supports to one **tRSU** by the other n drivers, the **tRSU** will be trusted by all the drivers. Intuitively, an **tRSU** can simply broadcast all its possessing signed warning messages to convince any other approaching vehicle of the authenticity of this **tRSU**, but it may impose a large communication overhead on the system if n is large. It is worth noting that the larger n is, the more secure the proposed system can be. Hence, instead, the **tRSU** first aggregates n signatures $\sigma_1, \sigma_2, \cdots, \sigma_n$ into one, i.e.,

$$\sigma = \sum_{j=1}^{n} \sigma_j = \sum_{j=1}^{n} SK_1^j + \sum_{j=1}^{n} h(m, PID_2^j) \cdot SK_2^j \tag{5.6}$$

then sends out the signed warning message with the following format

Payload Head	Payload	Signature
$PID^1\|\|\cdots\|\|PID^n$ ($84 \cdot n$ bytes)	m (200 bytes)	σ (64 bytes)

After receiving the aggregated warning message, any vehicle can check its validity by the following equation,

$$\begin{aligned} \hat{e}(\sigma, P) &= \hat{e}\left(\sum_{j=1}^{n} PID_1^j, P_{pub1}\right) \cdot \hat{e}\left(\sum_{j=1}^{n} h^j \cdot H^j, P_{pub2}\right) \\ &\text{where } h^j = h(m, PID_2^j), H^j = H(PID_1^j, PID_2^j) \end{aligned} \tag{5.7}$$

If it holds, the aggregated warning message can be convinced. Otherwise, the warning message will be filtered out. Since

$$\begin{aligned} &\hat{e}(\sigma, P) \\ =&\hat{e}\left(\sum_{j=1}^{n} SK_1^j + \sum_{j=1}^{n} h^j \cdot SK_2^j, P\right) = \hat{e}\left(\sum_{j=1}^{n} SK_1^j, P\right) \cdot \hat{e}\left(\sum_{j=1}^{n} h^j \cdot SK_2^j, P\right) \\ =&\hat{e}\left(\sum_{j=1}^{n} s_1 \cdot PID_1^j, P\right) \cdot \hat{e}\left(\sum_{j=1}^{n} h^j \cdot s_2 \cdot H^j, P\right) \\ =&\hat{e}\left(\sum_{j=1}^{n} PID_1^j, P_{pub1}\right) \cdot \hat{e}\left(\sum_{j=1}^{n} h^j \cdot H^j, P_{pub2}\right) \end{aligned} \tag{5.8}$$

5.4.3 Wrong-way Warning

Next, a wrong-way warning system is presented. The proposed wrong-way warning system is composed of the following two phases: the vehicle movement prediction phase and the wrong-way detection and warning phase. First, an **tRSU** or a vehicle predicts the movement of any approaching vehicle and its neighboring vehicles, respectively. Then, the movement of the vehicle is checked against its current location as well as road condition. If a possible wrong-way incident is going to happen, a wrong-way warning will be forwarded to the vehicle to alert the driver.

Vehicle Movement Prediction phase

In this phase, the **tRSU** or the vehicle performs the movement prediction to understand the possible moving pattern of an approaching vehicle. The vehicle's movement prediction is comprised of two scenarios: along a road scenario and at an intersection scenario. There are only two directions a vehicle would go in the first scenario, either frontward or backward. In this scenario, we define a R^3 space, where a sample in the space is a three-dimensional vector which is presented as follows:

$$\langle Direction,\ Speed,\ Acceleration \rangle \tag{5.9}$$

where *Direction* denotes the direction that a vehicle is going in, such as east or west, *Speed* denotes the velocity of a driving vehicle, and *Acceleration* denotes whether a driving vehicle accelerates or decelerates. If the value of the field Acceleration is positive, then the vehicle is accelerating. Otherwise, the vehicle is decelerating.

The vectors (X) in the R^3 space are regarded as a feature of the vehicle which can be extracted from an RSU in an offline manner. Then, these vectors as training samples are input into the multilayer perceptron classifier as represented in Section 5.2. The back-propagation algorithm is employed to train the weights of our classifier. In this scenario, the number of neurons in an output layer is equal to two because there are only two possible outputs, going frontward or backward. To make a decision, the larger output of the two neurons is treated as a correct result. For instance, the first neuron denotes going frontward, and the second neuron denotes going backward. If the result of the output layer is that the first neuron is larger than the second, this means that the vehicle will go frontward in the near future.

In a VANET, in most cases of the first scenario, a vehicle will go forward unless some accidents occur. However, when we take the second scenario into account, in which a vehicle is going through an intersection, the direction prediction of a vehicle will become much more complicated. Generally speaking, when a vehicle arrives at an intersection, as shown in Fig. 5.4, there are four directions a vehicle can choose among.

For example, a vehicle might turn left, turn right, go ahead, or U-turn. Similar to the first scenario, we define a R^5 space, and a sample in the space is a five-dimensional vector as presented below:

$$\langle Direction,\ Speed,\ Acceleration, Turn\text{-}Light,\ Traffic\text{-}Light\rangle \tag{5.10}$$

where the first three fields have the same meaning as presented in the first scenario. The fourth field, Turn-Light, denotes signals of the turn light of a vehicle, particularly when a vehicle is going to turn at an intersection. As we define it, this field has five possible values, 0.2, 0.4, 0.6, 0.8, and 1, which denotes the flashing of a left-turn light, the flashing of a right-turn light, the flashing of a brake light, the flashing of both a left-turn light and a brake light, and the flashing of both a right-turn light and a brake light of the vehicle, respectively. The last field, Traffic-Light, indicates the color of the current traffic light, red, green or yellow.

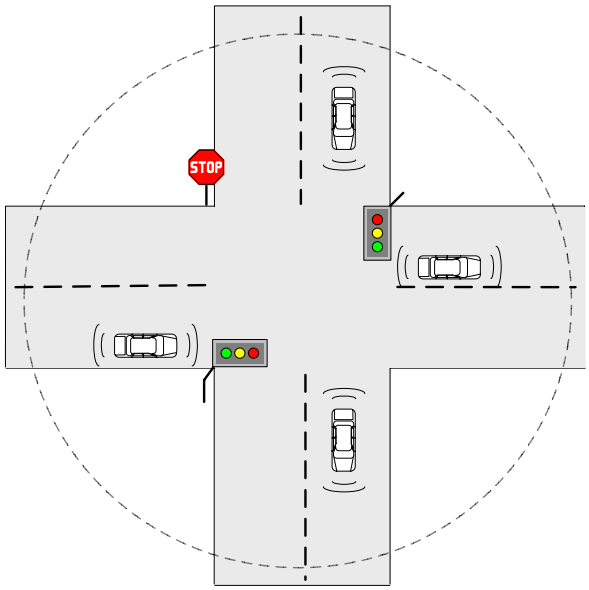


Figure 5.4: The movement direction prediction at an intersection

Similar to the first scenario, vectors (X) in the R^5 space are regarded as training

samples which are also obtained from an RSU. The number of neurons of the output layers depends on how many possible directions an intersection has, and the value is equal to four in Fig. 5.4, for example. Each neuron denotes the direction that a vehicle is going to turn to, and the neuron in the output layer that has the largest value indicates the predication result. Now, through predicting a vehicles movement direction, the **tRSU** or the vehicle has the knowledge of a vehicle's future movement; thus, the **tRSU** and the vehicle is able to find out whether the vehicle is going to enter a closed road or lane based on its current location.

Wrong-way detection and warning phase

Based on the prediction result in the aforementioned phase, the **tRSU** or vehicle further obtains the vehicle's driving direction, location from the vehicle's broadcast traffic-related message, and then checks against the road closure conditions. Next, the **tRSU** or vehicle executes the wrong-way check, which is illustrated in the following example as shown as in Fig. 5.5.

V_1 is driving on University street southbound, and V_3 and V_4 are driving on University street northbound. Also, V_2 is driving on King street eastbound. Further, part of King street is closed due to an accident. An **tRSU** is installed to inform the drivers about the road closure. Based on V_3's broadcast traffic-related information, the **tRSU** notices that V_3 is going to make a right turn and enter an unsafe and closed area. Then, a wrong-way warning message will be sent to V_3 by the **tRSU** to alert the driver.

5.5 Performance Analysis

5.5.1 Security Analysis

In this subsection, we discuss how the proposed secure VANET-based road traffic control system prevents several general attacks described in the threat models in Section

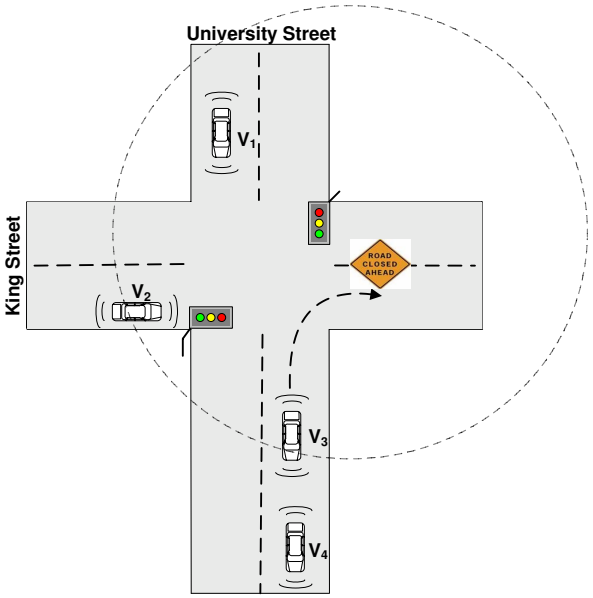


Figure 5.5: Wrong-way detection and warning

5.3.2.

Analysis on Conditional Privacy

To analyze the conditional privacy, we need to show that the following two statements hold: i) no other OBUs and RSUs get to know the real OBU identity from the signed warning messages, and ii) the MTO has the ability to trace the real OBU.

i) Given a signed warning messages (PID^i, m, σ_i), each OBU or RSU can verify its validity with respective to the pseudo-identity $PID^i = (PID^i_1, PID^i_2)$ by Eq. (5.4). However, based on Eq. (5.1), we know PID^i is actually a secure ElGamal ciphertext. Without knowing the master-key s_1, it is hard to recover the real identity ID from $C_1 = rP, C_2 = ID \cdot f(rP_{pub1})$ mod q. Suppose that there exists an adversary who can recover ID from (C_1, C_2) with a non-negligible probability ϵ. Then, by observation, we know the adversary must have either guessed the correct hash value of $f(rP_{pub1})$ or gained the right value rP_{pub1} from (rP, s_1P). Because $f(rP_{pub1})$ is randomly chosen from

$\mathbb{Z}_q^*$, we therefore know the successful guess probability is less than $1/q$. In sequence, we will further know the adversary can resolve the computational Diffie-Hellman (CDH) problem with another non-negligible probability $\epsilon - 1/q$. However, this result leads to the contradiction with the assumption that the CDH problem is hard in $\mathbb{G}_1$. Therefore, we can conclude that no other OBU or RSU can trace the real identity of OBU.

ii) With the master key s_1, the MTO can easily compute rP_{pub1} from C_1, and then recover ID by computing

$$\frac{C_2}{f(rP_{pub1})} \bmod q. \tag{5.11}$$

Therefore, based on the above analysis, the conditional privacy is achieved in secure road traffic control system.

Analysis on Bogus Road Control Message Attack

In order to get a better traffic condition, an adversary may launch the bogus road control message attack. However, since the conditional privacy is ensured, if the bogus road control message takes effects, the real identity of the adversary will be tracked by the MTO such that those abusers can be prosecuted later. Therefore, the conditional privacy actually provides the preventive strategy on this attack.

Analysis on Sybil Attack

In a sybil attack, an adversary generates a large number of pseudonymous entities to help a fake RSU to evolve into a trusted mobile RSU. On one hand, if the signatures signed on these pseudonymous entities cannot pass the verification, they will be filtered out and make no sense. On the other hand, if these signatures are valid, then the MTO could track the real identity of the adversary because of the conditional privacy preservation. Therefore, the sybil attack can also be prevented.

Analysis on Aggregated Warning Message

Eq. (5.8) has shown that if all signatures $\sigma_1, \sigma_2, \cdots, \sigma_n$ are valid, then the aggregated signature $\sigma = \sum_{j=1}^{n} \sigma_j$ is also valid. Now, to analyze the aggregated warning message, we should also show that given $n-1$ valid signatures $\sigma_2, \cdots, \sigma_n$, it is impossible for an adversary to forge an aggregated signature σ which aggregates n signatures. Suppose that an adversary can forge an aggregated signature σ satisfying Eq. (5.7) from $n-1$ signatures $\sigma_2, \cdots, \sigma_n$. Then, since for $j = 2, \cdots, n$

$$\begin{aligned} \hat{e}(\sigma_j, P) &= \hat{e}\left(PID_1^j, P_{pub1}\right) \cdot \hat{e}\left(h^j \cdot H^j, P_{pub2}\right) \\ &\text{where } h^j = h(m, PID_2^j), H^j = H(PID_1^j, PID_2^j) \end{aligned} \tag{5.12}$$

we will have

$$\begin{aligned} \hat{e}\left(\sigma - \sum_{j=2}^{n} \sigma_j, P\right) &= \hat{e}\left(PID_1^1, P_{pub1}\right) \cdot \hat{e}\left(h^1 \cdot H^1, P_{pub2}\right) \\ &\text{where } h^1 = h(m, PID_2^1), H^1 = H(PID_1^1, PID_2^1) \end{aligned} \tag{5.13}$$

which however contradicts with the assumption that Bilinear Pairing Inverse (BPI) Problem "*Given* $P \in \mathbb{G}_1, \hat{e}(Q, P) \in \mathbb{G}_2$*, compute* $Q \in \mathbb{G}_1$ " is hard [73]. Therefore, we can conclude that the aggregated warning message is secure against the forgery attack.

5.5.2 Efficiency Analysis

We analyze the reduction of bandwidth consumption due to the proposed scheme based on aggregated signature compared with other schemes based on the regular public key digital signature and BLS non-identity-based aggregation [58].

The total execute time for verifying a warning message is composed of three aspects of cryptographic operations, including the time for pairing computation from $\mathbb{G}_1 \times \mathbb{G}_1$ to $\mathbb{G}_2$, the time for map-to-point hash operation, and the time for point multiplication in $\mathbb{G}_1$, which is shown in Table 5.1.

The total execute time for verifying the proposed aggregated signature is

Table 5.1: Time costs of dominant cryptographic operations

Operation	Description	Time
T_{pair}	Time for one pairing computation from $\mathbb{G}_1 \times \mathbb{G}_1$ to $\mathbb{G}_2$	15.73 ms
T_{mtp}	Time for one map-to-point hash operation	0.15 ms
T_{pmul}	Time for one point multiplication in $\mathbb{G}_1$	2.34 ms

$$\begin{aligned} T_{\mathsf{ver}} &= 3T_{\mathsf{pair}} + n \cdot (T_{\mathsf{mtp}} + T_{\mathsf{pmul}}) \\ &= 47.19 + n \cdot 2.49 \text{ ms} \end{aligned} \tag{5.14}$$

Further, if without aggregation, the total execute time for verifying a warning message is

$$\begin{aligned} T_{\mathsf{ver}} &= n \cdot (3T_{\mathsf{pair}} + T_{\mathsf{mtp}} + T_{\mathsf{pmul}}) \\ &= n \cdot 49.68 \text{ ms} \end{aligned} \tag{5.15}$$

Also, the total execute time for verifying a warning message with BLS non-identity-based aggregation is

$$\begin{aligned} T_{\mathsf{ver}} &= (n+1) \cdot T_{\mathsf{pair}} + n \cdot T_{\mathsf{mtp}} \\ &= 15.73 + n \cdot 15.88 \text{ ms} \end{aligned} \tag{5.16}$$

Obviously, the total execute time for verifying a warning message with the proposed scheme is the shortest one among the aforementioned schemes, particularly, as n becomes larger.

5.5.3 Accident Reduction Analysis

We consider an abnormal area with n accident scenes. For simplicity, we assume that it is possible that every vehicle attempts to enter the wrong way with probability of p_1 even there is an **tRSU** on the road, and then try to merge back to the main stream carelessly with probability of p_2, which results in an incident. Further, we denote the accuracy of the movement prediction as p_3. Hence, we have the probability $p_{accident}$ of having car accident without wrong-way warning

$$p_{accident} = 1 - (1 - p_1 p_2)^n \tag{5.17}$$

And, the probability $p^{'}_{accident}$ of having car accident with wrong-way warning

$$p^{'}_{accident} = 1 - (1 - p_1 p_2 (1 - p_3))^n \tag{5.18}$$

In an effort to evaluate the accident reduction under the proposed wrong-way warning scheme, the accuracy rate of the direction prediction of a vehicle's movement plays an important role. Hence, the primary issue is to calculate the accuracy rate of the direction prediction of a vehicle's movement. Since the scenario of driving at an intersection is much more complicated than the scenario of driving along the road, without loss of generality, we take the first one as a test environment. Specifically, the physical location, 398 Westmount Rd. N, Waterloo, Ontario, Canada, is taken as our test intersection, which is shown in Fig. 5.6 [60]. Eight hundred samples are collected, and each sample is a five-dimensional vector, where each element of the vector is the same as presented before. In our data set, Direction is towards the west, and Speed records the instant velocity of a vehicle. In addition, the Addition field provides the information about traffic light, red, yellow, green, and left-arrow green. Since it is forbidden for a vehicle to U-turn at that intersection, the desired output of a vehicle's movement is turning left, turning right, and going ahead.

A three-layer perceptron is employed, and the number of neurons of the input layer is equal to five, where each presents a feature. The number of neurons of the hidden

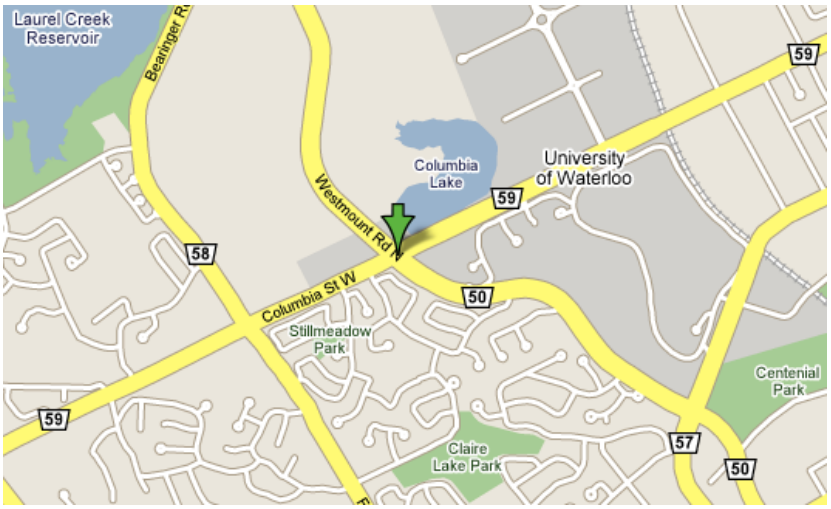


Figure 5.6: The intersection of the data collection

layer is equal to ten, and the number of neurons of the output layer is equal to three, where the biggest associated output on the neuron denotes the responding decision. The data set is divided into two parts, a training set with 600 samples and a testing set with 200 samples.

Table 5.2: The performance of movement prediction

	Turn left	Turn right	Go ahead	Total
Total number	71	65	64	200
Accurate number	68	64	64	196
Accurate rate	95.7	98.4	100	98.0

Table 5.2 presents the accuracy of the prediction. There are a total of 200 samples for testing. 71 out of 200 vehicles turned left at the intersection, and 68 samples are classified correctly; 65 out of 200 vehicles turned right at the intersection, and

64 samples are classified correctly; 64 out of 200 vehicles went straight ahead at the intersection, and 64 is classified correctly. Thus the total accuracy rate is 98.0%. The key reason why the wrong prediction occurs is traffic violations. For example, some vehicles do not show their left-turn (right-turn) light when they turn left (right), or even indicate the wrong turn light.

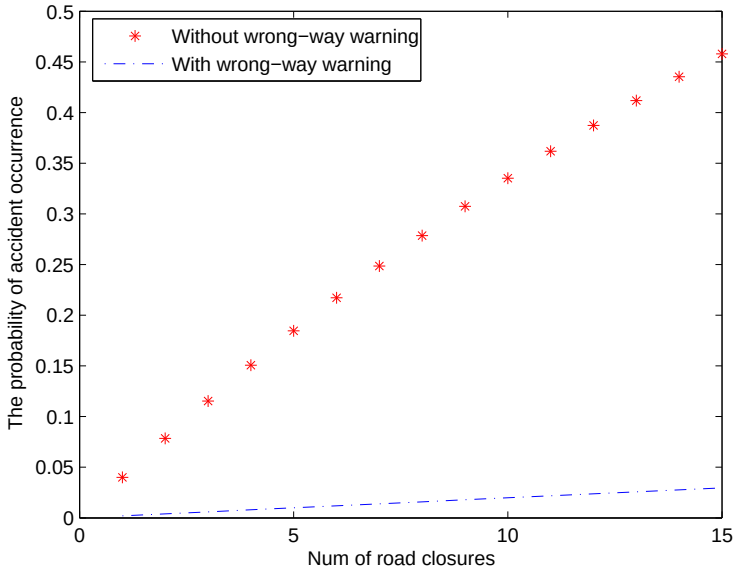


Figure 5.7: Accident reduction due to wrong-way warning

Fig. 5.7 shows the probability of accident occurrence with respect to the number of road closures in an abnormal area under both situations where or not wrong-way warning system exists. It can be seen that a car accident may likely happen when a wrong-way warning system does not exist. Further, the probability of accident occurrence in an abnormal area increases with the increase of road closures, but more serious in the case where a wrong-way warning system is not present. It is also observed that the accuracy of the prediction has big impact on the probability of accident occurrence as well, which is shown in Fig. 5.8. The more accurate the movement prediction is, the

safer an abnormal area can be.

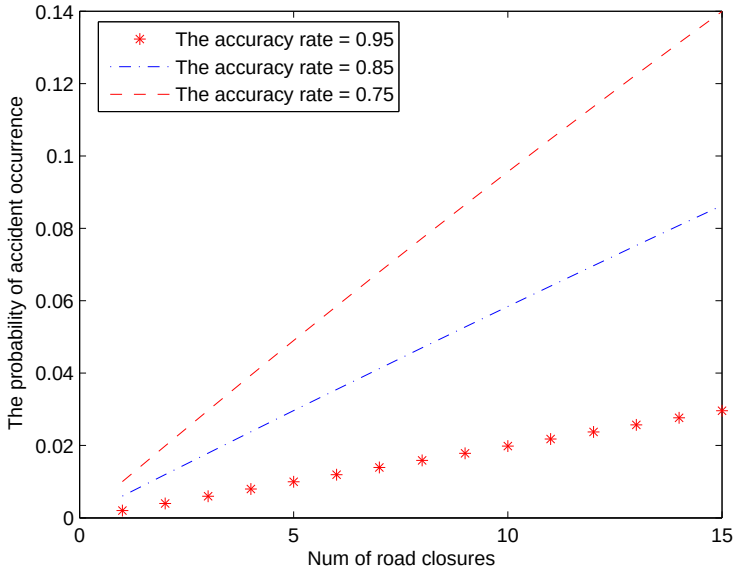


Figure 5.8: Accident reduction with different accuracy of movement prediction

5.6 Summary

In this chapter, we have proposed a novel secure road traffic control system based on VANETs along with a suite of strategies for mitigating the vicious effects due to the malicious attackers. To achieve the proposed application scenario, a new implementation of temporary RSU, termed **tRSU**, was introduced, which is automatically formed by those vehicles involved in an abnormal situation, such as a car accident, in order to serve as temporary RSU that can improve the safety at the scene of the accident. In addition, the proposed system can achieve an intelligent transportation flow control by helping vehicles to circumvent the areas with abnormal situations while ensuring the security and privacy of the users from various threats. Analysis results showed

that the proposed system can improve the road safety in an abnormal situation significantly when road authority is absent at the scene, which can be considered as the most dangerous moment for the driving public.

Chapter 6

Secure VANET-based Toll Collection System

6.1 Introduction

Road system is the most important factor in determining economic performance. In recent years, in order to promote and sustain continued economic growth, we have witnessed dramatic road infrastructure development all over the world. It not only promotes a sustainable and continued economic growth but also provides the drivers with values in terms of time savings, convenience, better-maintained roads and traveler services. However, road construction, maintenance and operation are very expensive. Nowadays, many public roadways are seriously underfunded and badly maintained, which will also adversely affect economy. This results that government not only increases the tax to cover the shortage of the funding, but also starts transferring the development, operation and maintenance of roads to the private sector, which results toll road, also known as *pay-as-you-go toll road*. It introduces the whole economic with toll road. One of the main challenges facing toll road is toll collection. At present, there are mainly two types of toll collection methods. The first one is manual toll

collection, where the driver has to stop at a toll booth and pays the toll fee in cash or with credit card. This would cause the delay on toll roads. Obviously, the delay incurred in toll collection becomes very annoying to drivers, which obviously violates the original premise for improving both customer satisfaction and efficiency of traffic flow. Thus, a lot of toll roads began electronic tolling-only, i.e., *Electronic Toll Collection* (ETC). ETC takes advantage of wireless communication technologies to perform an electronic monetary transaction between the cars passing through a toll station and the toll agency. It determines whether the cars passing are enrolled in the program, and alerts enforcers for those that are not. It debits electronically the accounts of registered cars without their stopping, or even opening a window. When a registered vehicle passes through the toll booths, its tag, also known as transponder, is automatically detected and the appropriate fee is deducted from the driver's account. The transponder is a small electronic device fitted on the inside of the vehicle windscreen which is read either by roadside sensors located in entry and exit lanes. Vehicle without the transponder, will be taken image of its license plate, and recognized through *license plate recognition* (LPR) system. Then, the charges will be applied to the owner of that license registered with the authority, such as *Ministry of Transportation* (MTO). Then tolls are calculated based on the factors like time of the day, vehicle class, distance traveled, etc. afterwards, a bill is mailed to customer for usage.

Despite the pluses of currently existing ETC technology, it has some downfalls and suffers from some drawbacks concerning cost, fraud, and privacy, which are shown as follows:

- Firstly, besides toll road usage, drivers have to pay either monthly transponder lease fees or video toll charges. In reality, the toll charges are one-third more for drivers who do not have a transponder to offset the costs caused by video toll charges. It is highly like that a toll road operator tries to minimize transponder lease fees in order to encourage drivers to choose the toll road. However, there

could be many toll road operators in an area or country. It is impractical and inconvenient for a driver to register with several toll road operators and mount more than one transponders in his/her car. High cost prevents drivers from choosing toll road, and then flashes the red light to the construction of toll road.

- Secondly, it is vulnerable to fraud by drivers. In reality, it is very easy for a malicious driver to counterfeit his license plate to avoid tolls, such as fake license plate. Further, it is also subject to some advanced threats, such as by of way of using a license plate cover that can prevent high angle mounted toll road cameras from getting a clear shot of a license plate, which results in the failure of *license plate recognition* (LPR) system. However, it is usually too late when toll road operators discover fraud.

- Thirdly, there is an increasing demand on driver privacy and anonymity. The driver's personal information and his driving history need to be well protected.

Thus, having a secure and effective toll fare collection system is more than critical to its overall success of a toll road system. In this chapter, we aim to introduce a novel efficient and secure payment system for road toll collection based on VANETs. By designing a tollgate specifically for electronic toll collection, it is possible to carry out open-road tolling, where the driver does not need to slow at all when passing through the tollgate. Further, the driver privacy and anonymity are protected, and traceability is provided where a particular transaction can be traced back to a driver only when it is necessary. For example, the authorities should be able to reveal the identity of a driver involved in a particular transaction in the case of a traffic event dispute such as a crime/car accident scene investigation, which can be used to look for witnesses. For example, by using entry and exit a driver used and date, the authorities can figure who has possibly passed a crime/car accident scene.

The remainder of the chapter is organized as follows. In Section 6.2, preliminaries

are presented. In Section 6.3, a secure VANET-based toll collection system is introduced. Section 6.4 discusses the security of the proposed system. Finally, we summarize this chapter in Section 6.5.

6.2 Preliminaries

6.2.1 Elliptic Curve Cryptosystem

The *elliptic curve cryptosystems* (ECCs) were first introduced by Miller [63] and Koblitz [17]. Since then, many researcher have examined elliptic curves cryptosystems due to their high bit security. The elliptic curve cryptosystems which are based on the elliptic curve logarithm over the finite field have many advantages over other convenient cryptosystems [35, 36]. First, the key size in ECCs can be much smaller over the other cryptosystems. Second, even if the factoring and multiplicative group discrete logarithm are broken, the elliptic curve discrete logarithms might be still intractable. Therefore, we will design our system based on the elliptic curve cryptosystems.

Let p be a large prime. In the finite field $\mathbb{Z}_p$, an elliptic curve is represented as

$$\mathbf{E} : y^2 = x^3 + ax + b \tag{6.1}$$

where $a, b \in \mathbb{Z}_p$ and $4a^3 + 27b^2 \neq 0 \bmod p$. The elliptic curve indicates the integer points set that contains all points over the elliptic curve and a point of infinity $\mathbb{O}$. The point of infinity $\mathbb{O}$ is the third points of intersection of any straight line with the curve, so that there are points including (x, y), $(x, -y)$, and $\mathbb{O}$ on the straight line. The necessity of $4a^3 + 27b^2 \neq 0 \bmod p$ is to guarantee that the curve $y^2 = x^3 + ax + b \bmod p$ will not cause repeated factors. The set $\mathbf{E}_p(a, b)$ defines a finite Abelian group, then the calculation in the finite Abelian group can be precisely executed because the occurrence of round off error in cryptographic application is disallowed.

The set of elliptic curve points forms a commutative finite group under the rules

of addition operation, the infinity $\mathbb{O}$ serves as the additive identity, and the following relations hold for all $P, Q, R \in \mathbf{E}_p(a, b)$:

1. $P + \mathbb{O} = \mathbb{O} + P = P$ (existence of an identity element)
2. $P + Q = Q + P$ (commutativity)
3. $(P + Q) + R = P + (Q + R)$ (associativity)
4. there exists $(-P)$ such that $-P + P = P + (-P) = \mathbb{O}$ (existence of inverses)

For any two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ over $\mathbf{E}_p(a, b)$, the elliptic curve addition operation, which is denoted as $P + Q = (x_R, y_R)$, satisfies the following rules.

$$\begin{cases} x_R = \lambda^2 - x_P - x_Q \\ y_R = \lambda(x_P - x_R) - y_P \end{cases} \tag{6.2}$$

where

$$\begin{cases} \lambda = \dfrac{y_Q - y_P}{x_Q - x_P} \text{ if } P \neq Q \\ \lambda = \dfrac{3x_P^2 + a}{2y_P} \text{ if } P = Q \end{cases} \tag{6.3}$$

We refer to [17, 63] for a more comprehensive description of how ECCs work.

6.2.2 Blind Signature

The concept of blind signature was first introduced by Chaum [74, 75]. Different from the normal digital signature schemes, in a blind signature scheme, a signer signs a message without knowing what the message contains. That is, the message is blinded by a requester. After receiving the signed message from the signer, the requester can derive the valid signature of the message from the signer. Anyone can verify the blind signature using the public key of the signer. If the message and its signature are published, the signer can verify the signature, but he/she cannot link the message-signature pair. Due

to these two properties: blindness and untraceability, blind signatures are widely used used to realize a lot of cryptographic protocols such as secure voting protocol and electronic payment systems

6.2.3 Micro-Payment

A micro-payment scheme is an electronic payment system designed to allow efficient frequent payments of small amounts (e.g., less than one dollar or a few cents). In order to be efficient and keep the transaction cost very low, micro-payments minimize the communication and computation used. In contrast to macro-payment, micro- payment schemes aim to allow offline payment verification using lightweight cryptosystems. The systems do not require high transaction security, in order to increase efficiency. The cost of fraud is made more expensive than the possible value to be gained by cheating.

A micro-payment system is generally composed of three entities, i.e., customer, vender, and broker. Customers open an account with a broker. The broker issues a digitally signed certificate, which authorizes the customer to make PayWord chain and assures vendors that the customer's PayWords are redeemable. The PayWords employs the cryptographic properties of digital signature and hash chain. Customer creates the PayWord chain $w_1, w_2, \cdots, w_n$ in reverse order by picking the last Payword w_n at random, and then computing $w_{i-1} = h(w_i)$, where h is a collision-resistant hash function, and $i = 1, \cdots, n$. Here w_0 is the root of the PayWord chain, and is not a PayWord itself. The commitment of the PayWord chain contains the root w_0, but not any PayWord w_i, where $i \geq 1$. The i-th payment (for $i = 1, 2, \cdots$) from the client to the vendor consists of the pair (w_i, i), which the vender can verify by checking the commitment and $w_0 = h^i(w_i)$.

We refer to [76] for a more comprehensive description of Micro-Payment.

6.2.4 Security Requirements

In this subsection, we discuss the properties of an e-Toll payment system. In order to solve the above mentioned issues, an e-Toll system has to meet the following requirements:

- Correctness: If an honest driver runs e-Toll purchase protocol with the bank and runs any of the Toll payment protocol with the RSUs, the RSUs will accept the e-Toll.
- Unforgeability: E-Toll is unforgeable. Only the bank can issue the valid e-Toll, anyone else can't.
- Separability: The separability would be feasible and perhaps desirable in the case of e-Toll. An e-Toll can be divided into several mini-E-Tolls, and the total amount of these mini-E-Tolls equals to the original E-Toll.
- Double-spent proof: An e-Toll is not allowed to be double-spent. Once the double-spent occurs, it can be detected.
- Conditional anonymity: In the normal cases, the e-Toll spending doesn't leak the driver's identity, and the driver is kept anonymity. However, if the driver double-spent the e-Toll, then with the help of trusted third party, the driver's identity can be revealed.

6.3 Secure VANET-based Toll Collection System

In this section, we introduce a novel secure VANET-based toll collection system. For ease of reference, we first list the notations used throughout the description of the proposed system as follows:

Notations	Descriptions
$\mathcal{B}$	Bank who issues the e-toll
$\mathcal{D}$	Driver who purchases the e-toll and participate in the toll payment protocol
$\mathcal{T}_1$, $\mathcal{T}_2$	Trusted third party, $\mathcal{T}_1$ the register manager, $\mathcal{T}_2$ the transaction manager
$\mathcal{P}_1$, $\mathcal{P}_2$, $\cdots$, $\mathcal{P}_{n_p}$	n_p toll road operators
RSU_{ij}, $1 \leq j \leq n_r$	n_r RSUs of the i^{th} toll road operator $\mathcal{P}_i$

6.3.1 System Architecture and Setup

For the considered system architecture, there are four types of network entities: the drivers, the *trusted third parties* (TTPs), the Bank, and the toll road operators, while their relationship is shown in Fig. 6.1. The Bank has a mutual agreement with each toll road operator such that a bank-issued e-Toll can be used to pay the toll when a driver drives the toll roads operated by those operators. A driver has to purchase e-Toll from the Bank in order to travel the toll roads run by an operator, or may otherwise be charged the cost for license plate recognition or toll-road violation processing. At entries and exits of the toll roads, which are toll collection points in the proposed system, e-Tolls are collected and then accumulated into a batch and settled automatically at regular time intervals, e.g., at the end of each day, with the Bank. This settlement can be viewed as a transaction between the Bank and the toll road operators. When a batch is submitted, the Bank transfers the corresponding amounts to the operator's bank account. Similar to credit card transaction processing, by dealing with a batch of clearance requests at a time, the Bank can be relieved from involving every transaction.

Let p be a large prime, (eg. $p > 3$). Randomly choose two field elements $a, b \in \mathbb{F}_p$

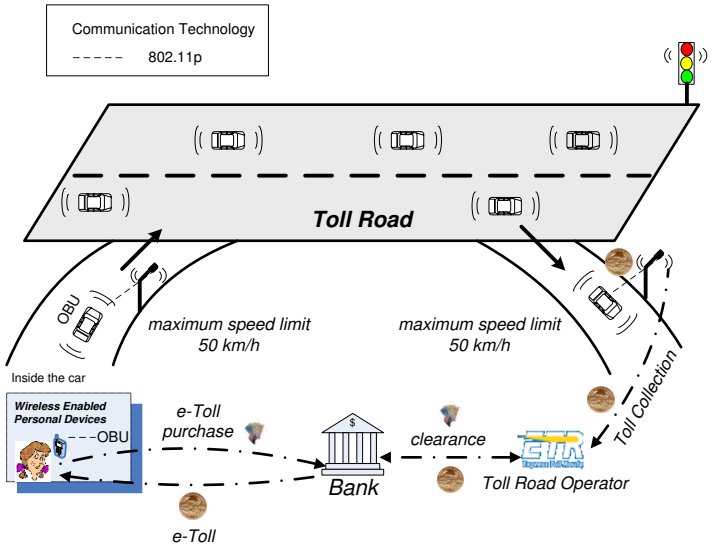


Figure 6.1: VANET-based toll collection system architecture

and define the elliptic curve equation

$$\mathbf{E} : y^2 = x^3 + ax + b \pmod{p}$$

over $\mathbb{F}_p$, where $4a^3 + 27b^2 \neq 0 \pmod{p}$. The cardinality of $\mathbf{E}$ should be divisible by a large prime number with regard to the security issue raised by Pohlig and Hellman [68].

Let $P = (x_P, y_P)$ be a generator point over $\mathbf{E}(\mathbb{F}_p)$ whose order is a large prime number q, where $P \neq \mathbb{O}$, and $\mathbb{O}$ denotes the point at infinity. In the end, the system parameters $\{\mathbf{E}(\mathbb{F}_p), P, q\}$ are made public. The system parameters, in addition, also include four cryptographic hash functions: H_0, H_1, H_2 and H, where $H_i : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, for $i \in \{0,1,2\}$ and $H : \{0,1\}^* \rightarrow \mathbf{E}(\mathbb{F}_p)$ [45].

The Bank $\mathcal{B}$ chooses a random number $x_B \in \mathbb{Z}_q^*$ as his private key, and computes the corresponding public key $Y_B \in \mathbf{E}(\mathbb{F}_p)$, where $Y_B = x_B P$. A driver $\mathcal{D}$ can purchase e-Toll from the Bank $\mathcal{B}$.

There are two trusted third parties $\mathcal{T}_1$, $\mathcal{T}_2$ in the proposed system. One of the TTPs, for example $\mathcal{T}_1$, is the register manager, and the other one, $\mathcal{T}_2$, can be the transaction

manager. A specific e-Toll can be traced to a specific e-Toll purchase transaction only with approval and involvement of two TTPs, which results in the discovery of the real identity of the driver. Each trusted third party $\mathcal{T}_i$, $i \in \{1, 2\}$, chooses a random number $x_{Ti} \in \mathbb{Z}_q^*$ as his private key, and computes his individual public keys $Y_{Ti} \in \mathbf{E}(\mathbb{F}_p)$, where $Y_{Ti} = x_{Ti}P$.

Without loss of generality, suppose that there are total n_p toll road operators $\mathcal{P}_1, \cdots \mathcal{P}_{n_p}$ in the system. Each operator $\mathcal{P}_i$, for $i = 1, \cdots, n_p$ chooses a random number $x_i \in \mathbb{Z}_q^*$ as his private key, and computes the corresponding public key $Y_i \in \mathbf{E}(\mathbb{F}_p)$, where $Y_i = x_iP$. Further, we assume that each toll road operator $\mathcal{P}_i$, for $i = 1, \cdots, n_p$ administrates n_r RSUs (denoted as RSU_{ij}, where $1 \leq j \leq n_r$) to toll. Then, for each RSU RSU_{ij}, the toll road manager $\mathcal{P}_i$ generates RSU_{ij}'s location-aware key pair as follows.

- RSU_{ij} first chooses a random number $x_{ij} \in \mathbb{Z}_q^*$, computes $R_{L_{ij}} = x_{ij}P$, and sends $(L_{ij}, R_{L_{ij}})$ to the toll road operator $\mathcal{P}_i$, where L_{ij} is the location of the RSU RSU_{ij}.

- Upon receiving $(L_{ij}, R_{L_{ij}})$, $\mathcal{P}_i$ chooses a random number $r_{ij} \in \mathbb{Z}_q^*$, computes $R_{ij} = r_{ij}P$, $d_{ij} = r_{ij} + x_i \cdot H_0(L_{ij}||R_{L_{ij}}||R_{ij}) \bmod q$. In the end, $\mathcal{P}_i$ sends the location-aware key $LSK_{ij} = (R_{ij}, d_{ij})$ to RSU_{ij}.

- RSU_{ij} checks its validity by $d_{ij}P \stackrel{?}{=} R_{ij} + H_0(L_{ij}||R_{L_{ij}}||R_{ij})Y_i$. Then, RSU_{ij} computes the private key $s_{ij} = x_{ij} + d_{ij} \bmod q$ such that $s_{ij}P = R_{L_{ij}} + R_{ij} + H_0(L_{ij}||R_{L_{ij}}||R_{ij})Y_i$.

6.3.2 E-Toll Purchase Protocol

When a driver $\mathcal{D}$ wants to purchase e-Toll, the following steps will be executed, which is shown in Fig. 6.2.

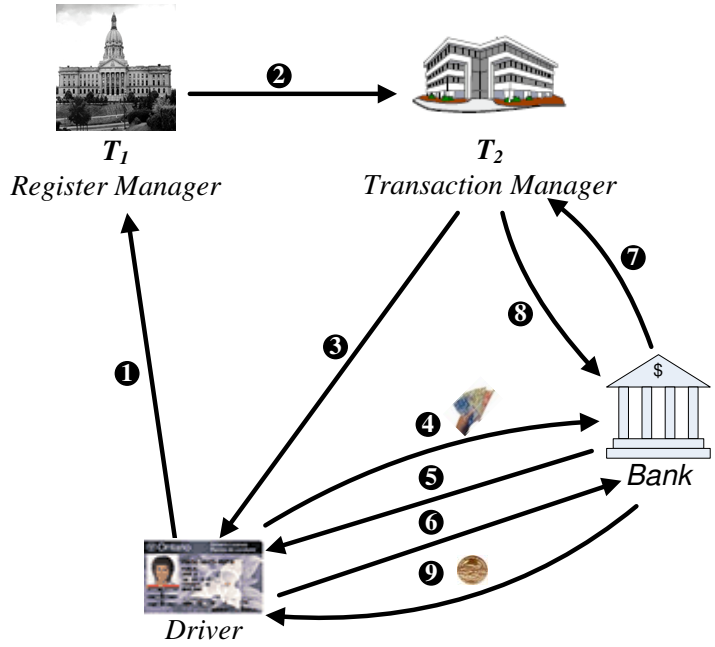


Figure 6.2: E-Toll purchase

Step 1. The driver $\mathcal{D}$ randomly chooses a random numbers $r \in \mathbb{Z}_q^*$, and computes $C, R \in \mathbf{E}(\mathbb{F}_p)$

$$\begin{cases} C = ID + r \cdot Y_{T1}, \\ R = rP \end{cases} \tag{6.4}$$

where $ID \in \mathbf{E}(\mathbb{F}_p)$ is the driver's legal identity. The driver $\mathcal{D}$ then submits (C, R) to the register manager $\mathcal{T}_1$.

Step 2. After receiving (C, R), the register manager $\mathcal{T}_1$ first uses his private key x_{T1} to recover the driver's identity as

$$ID = C - x_{T1} \cdot R \tag{6.5}$$

then authenticates the validity of ID. If ID is invalid, $\mathcal{T}_1$ refuses the driver's request. Otherwise, $\mathcal{T}_1$ chooses a unique randomized identity RID, stores (ID, RID) into his local database, and forwards (RID, R) to the transaction manager $\mathcal{T}_2$.

Step 3. When the transaction manager $\mathcal{T}_2$ receives (RID, R), he chooses two random numbers $\alpha, \beta \in \mathbb{Z}_q^*$, and computes R_1, R_2, c, z, where

$$\begin{cases} R_1 = \alpha P, R_2 = \beta R = \beta r P \\ c = H_0(R_1, R), \\ z = \alpha - c \cdot x_{T2} \bmod q \end{cases} \tag{6.6}$$

$\mathcal{T}_2$ then sends (R_2, c, z) back to the driver $\mathcal{D}$, and stores $(RID, \beta P, c)$ into his local database. Here, c in an unique identifer of this protocol instance such that

$$H_0(R_3, R) = c, \text{ where } R_3 = zP + cY_{T2} \tag{6.7}$$

The correction is as follows,

$$\begin{aligned} & H_0(R_3, R) \\ = \; & H_0(zP + cY_{T2}, R) \\ = \; & H_0((\alpha - c \cdot x_{T2})P + cY_{T2}, R) \\ = \; & H_0\left(\alpha P - c \cdot x_{T2} P + cY_{T2}, R\right) \\ = \; & H_0\left(\alpha P, R\right) = H_0\left(R_1, R\right) = c \end{aligned} \tag{6.8}$$

Step 4. When the driver $\mathcal{D}$ receives (R_2, c, z), he uses r to recover βP as follows,

$$r^{-1} R_2 = r^{-1} \beta r P = \beta P \tag{6.9}$$

In such a way, only the driver $\mathcal{D}$ knows the secret information βP with the transaction manager $\mathcal{T}_2$.

Assume the value for toll unit is v\$ and the driver $\mathcal{D}$ wants to purchase the e-Toll 100\$. He first generates a hash chain $h_0, h_1, \cdots, h_n$ initiated from a random s, where $h_n = s$, $h_{i-1} = h(h_i), 1 \leq i \leq n$, and $n = \frac{100}{v}$.

The driver notifies the bank $\mathcal{B}$ and submits the message (R, c, z) and payment 100\$ to the bank $\mathcal{B}$.

Step 5. When the bank $\mathcal{B}$ receives (R, c, z) and 100\$, he first uses the trusted third party $\mathcal{T}_2$'s public key Y_{T2} to verify the validity of (R, c, z) by checking

$$H_0(zP + cY_{T2}, R) = c$$

If it is not valid, the bank $\mathcal{B}$ refuses this request. Otherwise, he chooses a random number $k \in \mathbb{Z}_q^*$, computes and returns

$$K = kP \in \mathbf{E}(\mathbb{F}_p) \tag{6.10}$$

to the driver $\mathcal{D}$.

Step 6. When the driver $\mathcal{D}$ receives K, he first computes c_0, c_1, c_2, where

$$c_i = H_i(\beta P), \text{ where } i = 0, 1, 2 \tag{6.11}$$

and $ch = h_0 \cdot H_0(c_1, c_2) \bmod q$, $M = H(100\$, h_0, c_0) \in \mathbf{E}(\mathbb{F}_p)$. Then, he computes σ_1 and m', where

$$\begin{cases} \sigma_1 = M + c_1 P + c_2 K \in \mathbf{E}(\mathbb{F}_p) \\ m' = c_2^{-1} \cdot H_0(\sigma_1) \pmod q \end{cases} \tag{6.12}$$

The driver $\mathcal{D}$ also chooses a random number $u \in \mathbb{Z}_q^*$, and computes U, θ, where

$$\begin{cases} U = uP \in \mathbf{E}(\mathbb{F}_p) \\ \theta = u - rH_0(R, U, m') \pmod q \end{cases} \tag{6.13}$$

In the end, $\mathcal{D}$ sends (ch, m', U, θ) to the bank $\mathcal{B}$.

Step 7. Upon receiving (ch, m', U, θ), the bank $\mathcal{B}$ can use $R = rP$ that is authenticated in *Step 5* to verify the validity of (m', U, θ) by the following equation,

$$\theta P = U - H_0(R, U, m')R \tag{6.14}$$

The correction is as follows,

$$\begin{aligned} & \theta P \\ = \ & (u - rH_0(R, U, m'))P \\ = \ & uP - rH_0(R, U, m')P \\ = \ & U - H_0(R, U, m')R \end{aligned} \tag{6.15}$$

Once (m', U, θ) is valid, the bank $\mathcal{B}$ sends $(c, ch, K, 100\$)$ to the trusted third party $\mathcal{T}_2$.

Step 8. After receiving $(c, ch, K, 100\$)$, the trusted third party (transaction manager) $\mathcal{T}_2$ retrieves the stored $(RID, \beta P, c)$ through the identifier c, and computes $c_i = H_i(\beta P)$, where $i = 0, 1, 2$. Then, $\mathcal{T}_2$ computes h_0, M, σ_1, m^*, where

$$\begin{cases} h_0 = ch/H_0(c_1, c_2) \bmod q \\ M = H(100\$, h_0, c_0) \in \mathbf{E}(\mathbb{F}_p) \\ \sigma_1 = M + c_1 P + c_2 K \in \mathbf{E}(\mathbb{F}_p) \\ m^* = c_2^{-1} \cdot H_0(\sigma_1) \pmod q \end{cases} \tag{6.16}$$

In the end, m^* is returned back to the bank $\mathcal{B}$, and $\mathcal{T}_2$ updates $(RID, h_0, c, c_0, 100\$)$ in his database.

Step 9. After the bank $\mathcal{B}$ receives m^*, he checks whether $m' = m^*$ or not. If yes, the bank $\mathcal{B}$ can believe that the driver $\mathcal{D}$ honestly purchases the e-Toll 100\$, and therefore computes

$$\sigma_2' = m' \cdot x_B + k \pmod q \tag{6.17}$$

and sends σ_2' back to the driver $\mathcal{D}$. Otherwise, the bank $\mathcal{B}$ thinks that the driver $\mathcal{D}$ is dishonest and terminates transaction.

Step 10. After receiving σ_2', the driver $\mathcal{D}$ computes

$$\sigma_2 = \sigma_2' \cdot c_2 + c_1 \pmod q \tag{6.18}$$

and checks if

$$\begin{aligned} & -\sigma_2 P + H_0(\sigma_1) Y_B + \sigma_1 \\ = \; & -(m' x_B c_2 + k c_2 + c_1) P + H_0(\sigma_1) Y_B + \sigma_1 \\ = \; & -m' x_B c_2 P - k c_2 P - c_1 P + H_0(\sigma_1) Y_B + \sigma_1 \\ = \; & -m' c_2 Y_B - c_2 K - c_1 P + H_0(\sigma_1) Y_B + \sigma_1 \\ = \; & -H_0(\sigma_1) Y_B - c_2 K - c_1 P + H_0(\sigma_1) Y_B + M + c_1 P + c_2 K \\ = \; & M \end{aligned} \tag{6.19}$$

If it is valid, the blind signature on e-Toll 100$ is $(\sigma_1, \sigma_2, c_0)$. Then, anyone can check its validity by the following equation

$$-\sigma_2 P + H_0(\sigma_1)Y_B + \sigma_1 = H(100\$, h_0, c_0) \tag{6.20}$$

In such a way, the driver $\mathcal{D}$ finishes purchasing e-Toll $(100\$, \sigma_1, \sigma_2, c_0)$ as well as a secret payment chain $(h_0, \cdots, h_n)$.

6.3.3 Toll Payment Protocol

In this subsection, toll payment protocol is described. The payment is carried out in two stages. First as a driver enters the toll road, the driver is recorded the entry automatically by RSU issuing an e-Ticket to the driver, where RSU is operated by the toll road operator and located along entry lanes. In the second one, the driver takes an exit and leaves the toll road. Then the driver submits the e-Ticket to the RSU, which is located along exit lanes. The RSU then calculates the toll based on some factors, such as, distance traveled, data in the car-identification chips including vehicle weight and class, and prompts the driver to pay the right amount of toll. Finally, the driver pays the toll by submitting the appropriate amount of e-Toll, and the RSU issues a signed e-Receipt to the driver.

There are three entities involved in this protocol: the driver, RSU located at toll road entry location, namely *entrance RSU*, and RSU located at toll road exit location, namely *payment RSU*. The proposed e-Toll payment protocol are shown in Fig. 6.3, and the basic steps of the protocol are further described in the following paragraphs.

E-Ticket issuing protocol. We first introduce E-Ticket issuing protocol when a driver enters the toll road from the entry where *entrance RSU* RSU_{ij} is located, shown in Fig. 6.4.

Step 1. When a driver drives a car and is entering a toll road, the driver sends an e-Ticket request message to the *entrance RSU* RSU_{ij}, which contains a random number n, the location of the vehicle L_D, and a timestamp T.

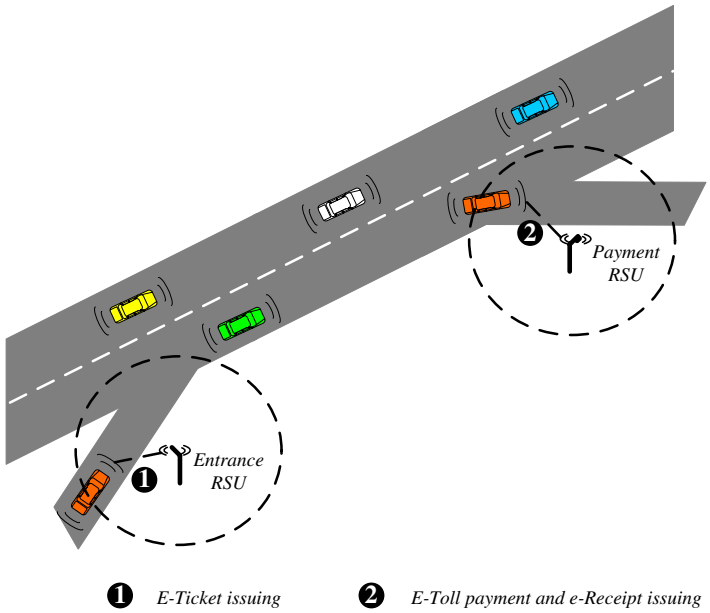


Figure 6.3: E-Toll payment

Step 2. After receiving the e-Ticket request, the *entrance RSU* RSU_{ij} under the location L_{ij} chooses a random number $r \in \mathbb{Z}_q^*$, computes $R = rP$ and $\beta = H_0(L_{ij}||R_{Lij}||R_{ij}||R||m)$, where $m = n||T||L_{ij}$. Then, the RSU_{ij} sets the signature $(R_{Lij}, R_{ij}, R, \sigma)$, where $\sigma = r + s_{ij}\beta \bmod q$. Then, the RSU_{ij} sends $(R_{Lij}, R_{ij}, R, \sigma)$ to the driver $\mathcal{D}$ as well as L_{ij}.

Step 3. The driver $\mathcal{D}$, upon receipt of $(R_{Lij}, R_{ij}, R, \sigma, L_{ij})$, then verifies the signature $(R_{Lij}, R_{ij}, R, \sigma)$ on message m with respect to the location L_{ij}, the following equation will be checked.

$$\sigma P \stackrel{?}{=} R + \beta(R_{Lij} + R_{ij} + H_0(L_{ij}||R_{Lij}||R_{ij})Y_i) \tag{6.21}$$

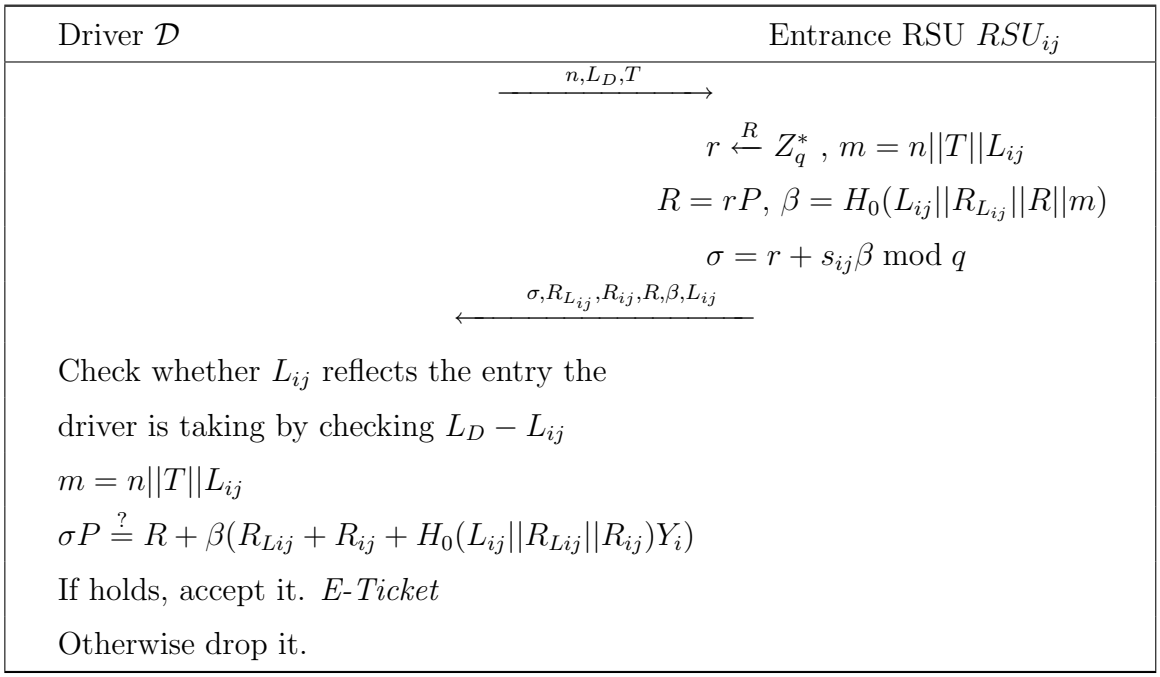


Figure 6.4: E-Ticket issuing protocol

If it holds, the e-Ticket $(R_{Lij}, R_{ij}, R, \sigma)$ can be accepted, otherwise rejected, since

$$\begin{aligned} & R + \beta(R_{Lij} + R_{ij} + H_0(L_{ij}||R_{Lij}||R_{ij})Y_i) \\ = \; & rP + \beta(x_{ij}P + r_{ij}P + H_0(L_{ij}||R_{Lij}||R_{ij})x_iP) \\ = \; & rP + \beta(x_{ij} + r_{ij} + H_0(L_{ij}||R_{Lij}||R_{ij})x_i)P \\ = \; & rP + \beta(x_{ij} + d_{ij})P \\ = \; & rP + \beta s_{ij}P = \sigma P \end{aligned} \tag{6.22}$$

E-Toll payment protocol. We next introduce E-toll payment protocol when the driver leaves the toll road from the road exit location where payment RSU $RSU_{ij'}$ is located, shown Fig. 6.5.

Step 1. The driver first submits the *e-Ticket* to the RSU located along exit lanes.

Step 2. After receiving the *e-Ticket*, the payment RSU checks the *e-Ticket* and calculates the toll based on some factors, such as, distance traveled, data in the car-

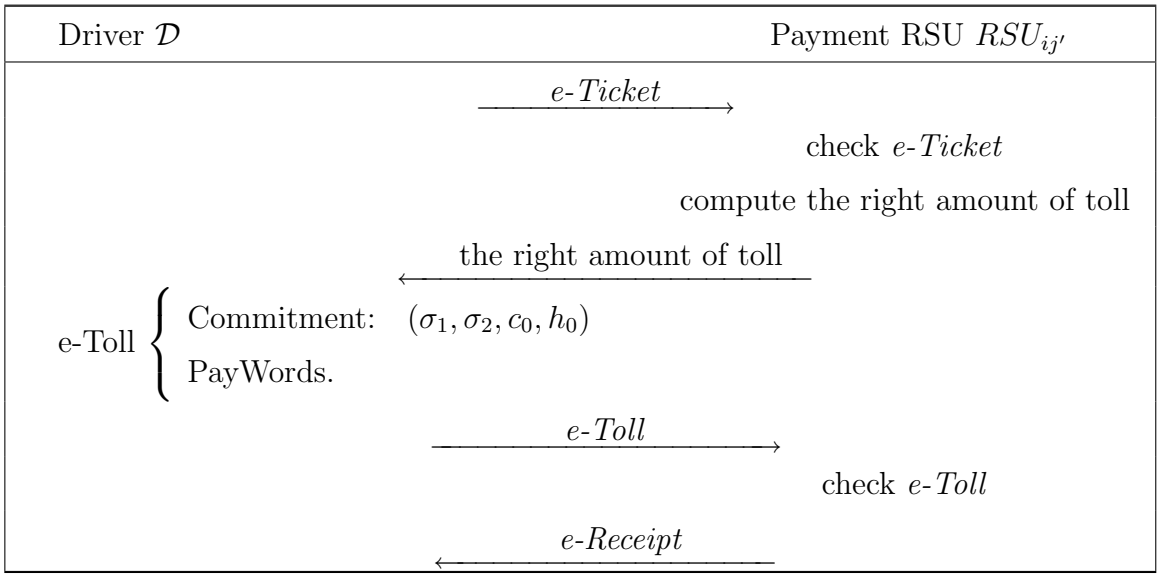


Figure 6.5: E-Toll payment protocol

identification chips including vehicle weight and class, prompts the driver to pay the right amount of toll.

Step 3. The driver pays the toll by submitting the appropriate amount of e-Toll by commitment $(\sigma_1, \sigma_2, c_0, h_0)$ and PayWords.

Step 4. The payment RSU issues a signed *e-Receipt* on e-Toll to the driver.

Note. To securely issue the *e-Receipt*, we employ the certificateless signature technique as that in *e-Ticket* issuing protocol. Certificateless signature technique is intended to solve the key escrow problem which is inherent in identity-based cryptography, while at the same time, eliminate the use of certificates as in the Public Key Infrastructure (PKI), which is generally considered to be costly to use and manage. Therefore, the toll road operator doesn't need to assign each subordinated RSU a public key and its certificate, and the verifier also doesn't need to explicitly authenticate the RSU's public key firstly, but directly authenticate the validity of the signature (*e-Ticket* and *e-Receipt*) with respect to the operator's public key and the RSU's location.

6.3.4 Traceability Protocol for Double Spending

An e-toll is not allowed to be double-spent. Once the bank $\mathcal{B}$ found one e-Toll is double-spent, he can ask the trusted third party $\mathcal{T}_1$ and $\mathcal{T}_2$ to track the driver's real identity by Algorithm 3.

Data: A disputed e-Toll $(\sigma_1, \sigma_2, c_0)$ on 100\$

Result: Driver's real identity ID of this disputed e-Toll

1 **begin**

2 ▷ Transaction Manager $\mathcal{T}_2$: retrieve $(RID, h_1, c, c_0, 100\$)$ in his local database with search identifier c_0, send the resulted RID to $\mathcal{T}_1$.

3 ▷ Register Manager $\mathcal{T}_1$: retrieve (ID, RID) in his local database with search identifier RID.

4 **return** ID

5 **end**

Algorithm 3: TraceRealIdentity()

6.4 Security Analysis

In this section, we examine the correctness and security of our proposed protocol, eg. unforgeability and unlinkability. We also show how to cope with the possible abuse of the unlinkability property under the assistance of the trusted third party.

6.4.1 Correctness

To ensure the correctness, we should first prevent the driver $\mathcal{D}$ from deviating from the right protocol to elude traceability of the trusted third party. In our protocol, to request a valid blind signature of the bank $\mathcal{B}$ on an e-Toll M on 100\$, the driver $\mathcal{D}$ should not

only submit the blinded message m' to the bank, but also send 100$ to the transaction manager $\mathcal{T}_2$ by the bank $\mathcal{B}$'s forwarding. The transaction manager $\mathcal{T}_2$ himself computes the blinded message m^* according to the previous registration information and then send m^* to the bank. By comparing the blinded messages m' and m^*, the bank $\mathcal{B}$ can judge whether the driver $\mathcal{D}$ is honest or not, although he doesn't know the real identity of the driver $\mathcal{D}$.

The second correctness we should consider is to prevent the bank $\mathcal{B}$ from sending an invalid signature to the driver $\mathcal{D}$. Therefore, when the driver $\mathcal{D}$ receives σ_2' from the bank $\mathcal{B}$, he should first compute $\sigma_2 = \sigma_2' \cdot c_2 + c_1 \pmod{q}$, and use the bank's public key Y_B to check the correction by equation

$$-\sigma_2 P + H_0(\sigma_1) Y_B + \sigma_1 = M \tag{6.23}$$

Thus, according to the above two aspects, the correctness of our proposed protocol is ensured.

6.4.2 Unforgeability

The unforgeability of the proposed system is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP) "*Given* (P, aP)*, to compute such an* $a \in \mathbb{Z}_q^*$". In the following, the security of all signatures involved in our proposed system are analyzed.

The trusted third party $\mathcal{T}_2$'s signature (c, z) on $r_1 P$ is unforgeable

In the random oracle model [59], we can prove the signature (c, z) is secure against existential forgery under an adaptively chosen message attack. Suppose that there is a polynomial time adversary $\mathcal{A}$ which takes $R = rP$ and Y_{T2} as input, and outputs an existential forgery of a signature from the trusted third party with a non-negligible probability. Then, by the forking lemma [69], $\mathcal{A}$ may get two forgeries of signature

from the trusted third party $\mathcal{T}_2$ for the same R within a polynomial time. Let the two signature forgeries for R be (c, z) and (c', z'), where

$$\begin{cases} c = H_0(R_1, R), c' = H_0'(R_1, R) \\ z = \alpha - c \cdot x_{T2} \pmod{q} \\ z' = \alpha - c' \cdot x_{T2} \pmod{q} \end{cases} \tag{6.24}$$

Since $c \neq c'$, it follows that

$$z - z' = c'x_{T2} - cx_{T2} \pmod{q} \tag{6.25}$$

and we will have

$$x_{T2} = \frac{z - z'}{c' - c} \pmod{q} \tag{6.26}$$

The above equation means we can get x_{T2} from $Y_T = x_{T2}P$. But it will contradict with the ECDLP assumption. Therefore, the trusted third party $\mathcal{T}_2$'s signature (c, z) on $R = rP$ is unforgeable.

The driver's signature (U, θ) on m' is unforgeable

Since $R = rP$ has been signed by the trusted third party $\mathcal{T}_2$, $R = rP$ can be regarded as the driver's temporary public key delegated by the trusted third party $\mathcal{T}_2$. Thus, in the random oracle model, the driver's signature (U, θ) on m' with respect to the public key $R = rP$ is also secure against existential forgery under an adaptively chosen message attack.

We still suppose that there is a polynomial time adversary $\mathcal{A}$ which takes m' and $R = rP$ as input, and outputs an existential forgery of a signature from the driver with a non-negligible probability. Then, by the forking lemma, $\mathcal{A}$ may get two forgeries of signature from the driver for the same m' within a polynomial time. Let the two signature forgeries for m' be $(U = uP, \theta)$ and $(U = uP, \theta')$, where

$$\begin{cases} \theta = & u - rH_0(R, U, m') \pmod q \\ \theta' = & u - rH_0'(R, U, m') \pmod q \end{cases} \tag{6.27}$$

Since $H_0(R, U, m') \neq H_0'(R, U, m')$, it follows that

$$\theta - \theta' = r(H_0'(R, U, m') - H_0(R, U, m')) \pmod q \tag{6.28}$$

and thus we will have

$$r = \frac{\theta - \theta'}{H_0'(R, U, m') - H_0(R, U, m')} \pmod q \tag{6.29}$$

It also means we can get r from $R = rP$. But it will contradict with the ECDLP assumption. Therefore, the driver's signature (U, θ) on m' is unforgeable.

The bank's blind signature $(\sigma_1, \sigma_2, c_0)$ on M is unforgeable

Clearly, the signature $(\sigma_1, \sigma_2, c_0)$ on M is the Nyberg-Rueppel signature [67]. Assume that an adversary $\mathcal{A}$ wants to forge a signature on a valid message $M = H(100\$, h_1, c_0)$, he can first chooses σ_1, then according to the relation

$$-\sigma_2 P + H_2(\sigma_1)Y_B + \sigma_1 = M \tag{6.30}$$

he should compute $\sigma_2 \in \mathbb{Z}_q^*$. However, it is infeasible for him to compute σ_2 due to the hardness of ECDLP problem. With the similar reason, $\mathcal{A}$ also can't compute σ_1, if σ_2 is first chosen. Therefore, based on these two points, the bank's blind signature $(\sigma_1, \sigma_2, c_0)$ on M is unforgeable.

The RSU's e-Ticket is unforgeable

The RSU's e-Ticket is of form $(R_{Lij}, R_{ij}, R, \sigma)$, it is also provably secure against the adaptively chosen message attacks in the random oracle model. Suppose that there is a polynomial time adversary $\mathcal{A}$ can existentially forge the signature (e-Ticket). Then, by the forking lemma, $\mathcal{A}$ can get two forgeries for the same m within a polynomial

time in the random oracle model. Let the two signature (e-Ticket) forgeries for m be $(R_{Lij}, R_{ij}, R, \sigma)$ and $(R_{Lij}, R_{ij}, R, \sigma')$, where

$$\begin{cases} \beta = & H_0(L_{ij}||R_{Lij}||R_{ij}||R||m) \\ \beta' = & H_0'(L_{ij}||R_{Lij}||R_{ij}||R||m) \\ \sigma = & r + s_{ij}\beta \pmod q \\ \sigma' = & r + s_{ij}\beta' \pmod q \end{cases} \tag{6.31}$$

Since $\beta \neq \beta'$, it follows that

$$\sigma - \sigma' = s_{ij}\beta - s_{ij}\beta' \pmod q \tag{6.32}$$

and we will have

$$s_{ij} = \frac{\sigma - \sigma}{\beta - \beta'} \pmod q \tag{6.33}$$

The above equation shows we can get s_{ij} such that

$$s_{ij}P = (R_{Lij} + R_{ij} + H_0(L_{ij}||R_{Lij}||R_{ij})Y_i) \tag{6.34}$$

But it will contradict with the ECDLP assumption. We note that although the toll road operator $\mathcal{P}_i$ knows d_{ij}, he still can't know s_{ij}, since $s_{ij} = x_{ij} + d_{ij} \bmod q$ includes the RSU's partial private key x_{ij}. Therefore, based on these analysis, the e-Ticket is valid and unforgeable.

The RSU's e-Receipt is unforgeable

Since the RSU's e-Receipt adopts the same signature used in e-Ticket, we can conclude that the e-Receipt is also unforgeable.

6.4.3 Unlinkability

In *Step 6*, since (c_1, c_2) are two random numbers in $\mathbb{Z}_q^*$, $\sigma_1 = M + c_1P + c_2K$ is then a random element in $\mathbf{E}(\mathbb{F}_p)$. In sequence,

$$m' = c_2^{-1} \cdot H_0(\sigma_1) = c_2^{-1} \cdot H_0(M + c_1P + c_2K) \tag{6.35}$$

is also a random number in $\mathbb{Z}_q^*$. Therefore, although the bank $\mathcal{B}$ receives the blinded message m', the m' will not leak any information about the real message M.

Given a valid signature $(\sigma_1, \sigma_2, c_0)$ and any view (m', K) of the bank, there always exists a unique pair blinding factors (c_1, c_2) such that

$$m' = c_2^{-1} \cdot H_2(-\sigma_2 P + H_2(\sigma_1)Y_B + \sigma_1 + c_1P + c_2K) \tag{6.36}$$

Therefore, due to the randomness of the blinding factors (c_1, c_2), the bank cannot link a signature $(\sigma_1, \sigma_2, c_0)$ to the corresponding instance of signature issuing protocol. Therefore, our proposed protocol satisfies the unlinkability.

6.4.4 Traceability with the Aid of Trusted Third Party

In our proposed protocol, to cope with the possible abuse of the unlinkability property, the trusted third party $\mathcal{T}_1$ and $\mathcal{T}_2$ will have enough information to trace the real identity ID from the abuse signature $(\sigma_1, \sigma_2, c_0)$, because they have stored the entry (ID, RID), $(RID, c, c_0, 100\$)$ in their respective database, and can cooperatively trace the real identity ID by running Algorithm 3. Therefore, with the aid of the trusted third party, the traceability property holds.

6.5 Summary

In this chapter, we have proposed a novel secure VANET-based toll collection system, which facilitates quick and reliable toll payment when a driver uses toll road. It not

only solves existing issues in the current toll collection systems, but also protects toll road users' privacy while ensuring the security of toll payment.

Chapter 7

Conclusions and Future Work

In this chapter, the contributions of this dissertation are concluded, followed by the future work.

7.1 Contributions

The major contributions of this thesis are mainly in two folds: Firstly, a Secure and Efficient RSU-aided Privacy Preservation Protocol is introduced, which can achieve efficient secure and privacy-preserving Inter-Vehicle Communications (IVC). With the key chain commitments distributed by RSUs, a vehicle can effectively authenticate any received message from vehicles nearby even in the presence of frequent group membership fluctuation. Compared with previously reported public key infrastructure (PKI)-based packet authentication protocols for security and privacy [19, 21], the communication overhead and computation cost of the proposed protocol are significantly reduced due to the adoption of a short message authentication code (MAC) tag attached in each packet for the packet source authentication and packet integrity check. Extensive performance evaluation demonstrates that the proposed protocol maintains acceptable packet latency with much less packet overhead, while significantly reducing the packet

loss ratio compared with that of the existing PKI-based protocols. Such advantages are particularly important and effective when the road traffic is heavy. Further, a complementary Efficient and Cooperative Message Validation Protocol, called ECMVP, is developed to deal with the situations where RSUs do not exist.

Secondly, two vehicle applications are proposed. The first one is a vehicle safety application, namely secure road traffic control system in VANET, to deal with the situations where instantaneous, temporary, and ad hoc traffic management efforts are required. This is to assist road traffic control by directing vehicular and pedestrian traffic around an accident scene or other road disruption areas. The thesis provides solutions on how to rapidly and accurately disseminate road conditions information to the public through the state-of-the-art VANET technologies, particularly by way of collaborative efforts among those drivers within the affected geographic area. The proposed VANET-based road traffic control system can help move vehicles safely and securely through the areas subject to abnormal situations while ensuring security and privacy of the users from various threats. The second one is a vehicle non-safety application, namely secure VANET-based toll collection system, to effectively and securely collect toll when drivers use toll roads.

7.2 Future Work

As for future research plans, the highest priority is to push the developed framework and schemes into industrious practice. To achieve this, we will work closely with automobile industry and apply findings from my research to building vehicle safety and non-safety applications in real world situations. Furthermore, the following research topics will be investigated as a continuation of my Ph.D. thesis work.

7.2.1 Secure and Efficient Certificate Revocation

In the traditional PKI architecture, the most commonly adopted certificate revocation scheme is through CRL, which is a list of revoked certificates stored in central repositories prepared in CAs. Based on such centralized architecture, alternative solutions to CRL could be by way of *Certificate Revocation System* (CRS), *Certificate Revocation Tree* (CRT), and *Online Certificate Status Protocol* (OCSP) [18], etc. The common requirement for these schemes is the high availability of the centralized CAs, where frequent data transmission with the OBUs for obtaining timely revocation information may cause significant overhead. Thus, with the high-speed mobility and extremely large amount of network entities in VANETs, the centralized CRL architecture may be far from realistic.

To tackle the problem, Raya *et al.* [19] proposed three certificate revocation protocols for VANETs, namely *Revocation using Compressed Certificate Revocation Lists* (RC2RL), *Revocation of the Tamper-Proof Device* (RTPD), and *Distributed Revocation Protocol* (DRP). RC2RL uses a compression technique to reduce the overhead of the distribution of the CRL. Instead of checking the status of a certificate, RTPD removes revoked certificates from their corresponding vehicles' certificate stores by introducing a tamper-proof device as a vehicle key and certificate management tool. In this case, the vehicle possessing the revoked certificates is informed of the certification revocation incident, by which the tamper-proof device automatically removes those revoked certificates. Different from RC2RL and RTPD, a distributed certificate revocation mechanism is implemented in DRP to determine the status of a certificate. In DRP, each vehicle is equipped with an attacker detection system, which enables a vehicle to identify any compromised peer. When a compromised or malicious vehicle is detected and located, its neighbors can work together to temporally revoke the compromised one. However, the aforementioned methods are still far from efficient and practical. we plan to design a suitable and efficient certificate revocation scheme for VANETs.

7.2.2 VANET-based Intelligent Traffic Flow Control

In the modern transportation systems, traffic lights take an important role in automatically performing traffic control and management in urban areas, which not only enhance the driver safety but also facilitate smooth multiplexing at the intersections, instead of purely relying on human manipulation and policeman on-line monitoring. In reality, traffic in a city is very much affected by the controller installed in each traffic light. Much attention has been put to make traffic light controllers more intelligent, by which an adaptive and context-aware traffic light control system can be achieved even if with the growing number of road drivers and the limited transportation resources. The intelligent control on the traffic lights will make the travelling time of the drivers in a metropolitan area reduced, which could save billions of dollars for our society. Obviously, collecting traffic information plays an important role in traffic flow control. Currently, this has been done by equipping the traffic lights with sensing devices such as pressure sensors for measuring inductance of inductive loops buried in the pavement. However, deploying sensors in the pavement at an intersection could be very expensive and difficult to maintain. In addition, the sensors can become inaccurate and fail to function regularly as time goes by. It is highly desired to have a reliable and cost effective approach to collect traffic information in an intelligent traffic light controlling system. Motivated by the observation, it is planned as a future research effort to design a VANET-based traffic flow information collection system for intelligent traffic flow control.

In the long term, we will continue studying cryptography and privacy enhancing technologies, which serve as basis for various privacy-preserving security systems in my current research. In addition, we are interested in studying security and privacy issues with healthcare information technology. Recently, more healthcare providers are tied to information highway to allow patient data more easily shared. However, with more strict regulations, such as HIPAA, ensuring personal privacy with respect to medical

records and healthcare-related information has become an urgent need. In our future work, we plan to develop novel protocols, algorithms, and techniques to meet security objectives, such as confidentiality, integrity and privacy, of key identified problems while allowing patient information to be easily shared in the healthcare system.

Bibliography

[1] State Traffic Safety Information For Year 2006, National Highway Traffic Safety Administration [Online]. Available:http://www.nhtsa.dot.gov/stsi/State_Info.cfm?Year=2003&State=CO&Accessible=0

[2] Increased Driving Safety Through Auto Accident Avoidance Technologies, Ford Motor Company. [Online]. Available:http://www.ford.com/innovation/car-safety/helping-avoid-accidents/accident-avoidance-technologies/avoid-accidents-349p

[3] Dedicated Short Range Communications (DSRC) Protocol. [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

[4] U.S. Department of Transportation, National highway traffic safety administration, *vehicle safety communications project - final report*, Apr. 2006. [Online]. Available: http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm

[5] IEEE Std 1609.2-2006. IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages, 2006.

[6] Traffic light. [Online] Available: http://en.wikipedia.org/wiki/Traffic_light

[7] C. Liu and J. T. Yu, "An analysis of DoS attacks on wireless LAN," *Proc.* 6^{th} *IASTED International Multi-Conference on Wireless and Optical Communications*, Banff, Alberta, Canada, July 2006.

[8] I. Aad, J.P. Hubaux, and E. Knightly, "Denial of service resilience in ad hoc networks," *in Proc. ACM MobiCom*, Philadelphia, PA, USA, Sep. 2004.

[9] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDoS-resilient scheduling to counter application layer attacks under imperfect detection," *in Proc. IEEE INFOCOM 2006*, Barcelona, Spain, pp. 1-13. Apr. 2006.

[10] J. V. E. Molsa, "Increasing the DoS attack resiliency in military ad hoc networks," in *Proc. IEEE MILCOM 2005*, Vol. 4, pp. 2282-2288, Atlantic City, New Jersey, USA, Oct. 2005.

[11] J. V. E. Molsa, "Cross-layer designs for mitigating range attacks in ad hoc networks", *in Proc.* 24^{th} *IASTED international conference on Parallel and distributed computing and networks*, pp. 64-69, Innsbruck, Austria, Feb. 2006.

[12] CAR 2 CAR Communication Consortium. [Online]. Available:http://www.car-to-car.org/index.php?id=130

[13] Secure Vehicular Communication (SeVeCom) project. [Online]. Available:http://www.sevecom.org/

[14] eSafety. [Online]. Available:http://ec.europa.eu/information_society/activities/esafety/index_en.htm

[15] Information Society and Media Directorate-General. [Online]. Available:http://ec.europa.eu/dgs/information_society/index_en.htm

[16] Sixth Framework Programme of the European Commission. [Online]. Available:http://cordis.europa.eu/fp6/dc/index.cfm?fuseaction=UserSite.FP6HomePage

[17] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.

[18] P. Wohlmacher, "Digital certificates: A survey of revocation methods," *Proc. ACM Wksp. Multimedia*, Los Angeles, CA, USA, Oct. 2000, pp. 111-114.

[19] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, Vol. 15, No. 1, pp. 39-68, 2007.

[20] M. Raya and J. Hubaux, "A security of vehicular ad hoc networks," *in Proc. the 3rd ACM workshop on Security of ad hoc and sensor networks SASN '05*, November 2005.

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

[22] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," *in Proc. INFOCOM '08*, Phoenix, Arizona, USA, Apr. 2008.

[23] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," *in Proc. Embedded Security in Cars (ESCAR)*, Cologne, Germany, Nov. 2005.

[24] J. Freudiger, M. Raya, M. Flegyhzi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," *in Proc. the First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 2007)*, Vancouver, British Columbia, Canada, Aug. 2007,.

[25] S. Ur Rahman, and U. Hengartner, "Secure Crash Reporting in Vehicular Ad hoc Networks," *in Proc. the third International Conference on Security and Privacy in Communication Networks (SecureComm 2007)*, Nice, France, Sep. 2007.

[26] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," *in Proc. INFOCOMM '99*, Vol. 2, pp. 708-716, Mar. 1999.

[27] F. Bergadano, D. Cavagnino, and B. Crispo, "Chained stream authentication," *in Proc. the 7th Annual Workshop on Selected Areas in Cryptography*, LNCS, Vol. 2012, Springer-Verlag, pp. 144-157, Waterloo, Ontario, Canada, Aug. 2000.

[28] B. Briscoe, "FLAMeS: fast, loss-tolerant authentication of multicast streams," *Technical report, BT Research*, 2000.

[29] A. Perrig, R. Canneti, D. Song, and J.D. Tygar, "The TESLA broadcast authentication protocol," *RSA Cryptobytes*, Vol. 5, No. 2, pp. 2-13, 2002.

[30] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

[31] R. Rivest and A. Shamir, "PayWord and MicroMint: two simple micropayment schemes," *in Proc. SPW '96*, LNCS, Vol. 1189, Springer-Verlag, pp. 69-87, Berlin, 1996.

[32] Q. Huang, I. Avramopoulos, B. Liu, and H. Kobayashi, "Secure data forwarding in wireless ad hoc networks," *in Proc. IEEE ICC '05*, Vol. 5, pp. 3525- 3531, Seoul, Korea, May 2005.

[33] P. Golle and N. Modadugu, "Authenticating streamed data in the presence of random packet loss," *in Proc. ISOC NDSS '01*, San Diego, California, pp. 13-22. USA, Feb. 2001.

[34] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *in Proc. Advances in Cryptology - Crypto '01*, LNCS, Vol. 2139. Springer-Verlag, pp. 213-229, 2001.

[35] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[36] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 469-472, 1985.

[37] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature: delegation of the power to sign messages," *IEICE Trans. Fundamentals*, Vol. E79-A, No. 9, pp. 1338-1353, 1996.

[38] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," *in Proc. 3rd ACM Conference on Computer and Communications Security - CCS '96*, ACM Press, pp. 48-57, 1996.

[39] B. Lee, H. Kim, and K. Kim, "Strong proxy signgture and its applications," *in Proc. SCIS '01*, pp. 603-608, 2001.

[40] B. Lee, H. Kim, and K. Kim, "An analysis of proxy signatures: is a secure channel necessary?," *in Proc. Topics in Cryptology - CT-RSA '03*, LNCS, Vol. 2612, Springer-Verlag, pp. 68-79, 2003.

[41] R. Lu, Z. Cao, X. Dong, "Efficient ID-based one-time proxy signature and its application in e-cheque," *in Proc. 5th International Conference on Cryptology and Network Security - CANS '06*, LNCS, Vol. 4301, Springer-Verlag, pp. 153-167, Suzhou, China, 2006.

[42] R. Lu and Z. Cao, "Designated verifier proxy signature scheme with message recovery," *Applied Mathematics and Computation*, Vol. 169, No. 2, pp. 1237-1246, 2005.

[43] Q. Xue and Z. Cao, "Factoring based proxy signature schemes," *Journal of Computational and Applied Mathematics*, Vol. 195, No. 1-2, pp. 229-241, Oct. 2006.

[44] C. L. Robinson, D. Caveney, L. Caminiti, G. Baliga, K. Laberteaux and P. R. Kumar, "Efficient message composition and coding for cooperative vehicular safety applications", *IEEE Trans. on Vehicular Technology*, Vol. 56, No. 6, pp. 3244-3255, 2007.

[45] B. Schneier, *Applied Cryptography* (2nd), John Wiley: New York, 1996.

[46] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," *in Proc. of Asiacrypt*'05, Taj Coromandel, Chennai, India, Dec. 2005.

[47] M. Reiter, "A security architecture for faulttolerant systems," PhD thesis, Department of Computer Science, Cornell University, Aug. 1993.

[48] M. Reiter, K. Birman, and R. van Renesse, "A security architecture for fault-tolerant systems," *ACM Transactions on Computer Systems*, Vol. 12, No. 4, pp. 340-371, Nov. 1994.

[49] V. Roca, A. Francillon, S. Faurite, "The use of TESLA in the ALC and NORM protocols. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-for-alc-norm-02.txt

[50] The Network Simulator - ns-2. [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/User_Information

[51] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). [Online]. Available: http://indigo.ie/ mscott/

[52] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," *ACM Wireless Networks*, Vol. 13, No. 5, pp. 569-582, 2007.

[53] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," *in Proc. the IEEE International Conference on Computer Communications (INFOCOM'08)*, Phoenix, Arizona, 2008.

[54] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, Vol. 25, No. 8, pp. 1557-1568, 2007.

[55] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," *in Proc. the International workshop on Vehicular ad hoc networks (VANET'04)*, pp. 29-37, 2004.

[56] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications - assumptions, requirements, and principles," *in Proc. Workshop on Embedded Security in Cars (escar'06)*, 2006.

[57] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *in Proc. Advances in Crytology - Crypto'04*, LNCS, vol. 3152. Springer-Verlag, pp. 41-55, 2004.

[58] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *in Proc. Advances in Cryptology - Asiacrypto '01*, LNCS, Vol. 2248. Springer-Verlag, pp. 514-532, 2001.

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

[60] Google Map. [Online]. Available: http://maps.google.ca/

[61] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 49-55, 2004.

[62] A. K. Jain, J. Mao, and K. M. Mohiuddin, "Artificial neural networks: a tutorial," *Jounal of IEEE Computer*, Vol. 29, No. 3, pp. 31-44, 1996.

[63] V. S. Miller, "Use of elliptic curves in cryptography", *in Advances in Cryptography - CRYPTO '85*, LNCS, Vol. 218, Springer-Verlag, pp. 417-426, 1986.

[64] 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. 1234-1243, 2001.

[65] M. Minsky and S. Papert, "Perceptrons: an introduction to computational geometry," MIT Press, Cambridge, Mass, 1969.

[66] T. Nakanishi and N. Funabiki, "A short verifier-local revocation group signature scheme with backward unlinkability," *in Proc. IWSEC '06*, LNCS, vol. 4266. Springer-Verlag, pp. 17-32, 2006.

[67] K. Nyberg and R. Rueppel, A new signature scheme based on the DSA giving message recovery, *in Proc. ACM Conference on Computer and Communications Security*, pp. 58-61, 1993.

[68] J. Pollard and M. Hellman, "An improved algorithm for computing logarithms over $GF(P)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, Vol. IT-24, No. 1, pp. 106-110, 1978.

[69] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptography*, Vol. 13, No. 3, pp. 361-396, 2000.

[70] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "Spins: security protocols for sensor networks," *Wireless Networks*, Vol. 8, No. 11, pp. 521-534, 2002.

[71] A.K. Saha, D. B. Johnson, "Modeling mobility for vehicular ad hoc networks", *in Proc.* 1^{st} *International Workshop on Vehicular Ad Hoc Networks*, pp. 91-92, Philadelphia, PA, USA, Oct. 2004.

[72] P. Wohlmacher, "Digital certificates: a survey of revocation methods," *in Proc. the ACM workshops on Multimedia*, Los Angeles, CA, USA, Oct. 2000.

[73] Y. Yacobi, "A note on the bilinear Diffie-Hellman assumption," Cryptology ePrint Archive: Report, 2002.

[74] D. Chaum, "Blind signatures for untraceable payments," *in Proc. Advances in Cryptology - Crypto'82*, Santa Barbara, California, USA, pp. 199-203, Aug. 1982.

[75] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, Vol. 28, No. 10, pp. 1030-1044, 1985.

[76] R. Rivest and A. Shamir, "PayWord and MicroMint: two simple micropayment schemes," *In Proc. of International Workshop on Security Protocols*, LNCS, Vol. 1189, Springer-Verlag, pp. 69-87, Berlin, 1996.

Author's Publications

[1] X. Lin, X. Sun, P.-H. 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, Nov. 2007.

[2] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: timed efficient and secure vehicular communications with privacy preserving," *IEEE Transactions on Wireless Communications*, to appear.

[3] X. Lin, R. Lu, P.-H. Ho, X. Shen, and Z. Cao, "TUA: a novel compromise-resilient authentication architecture for wireless mesh networks," *IEEE Transactions on Wireless Communications*, Vol. 7, No. 4, pp. 1389-1399, 2008.

[4] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 88-95, 2008.

[5] X. Lin, X. Ling, H. Zhu, P.-H. Ho, and X. Shen, "A novel localised authentication scheme in IEEE 802.11 based wireless mesh networks," *International Journal of Security and Networks*, Vol. 3, No. 2, pp. 122-132, 2008.

[6] X. Lin, R. Lu, H. Zhu, P.-H. Ho, and X. Shen, "Provably secure self-certified partially blind signature scheme from bilinear pairings," *in Proc. IEEE International Conference on Communications (ICC'08)*, Beijing, China, May 2008.

[7] X. Lin, C. Zhang, X. Sun, P.-H. Ho, and X. Shen, "Performance enhancement for secure vehicular communications," *in Proc. IEEE Global Communications Conference (GLOBECOM'07)*, Washington, DC, USA, Nov. 2007.

[8] X. Lin, P.-H. Ho, and X. Shen, "Towards compromise-resilient localized authentication architecture for wireless mesh networks," *in Proc. Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine 2007)*, Vancouver, British Columbia, Aug. 2007.

[9] X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, "ASRPAKE: an anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," *in Proc. IEEE International Conference on Communications (ICC'07)*, Glasgow, UK, June 2007. **(Best Paper Award)**

[10] X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "Two-factor localized authentication scheme for WLAN roaming," *in Proc. IEEE International Conference on Communications (ICC'07)*, Glasgow, UK, June 2007.

[11] X. Lin, R. Lu, P.-H. Ho, X. Shen, and Z. Cao, "A novel compromise-resilient authentication system for wireless mesh networks," *in Proc. IEEE Wireless Communications and Networking Conference (WCNC'07)*, Hong Kong, Mar. 2007.

[12] X. Lin, H. Zhu, B. Lin, P.-H. Ho, and X. Shen, "A novel voting mechanism for compromised node revocation in wireless ad hoc networks," *in Proc. IEEE Global Communications Conference (GLOBECOM'06)*, San Francisco, USA, Nov. 2006.

[13] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," *in Proc. the 27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, USA, Apr. 2008.

[14] C. Zhang, R. Lu, X. Lin,, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," *in Proc. the 27th IEEE International Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, USA, Apr. 2008.

[15] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: secure localized authentication and billing scheme for wireless mesh networks," *IEEE Transactions on Wireless Communications*, to appear.

[16] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Transactions on Vehicular Technology*, to appear.

[17] R. Lu, X. Lin, Z. Cao, J. Shao, and X. Liang, "New (t, n) threshold directed signature scheme with provable security," *Information Sciences*, Vol. 178, No. 3, pp.756-765, 2008.

[18] R. Lu, X. Lin, Z. Cao, L. Qin, and X. Liang, "A simple deniable authentication protocol based on the Diffie-Hellman algorithm," *International Journal of Computer Mathematics*, to appear.

[19] R. Lu, X. Lin, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "AICN: an efficient algorithm to identify compromised nodes in wireless sensor network," *in Proc. IEEE International Conference on Communications (ICC'08)*, Beijing, China, May 2008.

[20] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," *in Proc. IEEE International Conference on Communications (ICC'08)*, Beijing, China, May 2008.

[21] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "AEMA: an aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," *in Proc. IEEE International Conference on Communications (ICC'08)*, Beijing, China, May 2008.

[22] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, "A new dynamic group key management scheme with low rekeying cost," *in Proc. IEEE Wireless Communications and Networking Conference (WCNC'08)*, Las Vegas, Nevada, USA, Mar. 2008.

[23] R. Lu, X. Lin, H. Zhu, C. Zhang, P.-H. Ho, and X. Shen, "A novel fair incentive protocol for mobile ad hoc networks," *in Proc. IEEE Wireless Communications and Networking Conference (WCNC'08)*, Las Vegas, Nevada, USA, Mar. 2008.

[24] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "Secure localized authentication and billing for wireless mesh networks," *in Proc. IEEE Global Communications Conference (GLOBECOM'07)*, Washington, DC, USA, Nov. 2007.

[25] Z. Zhang, X. Lin, and P.-H. Ho, "Measuring intrusion impacts for rational response: a state-based approach," *in Proc. International Conference on Communications and Networking in China (Chinacom'07)*, Shanghai, China, Aug. 2007.

[26] C. Zhang, X. Lin, X. Sun, and P.-H. Ho, "A keyless facility access control system with wireless enabled personal devices," *in Proc. Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine 2007)*, Vancouver, British Columbia, Aug. 2007.

[27] C. Zhang, X. Lin, P.-H. Ho, X. Sun, and X. Zhan, "PPBR: privacy-aware position-based routing in mobile ad hoc networks," *in Proc. Military Communications Conference (Milcom'07)*, Orlando, Florida, Oct. 2007.

[28] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and ID-based signature scheme," *in Proc. IEEE International Conference on Communications (ICC'07)*, Glasgow, UK, June 2007.

[29] H. Zhu, X. Lin, P.-H. Ho, X. Shen, and M. Shi, "TTP based privacy preserving inter-WISP roaming architecture for wireless metropolitan area networks," *in Proc. IEEE Wireless Communications and Networking Conference (WCNC'07)*, Hong Kong, Mar. 2007.

[30] Z. Zhang, P.-H. Ho, X. Lin, H. Shen, "Janus: a two-sided analytical model for multi-stage coordinated attacks," *in Proc. the 9th Annual International Conference on Information Security and Cryptology (ICISC)*, Busan, Korea, Nov. 2006.