ANONYMOUS AUTHENTICATED ANNOUNCEMENT SCHEMES IN VEHICULAR AD HOC NETWORKS

Amizah Malip

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Information Security Group
Department of Mathematics
Royal Holloway, University of London

2014

Declaration

I, Amizah Malip, hereby declare that this thesis and the work presented in it is entirely my own. This doctoral study was conducted under the supervision of Dr. Siaw-Lynn Ng and Prof. Dr. Keith M. Martin. Parts of this thesis are based on the following papers:

- Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang. A Reputation-based Announcement Scheme for VANETs. *IEEE Transactions on Vehicular Technology,* 61(9): 4095-4108, 2012.
- A. Malip, S. Ng, and Q. Li. A Certificateless Anonymous Authenticated Announcement Scheme in Vehicular Ad Hoc Networks. In *Security and Communication Networks*, 7(3): 588-601, 2014.

The work presented in this thesis is the result of original research carried out by myself, in collaboration with others, whilst enrolled in the Information Security Group of Royal Holloway, University of London as a candidate for the degree of Doctor of Philosophy. This work has not been submitted for any other degree or award in any other university or educational establishment.

Amizah Malip
November 2014

Acknowledgements

My deepest thanks and gratitude to Dr. Siaw-Lynn Ng and Prof. Dr. Keith Martin, for their priceless supervision, support and patience; I have learned so much from you both. My heartfelt thanks to my family for their unconditional love. They are my constant source of inspiration and strength, I cannot thank them enough. Many thanks to all my friends in Royal Holloway for making my years through study a memorable one. In particular, Ciaran and Penying for always being there, and members of Mc Crea 355: Nadhem, Eduarda, Marcelo, Viet, Saif, Rostom, Alessio, and Rahman for the wonderful companionship; you all are the best. A special note goes to Jacques and Qin for helping with the programming and simulations, I have no idea how to start without you! I would also like to extend my gratitude to my Ph.D viva examiners: Prof. Dr. Nathan Clarke and Dr. Geraint Price for their time and effort reviewing the thesis. Last but not least, I thank University of Malaya and Ministry of Higher Education Malaysia for the generous fellowship to UK.

Abstract

This thesis adds to the design of new announcement schemes in vehicular ad hoc networks (VANETs). An announcement scheme allows vehicles to broadcast information about their surrounding to other vehicles in their proximity. This enables neighbouring vehicles to be aware of their driving environment and appropriate action can be taken upon receiving the messages. This may enhance road safety and traffic efficiency. Safety can only be achieved if the messages announced are reliable. A message announced is considered to be reliable if a receiver can be assured it was sent unmodified by a legitimate vehicle and the content of the message reflects the actual situation. Two common techniques to achieve this property is by using threshold method and reputation-based models. In a threshold method, a message is believed to be reliable if a vehicle receives messages of the same content announced by a number of distinct legitimate vehicles of a certain threshold within a time interval. In a reputation-based models, the reliability of a message is evaluated according to the reputation of the reporting vehicles; higher reputation reflects the likelihood a vehicle is announcing reliable messages. However, verification of reliability may violate privacy. Sensitive information such as its identity such be preserved and messages announced by a vehicle should be unlinkable. This is to prevent unlawful tracing and user profiling, as otherwise, it would be difficult to attract vehicles to join the network. The issues of security and privacy have been among the main concerns in the adoption of this technology. Such concerns are justified in the context of preserving and protecting user privacy whilst benefiting from the rich tools of vehicular communication systems. On the other hand, should misbehaviour arise, malicious vehicles should be traceable where it is identified to be held accountable and liable. It should also not be able to deny of having sent the message. This motivates the work described in this thesis.

We begin by defining the system and security model of an announcement scheme in VANETs. We analyse some related existing schemes in the literature which are based on (i) threshold mechanism and (ii) trust- and reputation-based models and examine

the extent to which they satisfy the contradictory requirement of reliability, privacy and accountability. Our analysis indicates that most schemes does not achieve message reliability and some schemes does not fulfil the requirement of accountability. In addition, most trust- and reputation-based schemes does not address the issue of privacy. This highlights the need to design a more efficient reliable privacy-preserving announcement schemes. Observation and comparison of different mechanisms used in some existing announcement schemes leads to our construction of a generic abstraction of an authenticated anonymous announcement scheme designed using threshold method. We also formulate a generic abstraction for an authenticated anonymous announcement scheme designed using reputation systems based on our proposed schemes. Within these abstractions, we give construction to three announcement schemes. The first scheme uses public key cryptography and reputation systems. We constructed another two schemes using certificateless signature. These schemes consider the challenging conflicting security requirements which we shall show has been achieved simultaneously in this thesis. We analyse the security of our proposed schemes and evaluate their performance. We validate the performance of our schemes by means of simulations. We then compare instantiation of our schemes with state-of-the-art announcement schemes, demonstrating that our schemes possess the attractive properties of message reliability, user privacy and accountability while achieving system robustness and performance efficiency.

Keywords: announcement scheme, vehicular ad hoc networks, reliability, privacy, accountability

Contents

List of Figures

List of Tables

Abbreviations

3A	Authenticated Anonymous Announcement Scheme
3G	3rd Generation of mobile phone standards
AHS	Advanced Cruise-Assist Highway Systems project
AP	Access Point
ASD	Aftermarket Safety Device
ASV	Advanced Safety Vehicle project
AU	Application Unit
C2CC	The CAR 2 CAR Communication
CA	Certificate Authority
CAMP	The Crash Avoidance Metric Partnership
CL-PKC	Certificateless-Based Public Key Cryptography
CLS	Certificateless Signature
CRL	Certificate Revocation List
DSRC	Dedicated Short Range Communications
DSSS	Driving Safety Support Systems
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
EU	European Union
GM	Group Manager
GPRS	General Packet Radio Service
GPS	Global Positioning System
GS	Group Signature
GSM	Global System for Mobile communications
GTA	Governmental Transportation Authority
ID-PKC	Identity-Based Public Key Cryptography
ISO	International Organization for Standards
ISS	Integrated Safety Systems
ITS	Intelligent Transportation Systems
IVC	Inter-Vehicle Communication
IEEE	Institute of Electrical and Electronics Engineers

KGC	Key Generator Center
MANET	Mobile Ad hoc Network
MS	Management Server
MLIT	Ministry of Land, Infrastructure and Transportation Japan
NILM	National Institute for Land and Infrastructure Management Japan
NoW	Network on Wheels project
OBU	On-Board Unit
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RA	Registration Authority
RS	Reputation Server
RSU	Road-Side Unit
SeVeCom	Secure Vehicular Communication project
simTD	Safety Intelligent Mobility - Test field Germany
SPDC	Safety Pilot Drivers Clinic
SPMD	Safety Pilot Model Deployment
TIGER	Topologically Integrated Geographical Encoding and Referencing
TM	Tracing Manager
TP	Trusted Party
TRD	Tamper Resistant Device
US	United States of America
V2I	Vehicle-to-Infrastructure communication
V2V	Vehicle-to-Vehicle communication
VAD	Vehicle Awareness Device
VANET	Vehicular Ad hoc Network
VIIC	Vehicle Infrastructure Integration Consortium
VM	Vehicle Manufacturer
VSC	Vehicle Safety Communications project
VSP	Vehicle Safety Pilot
WAVE	Wireless Access in the Vehicular Environment

Chapter 1

Introduction

We state the motivation of our research. We then present an overview on Mobile Ad Hoc Network (MANET) and Vehicular Ad Hoc Network (VANET) and specify the scope of our thesis. We present the objectives and contributions toward the research in this chapter.

Contents

1.1 Motivation

Transportation safety and efficiency is one of the main driving forces for the development of vehicular ad hoc networks (VANETs) [8, 19, 53, 77, 100]. Vehicles equipped with computing and communication devices will allow them to communicate with each other, as well as with the roadside units located at critical points along the road. The transmission of information in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) have the potential to significantly increase the safety of vehicular transportation by warning, supporting and assisting vehicles in critical situations. Various sensors, radar technology and computing platform can be incorporated to monitor, measure and assess a vehicle's surrounding to enable the issuance of early warnings to neighbouring

vehicles. The drivers benefit from the system as information on traffic congestion, accidents, potholes, and slippery roadways will allow receiving vehicles to respond quickly by assessing the situation and making decisions accordingly.

VANETs may help to ease travel by informing vehicles about traffic condition to enable drivers avoid congested route. Congestion is one of the most prevalent transport problems with the increasing traffic volume in recent years [47, 114]. Traffic delays continue to increase especially during peak period, in major cities and highly populated areas. Based on the annual road statistics reported in Transport Statistics Great Britain [108], traffic grew 3.2% between 2001 and 2011. This corresponds to 34 million new cars registered in 2011 compared to about 32 million cars in 2001. Traffic congestion causes an increase in vehicle operating costs (fuel and wear), productivity loss during traffic delay, pollution emissions and stress, particularly as traffic volumes approach a road's capacity.

Despite the increasing traffic volume, a falling rate of road casualties has been observed. According to the statistics published by the UK Department for Transport [108], a number of 203,950 casualties of all severities were reported in 2011, which is 35% lower compared to 2001. The rate drop is a positive progress which can be partly attributed to passive safety system such as airbags and seat belts. Road safety campaigns to increase public awareness and new and revised laws and regulations also play a role. On average, worldwide, over 1.2 million people die of road casualty every year and between 20 and 50 million others suffer non-fatal injuries, including disability [74, 85, 113]. India has the worst road traffic accident rate worldwide with over 130,000 deaths annually revealed by World Health Organization (WHO) [113]. In most regions of the world, the global epidemic of traffic accidents remains worrying. This epidemic may be caused by poorly maintained road conditions, lack of safety awareness and human errors. With the recent progress in information and communication technologies employed in VANETs, it may improve safety by early detection of potential dangers and alert vehicles in its proximity to be aware of the situation ahead of them so that appropriate actions can be taken.

Apart from road safety and traffic efficiency, additional add-on features such as internet access, parking, electronic toll collection, payment services, media download,

and location-based services can be incorporated into vehicles. This may enhance the user's convenience and comfort.

1.2 Problem Overview

The integration of information technology within vehicles resulted in vehicles being more than just a glass and steel but a hackable network of computers. The need for scrutiny is growing as vehicles are increasingly automated and connected to the internet. As vehicles get connected, they will face some of the same security threats as other network devices. It opens up the possibility for malicious adversaries to control certain aspect of the vehicle. This includes deactivating the brake system, send fake warning signals to the driver and rob the when they pull over to check their vehicle or disrupt with other accessories of the vehicles such as airbags, global positioning system (GPS), headlights and cruise control.

Car hacking was a topic in Defcon 21 held in Las Vegas in 2013 [97]. A car hacking code was released and car hacking via physical connection to the car was demonstrated. While these instances of vehicles being hacked were mostly for research purposes, this is due to change as connected vehicles become ubiquitous and therefore a more vulnerable target to criminals and scammers. In general, security is concerned with the protection against malicious manipulation of vehicles and network system, and privacy preservation of the vehicles. These aspects plays an important role when designing and implementing such applications. As VANETs safety applications may prevent life-endangering accidents, it must be protected against attacks. Security breach on a vehicle could pose a threat, leaving them vulnerable and potentially causing harm. A secure communication design in VANETs should be emphasized to ensure that vehicles can fully utilize the benefits provided by the safety applications. Hence the security of this category is mandatory, since the proper operation of any of these applications should be guaranteed even in the presence of attackers.

1.3 Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) [26] is a dynamic and self-configuring network consisting of a group of mobile nodes that communicate without requiring a fixed wireless infrastructure. When the mobile nodes are embedded within vehicles, the network is called a vehicular ad hoc network (VANET). As VANET is a type of MANET, we include a discussion on MANET for a comprehensive understanding of VANET.

Entities. A mobile ad hoc network (MANET) is composed of mobile nodes communicating peer-to-peer. The communication takes place over relatively bandwidth constrained wireless links in a self-organized pattern in the absence of a centralized infrastructure.

Type of communications. MANET applications are usually based on *one-to-one* (unicast) or *one-to-many* (multicast) messages. In a unicast with fixed addressing, the receiver of a message is another node in the network specified by its IP address. Similarly, in a multicast, the message by a sender is sent to a given subset of receivers. The network is decentralized, where all network activities including discovering the topology and delivering messages must be executed by the nodes themselves, that is, routing functionality will be incorporated into mobile nodes. Therefore, the message is sent over a *single-hop* (direct connection) or *multi-hops* (message relayed over multiple nodes) until it reaches its destination.

Characteristics. In MANETs, information is transmitted through single- or multi-hops between the nodes over a wireless channel. Wireless connection has lower capacity than infrastructure networks. The realized throughput of wireless communication, after accounting for the effects of multiple access, fading noise and interference conditions is often less than a radio's maximum rate. It has dynamic topologies where nodes move arbitrarily with different speed and direction, thus the network topology may change randomly and unpredictably. Mobile nodes in MANETs tend to be battery-operated with limited processing power. Energy is consumed in processing and transmitting information to its destination, as each node acts as an end user and a router.

Challenges. MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. The challenges of MANETs are limited wireless coverage, limited bandwidth and battery power, and dynamic network topology [26, 88, 116].

Applications. In the past few years, with the rapid advances in mobile ad hoc networking research, mobile ad hoc networks have attracted considerable attention and interests from commercial business industry, as well as the standards community. The introduction of new technologies such as the Bluetooth, IEEE 802.11 and cellular mobile networks (e.g., GSM, GPRS, and 3G) has fostered the deployment of ad hoc technology and new ad hoc networking applications has expanded substantially since then. Some MANETs applications are presented in Table 1.1 below, along with the services they provide in each area [26].

1.4 Vehicular Ad Hoc Networks

Entities. A VANET [19, 21, 103] is comprised of nodes: vehicles and roadside units (RSUs), and trusted parties (TPs). Onboard units (OBUs) embedded in vehicles enable short-range wireless connection for communication to occur between vehicles (V2V) and roadside units, which is commonly referred to as infrastructure (V2I). Stationary infrastructures located at fixed point along the road which are connected to the backbone of the network may facilitate the communication and provide information for vehicles.

Types of communication. Communication can be classified according to the number of senders and receivers involved. Single sender paradigms are: *one-to-one* (unicast)

Applications	Descriptions/services
Tactical Networks	◦ Military communication and operations. ◦ Automated battlefields.
Sensor Networks [4]	◦ Home applications and smart sensor nodes can be buried in appliances to allow end users to manage home devices locally and remotely. ◦ Environmental applications include tracking the movements of animals, chemical/ biological detection, precision agriculture, etc. ◦ Tracking data highly correlated in time and space, e.g., remote sensors for weather, earth activities.
Emergency Services	◦ Search and rescue operations, as well as disaster recovery; e.g., early retrieval and transmission of patient data (record, status, diagnosis) from/to the hospital. ◦ Replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire etc.
Commercial	◦ E-Commerce: e.g., electronic payments from anywhere.
Home and Enterprise Networking	◦ Home/Office Wireless Networking (WLAN) e.g., shared whiteboard application; use PDA to print anywhere.
Educational	◦ Setup virtual classrooms or conference rooms. ◦ Setup ad hoc communication during conferences, meetings, or lectures.
Entertainment	◦ Multi-user games. ◦ Outdoor Internet access.

Table 1.1: MANET applications

in which a single sender transmit message to a single receiver; *one-to-all* (broadcast) in which one source sends message to all nodes in the network within its proximity; and *one-to-many* (multicast) where a single source sends message to a given subset of nodes. Unicast is important especially for commercial and entertainment applications. Safety and efficiency applications, however, mainly use broadcast, which is sometimes denoted as "beacon" [6, 32, 94, 110, 111] or "heartbeat message" [16, 17, 104] in the literature. A variant of a broadcast is called geographic broadcast or simply referred to *geocast* where the dissemination of a message is limited to a specific geographic region.

The message could be transmitted over a *single-hop*, where the transmission of the mes-

sage is broadcast with no intermediate nodes, and/or *multi-hops*, where the message can be relayed by neighbours to receivers out of the broadcast range of the originator. In VANETs, both single-hop broadcast and multi-hop broadcast are used, depending on the application and scenario. According to the DSRC (Dedicated Short Range Communications) specifications [40] and due to their broadcast nature, safety messages are transmitted over a single-hop with a sufficient transmission power to warn vehicles in a range equal to the distance travelled in 10 seconds at the senders speed, thus eliminating the need for multi-hops. Nevertheless, some form of multi-hops exists. For instance, vehicles that receive warning messages estimate whether the reported problems can also affect their followers; in this case, they forward the messages to them [82].

Channels. Mobile, wireless and medium access technologies are rapidly evolving, and this evolution provides opportunities to utilize these technologies in support of advanced vehicle safety applications. In particular, the DSRC at 5.9 GHz developed by the IEEE team, with direct involvement from the European Telecommunications Standard Institute (ETSI) and International Organization for Standards (ISO) offers the potential to effectively support wireless data communications in V2V and V2I. We summarize the information on representative vehicular communication wireless link in Table 1.2 below [82].

Characteristics	802.11p WAVE
Bit rate	3 - 27 Mb/s
Communication range	$<$ 1000 m
Channel bandwidth	10 MHz
Allocation spectrum	75 MHz (US) 30 MHz (EU)
Frequency band	5.86 - 5.92 GHz
Standard	IEEE, ISO, ETSI

Table 1.2: VANET channels

Characteristics. Similar to MANETs, nodes in VANETs have short radio transmission ranges, low bandwidths, and self–organization and management of the nodes. However, there are several aspects in which the communication in these two ad hoc networks differ from each other [23]. Mobile nodes embedded in vehicles have higher computational power. They also have high mobility. The very high speed of real time

constraint is the unique characteristics of VANETs. It only gives a short period of connection time between neighbors. This may result in frequent changes in network topology and may cause considerable transmission overhead. Vehicle movements are also constrained by the road topology.

Challenges. In a higher network density, the message generated by vehicles may exceed the available bandwidth during a busy traffic period, for instance. Subsequently, this may cause network congestion that leads to transmission delay and packet loss. The long life cycle of vehicles will also impose some challenges to the design of an architectural system that will allow the onboard system to thwart rising threats and risks. A study in [59] proposed a component-based security architecture for VANETs that allows reconfiguration, enhancement or replacement of the components (substituting cryptographic algorithms, for instance) throughout the life cycle of the vehicle.

Applications. VANETs may become the largest ad hoc network ever deployed due to the various applications and potential benefits they provide for the safety and comfort of future VANETs users. VANETs applications are usually classified as safety and non-safety applications [19, 92]. Instances of non-safety applications include internet access, infotainment, parking, electronic toll collection and location-based services [64, 68, 98, 102]. Value added services contributes to enhance driver's traveling experience and convenience. Safety applications are further categorised as safety-related and safety-critical in [63]. Safety-critical is latency critical. This means that the information has to be transmitted and received quickly. Some examples of safety-critical applications [29, 69] include intersection transverse, lane merging or sudden brake alert. Meanwhile, safety-related messages [24, 25, 34, 36, 55, 65, 91] such as information on traffic congestion or road conditions (e.g. slippery road, potholes) has less time restriction. A summary of VANET application is presented in Table 1.3 below.

In this thesis, we focus on a single-hop broadcast scenario for safety-related applications. Our interest lies in improving transportation safety. This can be achieved via safety-related applications deployed in VANETs. The nature of a broadcast communication allows all vehicles within proximity to be aware of an event ahead of them, make decisions accordingly, and act upon the message received. The use of dedicated short range communication (DSRC) as a communication medium permits safety messages to

Applications	Descriptions/services
Safety-related	◦ Congestion notification. ◦ Road condition (e.g. slippery road, potholes). ◦ Detour notification.
Safety-critical	◦ Sudden braking. ◦ Intersection tranversing. ◦ Lane merging. ◦ Collision avoidance.
Non-safety	◦ Internet access (online game, instant messaging). ◦ Commercial information. ◦ Navigation (e.g. map, GPS). ◦ Automated toll payment service. ◦ Location-based services.

Table 1.3: VANET applications

be transmitted over a single-hop with a sufficient transmission power to warn vehicles in a range equal to the distance travelled in 10 seconds at the sender's speed, thus eliminating the need for multi-hop. Nevertheless, some form of multi-hop still exists. Vehicles that receive warning messages determine whether the reported problems can also affect their followers; in this case, they forward the messages to them. In some other case, a multi-hop may not be necessary, as an event occurring in a particular location may not be of interest or affect vehicles in a wider radius coverage.

1.4.1 Current Developments

Significant developments to create a safer and more efficient driving environment have taken place over the past years in the area of vehicular communication system. In this section, we explain the main characteristics of the standardization process and research projects initiatives, focusing on current developments in US, Europe, and Japan.

1.4.1.1 United States of America

The first milestone of standardization process is achieved by the Federal Communications Consortium (FCC) in the United States (US) in 1997. A licensed frequency band of about 75 MHz in the 5.9 GHz band was allocated for VANETs, which is commonly referred to as Dedicated Short Range Communications (DSRC) [40]. A similar band has been allocated in Europe and Japan - the 802.11p, also referred to as wireless access for vehicular environment (WAVE) adopted by the IEEE task group which provide wireless data communications for vehicles and roadside infrastructure.

The Crash Avoidance Metric Partnership (CAMP) launched in 1995 by Ford, General Motor, and Vehicle Infrastructure Integration Consortium (VIIC) has built research in accident prevention and network connected vehicles. VIIC consists of BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VolksWagen. Within CAMP, the Vehicle Safety Communication (VSC) project was initiated in 2002 under cooperation agreement with US Department of Transportation (DoT). The project aims to develop and facilitate the advancement of vehicle safety through communication technologies. VSC has defined preliminary communications requirements which include security and privacy, depending on safety applications. They further evaluated proposed DSRC standards, identified specific technical issues such as standardization and installation of security module (also known as a tamper resistant device) and related hardware integration required (e.g. GPS antenna and receiver, ethernet switch, and DSRC antenna). In CAMP VSC-2 (2005-2009), successful completed projects demonstrated basic feasibility of V2V communications using DSRC. The VSC project is currently in its third phase (VSC-3) which consists of Ford, GM, Honda, Hyundai-Kia, Mercedes, Nissan, Toyota, and VW-Audi.

The US DoT, CAMP and their research associates initiated Vehicle Safety Pilot (VSP), which consists of Safety Pilot Drivers Clinic (SPDC) and Safety Pilot Model Deployment (SPMD) [95]. The SPDC was conducted in 2011 and took place in six locations in US: Michigan, Minnesota, Florida, Virginia, Texas and California. Approximately 100 drivers were selected in each driver clinic to have hands-on experience with vehicles equipped with built-in wireless safety warning device. The test was to evaluate and understand drivers responsiveness and acceptance towards safety warnings in connected

vehicles. It was also to determine whether they find the system useful and help them to drive safer. The first phase received positive feedback where 9 out of 10 drivers value the safety benefits derived from the technology. They also express their likelihood of having the technology in their own vehicle [87].

The second phase of VSP, which is SPDM was initiated in the autumn of 2012, and ran until the autumn of 2013. The trial is composed of RSUs and 3000 vehicles conducted in Ann Arbor, Michigan. These participating vehicles include fully integrated safety systems (ISS), aftermarket safety devices (ASD) and vehicle awareness device (VAD). An ISS allows a vehicle to broadcast and receive messages, and process the information via visual, audio, and/or haptic warning of received messages to alert the vehicle driver. Such haptic technology that transfer information to the driver includes steering wheel vibration [9, 75, 76], driver's seat vibration [22, 33] and steering wheel torque signal [9, 20, 41, 62, 86]. The frequency of vibrations applied onto a steering wheel can be up to 200 Hz, with safety measure that such vibration will not affect the rotation of the steering wheel without manual intervention by the driver [9]. The driver's seat vibration is commonly used for vehicle navigation and warning system. For instance, the left part of the seat pan vibrates to inform the driver to turn left or the back support of the seat vibrates to warn the driver that the vehicle exceeded the speed limit permitted. Meanwhile, the steering wheel torque signal initiates a steering reaction or prohibiting a steering action of the driver. This will assist the driver in case of an imminent lane departure or a possible dangerous lane change manoeuvre [9, 20]. An ASD can send and receive messages from other vehicles over a DSRC wireless communications link. An ASD has a driver interface, runs V2V and V2I safety applications, and issues audible and visual warnings to the driver. Meanwhile, a VAD has limited capabilities. It does not generate warnings, but transmits a vehicles speed and location only over a DSRC wireless communications link. A demonstration of these safety applications were performed at the 22^{nd} ITS America Annual Meeting and Exposition on May 21-23, 2012, at the Gaylord National Convention Center in National Harbor, Maryland [78]. This demonstration involves vehicles from each of different participating manufacturers that supports one or more of the following safety applications: Emergency Electronic Brake Lights, Forward Collision Warning, Blind Spot Warning or Lane Change Warning, Do Not Pass Warning, Intersection Movement Assist and Left Turn Assist. The purpose of the demonstration is to evaluate human factor and usability, system effectiveness

and performance. It collects empirical data to present a more accurate and detailed understanding of the potential safety benefits from this technology. It also aim to show how V2V interoperability among vehicles from different automotive manufacturers can allow vehicles to communicate and understand each other. These connected vehicle safety systems may help drivers avoid crashes despite of vehicle make, model or type. The response solicited from participating drivers shows that 91% feels the V2V technology is necessary after training prior to the exposure. The acceptance rate increases to 93% after exposure to the technology [107].

The evolution of automotive safety development is composed of three phases [1]; the first and second phase which has been deployed were passive safety system (e.g. airbags and seat belt tighten) and active safety system (e.g. electronic stability control, collision avoidance system). In the current third phase (CAMP VSC-3), the V2V-Interoperability project that focused on security management of the system was initiated. The objective of the project is to establish technical requirements of main operations such as device initialization, certificate provisioning, and misbehaviour detection and revocation. It also aims to develop, test, validate and utilize a prototype security design [106, 107] that has been patent and published in 2011. The prototype security system requires a PKI which is deemed necessary to provide basis for trust relationship for vehicles in the system. It uses DSRC and 3G cellular as the communication system. Three types of communication were deployed in the prototype security system design: (i) safety related messages announced by vehicles, (ii) misbehaviour reported by vehicles to the trusted party (`TP`) and (iii) communication with the `TP` for a vehicle to acquire new certificates and the `TP` update vehicles with certificate revocation list (CRL). It allows vehicles to be connected to the `TP` server by connecting it to the infrastructure. The first batch of short term certificates were loaded onto vehicles during its initialization phase and subsequent loaded can be perform over-the-air. The short term certificates were updated automatically for privacy protection. The project will continue to assess and identify any system vulnerabilities and improve V2V communications for a deployment decision on vehicle safety coming in the next coming years.

1.4.1.2 Europe

There are several active VANET-related projects, with collaborations from the automotive industry, governmental agencies and academia in Europe. The European SeVeCoM project (2006-2009) [100] is coordinated by Trialog, and the consortium consists of four universities and three companies: Budapest University of Technology and Economics, École Polytechnique Fédéral de Lausanne, Katholieke Universiteit Leuven, Ulm University, DaimlerChrysler, Robert Bosch GmbH and Fiat Research Center. The project objective was to define the security architecture of such networks as well as to propose a roadmap for integration of security functions in these networks. It discussed different aspects of vehicular communications (VC), such as secure communication protocols, privacy issues, inter-vehicle security and various issues related to the implementation and practical deployment aspects. A prototype that implements various security components for a secure privacy-preserving vehicular communication was demonstrated at the 7^{th} Annual International Conference on Mobile System in Krakow, Poland [57]. The prototype follows the architectural components that satisfy the required security objectives and formal specification developed by SeVeCoM. The SeVeCom implementation is based on the communication system provided by BMW and runs on a computer connected to a dedicated vehicular communication subsystems, namely Denso Wireless Safety Units (WSUs). The IEEE 802.11p was utilized as the wireless communication system. The demonstrator composed of two application scenarios. The first one is a cooperative awareness application. Vehicles communicate with each other via exchange of periodic beacon messages. Warnings is displayed if there is a risk for collision, for instance. The second application features a road hazard warning system based on roadside units (RSUs) sending a road condition warning to approaching vehicles. This includes multi-hop forwarding of warning messages to reach vehicles in a larger coverage. The security aspects of both applications were heavily considered. An emulation of a hardware security module that is responsible for secure storage of secret key material, performing cryptographic tasks (such as signature generation and verification), and time stamping was designed. Vehicles were assigned with long-term identities with the presence of back-end certification authority who is responsible for certificate management and revocation. Privacy is achieved by means of updating pseudonyms. This includes change of cryptographic material and addresses used by the communication system, such as MAC addresses [58]. The demonstration of the prototype provides a

form of validation before such technology is deployed onto vehicles.

The CAR 2 CAR Communication (C2CC) Consortium [21] is an ongoing project founded by a collaboration of several vehicle manufacturers, which is dedicated to further increase safety and efficiency by means of inter-vehicle communications (IVC). The goal of the C2CC is to standardize interfaces and protocols of wireless communications between vehicles and their environment in order to make the vehicles of different manufacturers interoperable and also enable them to communicate with roadside units. It further aims to create an open European industry standard for Car2Car communication systems based on wireless communication and ensure European-wide inter vehicle operability. This include proposing deployment strategies and business models to catalyse market penetration.

The Network on Wheels (NoW) project (2004-2008) [77] was a joint effort of Germany's industry and academia: Mannheim University, Karlsruhe University, BMW, Daimler, Volkswagen, Siemens, Fraunhofer Institute for Open Communication Systems (FICS), and NEC Europe Ltd. Its objective is to specify and design a communication system for transmission of sensor data for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), introducting strategies and business models. The NoW project was deployed as a basis for field operational test in Safety in Mobility - test field Germany (simTD), a test field which we shall describe below.

The Safe Intelligent Mobility - Test field Germany (simTD), launched in 2012 in Frankfurt, Germany, was one of the world's largest field operational tests for V2V and V2I communication [42, 112]. The field operational test comprises of 400 vehicles and 100 RSUs provided by participants Audi, BMW, Daimler, Ford, Opel, and Volkswagen. The consortium also includes Bosch, Continental, Deutsche Telekom, regional infrastructure operators and German research institutions (Technische Universität München und Berlin, Universität Würzburg, Fraunhofer). In the project, various applications and services in the areas of road safety, traffic efficiency and additional value-adding services were tested. In one of the test fields conducted by Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT) under simTD, privacy protection techniques were integrated within participating vehicles, where the identity of vehicles were protected. This approach is realized by vehicles use pseudonyms that they frequently

change to avoid being tracked. Based on the evaluation of the field test, pseudonym resolution is possible when the situation dictates, such as when a vehicle is malfunctioning. Information transmitted over the ad hoc network between vehicles and infrastructure can be encrypted and signed as required. The necessary digital certificates were used by a special public key infrastructure (PKI) which is implemented and operated by Fraunhofer SIT. These cryptographic mechanisms provides data integrity, message authenticity and data confidentiality. The deployment of the test field were based on specification and standardization of CAR 2 CAR Communication (C2CC) Consortium and the European Telecommunications Standards Institute (ETSI). The field operation test is vital to demonstrate real-world and wireless connected vehicle safety capabilities. The work will pave way for full deployment of V2V and V2I systems in Europe. The test field will provide some of the data needed to develop next generation safety and mobility features.

1.4.1.3 Japan

Considerable effort has been invested in investigating various aspects of VANET systems and architecture in Japan. A number of projects studying inter-vehicle communication (IVC) systems has been initiated since the early 1980s and expanded their study to the standardization of IVC systems [43, 103].

The Advanced Cruise-Assist Highway Systems (AHS) [3] and Advanced Safety Vehicle (ASV) [8, 53] are ongoing development projects driven by the Ministry of Land, Infrastructure and Transportation (MLIT). The combination of AHS and AVS is called *Smartway*. The AHS project focuses on V2I communications and employs infrastructures that help to monitor highway condition (such as other vehicles, obstacles, highway surface conditions), assist drivers by providing information (such as speed limit and obstacle detection and avoidance) and create efficient traffic system. A test field involved participation by drivers from the general public was conducted from July 2000 to March 2001 in Tsukuba City. The demonstration site was at the National Institute for Land and Infrastructure Management (NILIM) test course of approximately 6 km in length. The results deduced from the test field verifies that the numerous safety applications provided by the AHS are effective in actual accident prevention [2].

The Advanced Safety Vehicle (ASV) program [8, 53] focuses on V2V communications and is composed of two aspects: active and passive safety. In the active safety trial, systems are tested which addresses inattention and driver errors. This includes drowsiness warning systems, vision enhancement systems, navigation systems, automatic collision avoidance systems and lane departure systems. Meanwhile, the passive safety systems includes impact absorption systems, occupant protection systems, pedestrian protection systems and door lock sensing systems. The project was initiated in 1991 and is now in its fifth generation ASV-5.

Honda Motor Co., has participated in ASV program since phase 1. Based on research conducted in ASV-1 (1991-1996) and ASV-2 (1996-2000), a number of advanced active safety systems has been developed and commercialized such as Adaptive Cruise Control, Collision Mitigation Brake System and Intelligent Night Vision System [48]. In 2005, Honda Advanced Safety Vehicle ASV-3 [49] was presented. Honda ASV-3 vehicles were designed with advanced technological features and support various safety applications including Oncoming Vehicle Information Assistance System, Intersection Stop & Go Assistance System, Head-on Collision Avoidance Assistance System, Cornering Speed Control System and Advanced Mayday System. In phase 4 of Advanced Safety Vehicle (2006-2010), Honda performed V2V and V2I testing on public roadways of its Driving Safety Support Systems (DSSS) in Tochigi Perfecture, Japan using vehicles developed in ASV-3 [50]. The purpose of the project was to utilize positional information gleaned from communications between vehicles and road infrastructure to help prevent certain types of traffic accidents. The objectives of the testing will be 1) to verify inter-vehicle and road-to-vehicle communications functions; 2) to verify DSSS functions; and 3) to collect and present data that will contribute to evaluating system effectiveness, thereby contributing to the prevention of accidents involving rear-end collisions, collisions between turning vehicles and oncoming vehicles, and collisions involving turning vehicles with vehicles passing on the inside.

In 2010, Honda participated in ITS-2010 where a large scale verification testing for DSSS, ASV and Smartway were performed in Tokyo, Japan. The testing was conducted using Honda latest generation of ASV-4 vehicles which are equipped with several new advanced safety technologies. These include a system that uses cameras for image recognition and radar that detects obstruction on roads. ASV-4 vehicles uses

V2V communications to relay information to other vehicles about its position and condition in a simple and clear way. Vehicles were alerted via audio and visual warnings, and tactile signals such as vibrating the brake or accelerator. The camera installed on vehicles will also be able to detect stop signs on road or notify vehicles when it approaches red traffic lights. As the result of ITS-Safety 2010, two V2I safety systems of DSSS and Smartway have been realized in Japan in 2011.

1.4.2 Security and Privacy Issues

In order to benefit from the tools of VANETs, the system requires secure communication protocols. Safety can only be achieved if the content of the messages transmitted are reliable. A message is considered reliable if the announcement was sent unmodified by a legitimate vehicle. The message should also reflect the actual situation. However, frequent communication between vehicles may pose privacy issue. Individual vehicle could be tracked based on messages announced, enabling *profiling* by an adversary. From the vehicle's perspective, sensitive information such as identity and location privacy should be preserved against unlawful tracing. This is an issue because aspect of vehicle's privacy has been studied in one of the projects. Lack of privacy may hinder the broad acceptance of this technology. Solving an inherent conflict between reliability and privacy poses significant challenges. At the same time, a compromise between a vehicle's privacy and accountability is desirable in case of dispute. In such situation, the misbehaved vehicle should be traceable by trusted parties and revoke from the system. They also could not deny having sent the message. We assume the presence of small fraction of adversaries that aims to disrupt the system. Availability and system robustness are also important issues.

1.4.3 Scope and Objectives of the Thesis

The scope of the thesis focuses on authenticated anonymous announcement (`3A`) schemes in VANETs. A `3A` scheme allows vehicles to broadcast safety-related messages regarding vehicles, road situation and traffic condition in VANETs. We concentrate on V2V communication, with the support of access points that relays messages between ve-

hicles and the trusted parties (TPs), who are responsible for managing the admission and eviction of vehicles to the scheme. We propose 3A schemes in a broadcast scenario for VANETs. We show that our schemes are reliable and anonymous while achieving performance efficiency.

Security and privacy are two critical concerns in the design of announcement schemes in VANETs. This Ph. D. thesis intends:

1. to find constructions of announcement schemes that are usable, secure, efficient and comparable (or better) than existing schemes;
2. to formulate a generic abstraction of a 3A scheme designed using threshold method;
3. to formulate a generic abstraction a 3A scheme designed using reputation system model;
4. to design three anonymous authenticated announcement (3A) schemes conciliating security, privacy and performance in VANETs based on the proposed abstractions:
    - the first scheme uses public key cryptography and reputation system;
    - the other two schemes were constructed using certificateless signature.

1.5 Organisation of Thesis

This thesis is organised as follows.

Chapter 2 studies the security and performance goals for the design of an efficient 3A scheme for vehicular communications. We then present different techniques used to achieve these goals and discuss the advantages and shortcomings of these techniques.

Chapter 3 reviews current literature on security and privacy-preserving announcement schemes in VANETs. The chapter is partition into two. The first part is based on threshold mechanism. We group recent protocols according to their main credentials

techniques and examine the extent to which they satisfy the goals discussed in Chapter 2. The second part reviews current literature on announcement schemes based on trust- and reputation-based models. We then summarize each part.

Chapter 4 presents a new `3A` which is designed using public key cryptography and reputation systems. This technique efficiently address the computation processing bottleneck in `3A` scheme for securing VANETs. We then perform simulations to evaluate its performance efficiency and discuss the results. This chapter is an extension of the publication below, where the scheme presented here provides privacy to vehicles.

- Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang. A Reputation-based Announcement Scheme for VANETs. IEEE Transactions on Vehicular Technology, 61(9):4095-4108, 2012.

In Chapter 5, we propose two privacy-preserving announcement schemes in VANETs. The first proposed scheme employs certificateless signature (`CLS`) and reputation systems as building blocks. The second scheme is constructed with `CLS` using threshold method. We show that our schemes allows entity authentication and message integrity while eliminating the necessity of certificates. This vastly reduces the overhead associated with certificate management. Analysis shows that cryptographic operations in `CLS` introduce only very slight overhead to the underlying VANETs while achieves high performance without degrading security. Most of the work presented in this chapter appears in the following publication.

- A. Malip, S. Ng, and Q. Li. A Certificateless Anonymous Authenticated Announcement Scheme in Vehicular Ad Hoc Networks. Security and Communication Networks, 7(3):588-601, 2014.

Chapter 6 contains concluding remarks of the thesis. We summarize our contributions and discuss some future directions of the research.

Chapter 2

Anonymous Authenticated Announcements Scheme

In this chapter, we define an anonymous authenticated announcements scheme and describe the presence of entities in the network. We then examine the contradictory requirements of a reliable, private and accountable VANET message announcement scheme, and consider how these contradictions may be resolved. We examine different techniques used to achieve these security requirements and examine on the advantages and shortcomings of the techniques.

Contents

2.1 Entities in a VANET

A VANET is composed of vehicles and stationary units along the road, known as roadside units. In addition, there will be trusted parties such as national transportation authorities or vehicle manufacturers, who may or may not be online. There also exist malignant entities who aim to disrupt the system.

2.1.1 Vehicles and Onboard Units

A vehicle is equipped with an onboard unit (OBU) and tamper resistant device (TRD), which is commonly assumed in the literature [24, 34, 36, 45, 92]. An onboard unit (OBU) is at least equipped with a (short range) wireless communication device dedicated for road safety, and potentially with other optional communication devices. Vehicles equipped with OBUs will be able to broadcast and endorse messages. These OBUs communicate directly if wireless connectivity exists between them. If there is no direct connectivity, dedicated routing protocols allow multi-hop communications, where messages are forwarded from one OBU to another, until it reaches the destination. Vehicles are also equipped with an application unit (AU) that can utilize the OBU's communication capabilities. Such units include hazard warning or a navigation system like a global positioning system (GPS) receiver that also allow clock synchronisation. Additional features such as speed, temperature, and wind sensors may also be available, depending on manufacturing design.

A tamper resistant device (TRD) such as a black box is integrated as part of the vehicle. The TRD is used to provide secure storage for private keys. Even in the possession of an attacker, this private information cannot be retrieved. The device also executes cryptographic operations correctly. Such operations include generating and verifying signatures. An attacker who is in control of a black box may generate fake

messages of his own choice. However, even though they control the input, the device will operate according to the protocol. Furthermore, the TRD should be supported with time stamping service [92]. The vehicle supplies the power source to recharge the device. A clock is also installed, where it is securely resynchronised (for instance, when passing by a roadside unit).

2.1.2 Roadside Units

A roadside unit (RSU) is a physical device located at fixed locations. Such locations include along the highways, intersections, roundabouts or traffic lights. To allow communications, a RSU is equipped with at least a network device for short-range wireless communication. The main roles of a RSU include the sending, receiving and forwarding of data to an OBU when the OBU enters the RSU communication range. RSUs may also communicate with other RSUs. An RSU may also act as information service provider running safety applications such as low bridge warnings, virtual traffic signalling or as an intersection controller. As it may be connected to an infrastructure network, the RSU may provide internet connection to OBUs.

VANETs technology should be partially operating upon its launch in the next few years. The basic functions and security mechanisms should be available during its first few years of deployment. However, the availability of infrastructures will not be pervasive, especially in the first years of deployments due to its administrative and installation cost. In this thesis, we will focus on anonymous authenticated announcement (3A) schemes that do not rely on RSUs.

2.1.3 Trusted Parties

Trusted parties (TPs) may be vehicle manufacturers (VMs) or governmental transportation authorities (GTAs) with which the vehicles are registered [92]. These TPs may play the role of certification authorities (CAs), registration authorities (RAs), key generator center (KGC) or reputation server (RS) and may be responsible for the distribution and management of identities and cryptographic credentials of the vehicles. Vehicles

registered with different TPs can communicate securely via cross-certification between TPs. In the literature, the TPs are commonly referred to as the certification authorities (CAs) [18, 28, 61, 92]. In some cases, the TP is known as a group manager (GM) and a tracing manager (TM) [24, 35, 66]. In our schemes presented in Chapter 4 and Chapter 5 and in other reputation-based schemes, the reputation server (RS) and management server (MS) plays the role of the TPs. Schemes differ on level of trust in TPs. Some schemes rely on a fully trusted TPs [115]. Meanwhile, in some other schemes, partial trust towards the TPs is assumed. The notion of partial trust is sometimes referred to as *honest-but-curious* or *semi-honest* [24, 36]; these two terms are often interchangeable in the literature. Informally, this assumption implies that the TPs faithfully follow all protocol specifications. However, they may store and analyze intermediate results to derive additional information [44]. The level of trust invested in these TPs may not be absolute. In our schemes presented in Chapter 4 and 5, we adopt a weaker trust assumptions that the TPs has no access to private secrets of a vehicle. A weaker trust assumption implies more robust system against vehicle control, say by a malicious TP or organized criminal, for whom it would be harder to access the vehicle's private key for instance. As the vehicle is the sole possessor of its private key, it also allows non-repudiation if misbehaviour occurs. We further discuss this in section 3.2.

The main role of the TPs is to manage long-term identities, credentials and cryptographic keys of vehicles. They are also responsible for revoking vehicles for administrative reasons or in case of misbehaviour. Periodic communication may take place between TPs and vehicles. As the TP may not be available all the time, an offline communication is assumed between these two entities [24, 81]. The roadside infrastructure or other infrastructure-based network (such as cellular radio network) may offer an alternative means of interactions.

2.1.4 Adversary

One of the common assumptions in VANETs is the presence of a small fraction of adversaries [24, 36, 45, 80, 92, 93] in the network. There are several types of adversaries discussed in the literature. More on the adversaries can be found in [83, 92]. There may be external or internal adversaries. An external adversary is an entity who

is without possession of any cryptographic credentials or direct physical access to the system. On the other hand, an internal attacker is a legitimate user of the VANET who is in possession of the credentials and black box. Legitimate dishonest users may cause more damage as they can control the black box to generate messages of their choice.

Adversaries can also be categorised as rational or irrational attackers. This type of adversarial model was considered in [10, 36]. A rational attacker has a plan for an attack to achieve his personal benefit where the benefits outweigh the cost. Meanwhile, an irrational attacker has no personal gain. For example in [92], a terrorist may intentionally cause traffic accidents and delays to create chaos without considering the consequences. An attack can also be performed by a group of colluding vehicles who have mutual agenda or interest. For instance, these colluding vehicles may announce a fake message regarding traffic congestion in a particular area to make way for themselves.

The adversarial model can be further categorised as active or passive attackers, which is considered in some schemes, such as in [56]. An active attacker vigorously participate in the network with intentions to cause disruption. Such attacks include generating bogus information, replay legitimate messages and modify a message. Meanwhile, a passive attacker attempts to learn and listen via eavesdropping for instance.

Another attributes to classify adversaries is that they can be local or extended [89, 92]. A local attacker has limited territorial control, despite controlling several entities (vehicles or roadside units). An extended attacker controls several entities in a wider coverage area scattered across the network, thus extending his scope.

In the anonymous authenticated announcement (`3A`) schemes proposed in the thesis, the presence of internal adversaries is considered. This is common in the literature, where most papers assume internal adversaries in the network [24, 45, 80]. As authentication phase prevents most of the attacks performed by an external adversary, the thesis focus on the existence of an internal adversary. An internal adversary can exploit their legitimacy to cause harm to other vehicles. Having the same capabilities as other legitimate vehicles, they can use their credentials issued by a trusted party

(TP) to perform attacks that are likely to be successful, which pose a real threat to the system.

2.2 Anonymous Authenticated Announcement (3A) Schemes

An announcement scheme is a system that facilitates dissemination of safety related messages in vehicular ad hoc network. A safety-related message contain information about speed, current time of the event, position, direction, acceleration and specific message to traffic events such as congestion notification, accidents or potholes alert. Transmission of safety messages in the network enable safer driving environment and traffic efficiency provided that the information announced is reliable. A message is considered to be reliable if the unmodified message was broadcasted by a legitimate vehicle and is trustworthy. However, in a large VANET environment, vehicles do not have a trust relationship with one another. This poses a challenging security problem as verification of message reliability may reveal some information about the sending vehicles. This contradicts with the requirement of privacy. At the same time, should misbehaviour arise, a vehicle should be held accountable. We examine these requirements in this section.

2.3 Requirements of Announcement Scheme in VANETs

Towards the deployment of vehicular communication systems, security and privacy are critical concerns and significant challenges to be met. In this section, we discuss the security objectives and performance efficiencies for a secure 3A scheme.

2.3.1 Reliability

To achieve traffic safety and efficiency, announcement messages have to be trustworthy, that is, the messages reflect actual situations. A receiving vehicle that is, say, 600m away from the reporting location may or may not be able to determine whether the

message it receives is true. Since vehicles do not have a trust relationship with other vehicles in general, a vehicle will only trust an announcement if it can be certain that this announcement was broadcast unmodified by a legitimate vehicle, and that the message is also not a falsehood. The first objective requires **message authentication** and **data integrity**. The second objective, which we shall refer to as **message truthfulness**, is not easily achieved. Different techniques have been proposed to achieve the second objective. These include *threshold method* and *trust-* and *reputation-based models*. In a threshold method, message truthfulness is established by knowing that messages of the same content were sent by many distinct legitimate senders. Meanwhile, in trust and reputation models, a message is considered reliable if the message generator has "good" reputation.

2.3.2 Privacy

The need and requirement for privacy are addressed differently in different countries. Some countries enforce drivers' identification mechanism for crime prevention. Other countries may adopt an opposite policy by mandatory privacy in the system. For instance, under European Union (EU) law, everyone is entitled to the protection right of personal data within the EU [30]. In this paper, we assume the requirement for privacy as it is one of vital reasons for public acceptance towards the deployment of a VANET [30, 37, 66, 92]. Communication in the network should be **anonymous** where a message should not reveal any information about the user. User-related privacy information should be protected in the presence of an unauthorised observer. Furthermore, the activities of the sender should be **unlinkable** to its source. In some schemes, a higher level of privacy is proposed where the identity of vehicles making announcements are protected, even from the authorities. However, full anonymity may allow for misbehaviour as vehicles or attackers may act maliciously without the fear of being caught. In recent papers [24, 35], some schemes allowing authorities to know the identity of the vehicles are proposed which achieve *conditional anonymity*, that is, the identity of the user remains anonymous unless they misbehave or malfunction of the device is detected.

2.3.3 Accountability

In a pervasive VANET environment, misbehaviour may take place as a result of hardware malfunctioning or it may be intentional. For instance, the safety–related messages may contain fake information, or may have been modified, discarded or delayed intentionally. In such situations, it is desirable to achieve accountability. Misbehaviour should be **traceable** to a source. It should also achieve **non-repudiation**, that is, a source cannot deny having sent the message. Furthermore, misbehaved vehicles should be **revoked** to prevent from future participation in the network. The identity of the vehicle may also be revealed by the authorities.

2.3.4 System Robustness

System robustness implies that the communication channel is authentic and integrity protected even in the presence of malicious or faulty nodes.

2.3.5 Efficiency

Computational Time. Safety-related applications in VANETs impose constraints in terms of real-time processing. The time sensitivity of information requires that processing latency on each vehicle is kept to an absolute minimum. Due to vehicle's high mobility, vehicles encounters short duration of connectivity. This implies that message should be generated quickly enough to be transmitted before the short communication ends. The authentication mechanism designed for a `3A` scheme must also allow fast message verification as delay in validating the information may render the message unused.

Communication Cost. According to DSRC [40], a vehicle broadcasts safety messages every 100-300 ms to other vehicles. A vehicle may receive many safety messages from other vehicles within a short span of time. Hence, the messages should be lightweight to not overload the communication medium, especially when the number of vehicles within the communication range is high.

Storage. Cryptographic authentication technique have been widely exploited to secure vehicular communication. Cryptographic credentials have to be securely stored and may have to be constantly updated due to various reasons. One of the reasons is to achieve privacy. Two techniques commonly used to satisfy the property of privacy is *pseudonyms* and *group signature*. In pseudonymous authentication, vehicles stores a number of public/private key, and its corresponding certificate. The changing of pseudonyms is required to make tracking of vehicles difficult. Therefore, the size of the anonymous key should be small to reduce storage space on vehicle. The implementation of group signature over anonymous certificate is that the former overcome the limitation of pre-storing a large number of anonymous certificates. However, the issue associated with group signature is that size of the signature is quite big.

2.4 Analysis of Security Mechanisms

In this section, we survey the literature for an overview of how these security requirements are achieved and evaluate their system performance.

2.4.1 Reliability of Messages

In a VANET safety application, building trust is vital. Vehicles are assumed to have a weak (or absence of) trust relationship with each other [24]. A vehicle will only trust an announcement if it can be certain that the message was generated by a legitimate vehicle without unauthorized modification and is not a falsehood. The first objective is commonly satisfied by some digital signature schemes, while the second is not as straightforward. Different techniques have been proposed to achieve the second requirement. These include *threshold method* and *trust-* and *reputation-based models*. We will further discuss these techniques in the next subsection.

2.4.1.1 Message Authentication and Data Integrity

One of the cryptographic mechanisms used to achieve message authentication and data integrity is symmetric primitives. This includes a message authentication code (MAC) appended to a message which is computed using a shared symmetric secret key. A third party would have to be shown the secret key to validate a MAC, and even then he would have not known which of the two parties computed the MAC. This technique is used in [25, 28]. While symmetric based techniques are computationally efficient, it does not provide the property of non-repudiation.

Digital signature of some form is more commonly used to solve the problem of authentication and integrity. A variety of digital signature schemes is used in existing literature: group signatures (GS) [18, 24, 66], message-linkable group signature (MLGS) [36], "traditional" public key cryptography (PKC) [18, 61, 80], and identity-based signatures [55]. Signing message using valid credentials from a trusted party (`TP`) will satisfy authentication and data integrity.

2.4.1.2 Message Truthfulness

Different techniques have been proposed to evaluate message truthfulness, which include threshold method [24, 34, 36, 61, 90], network modelling [45, 99], and trust-based and reputation-based models [38, 65, 70, 73, 84].

In a *threshold method*, a vehicle accepts a message if it receives messages with the same content that have been announced by a number of distinct vehicles that exceeds a threshold within a time interval. This is a common approach and is used in [24, 34, 45, 61, 90]. In a big VANET environment where the absence of initial trust is assumed, the receiver will only accept a message if it has been sent by a sufficient number of different vehicles in order to gain some assurance.

A threshold may be fixed system-wide [34, 90] or flexible [24, 45, 61]. In the first case, the threshold is set to a certain value and applies to all participants in the system. One of the weaknesses is that it may not be suitable for all scenarios. For instance,

the threshold may be higher in a city with high traffic density, but this may not be suitable for an area with a small density of road traffic. Meanwhile, a flexible threshold allows the user to determine the bound based on the content of the message and situation. The threshold should not be too high that insufficient endorsement occurred that might hinder the user from acting upon the information. It should not be too low that the decision may be affected by the presence of adversaries. Decision methods based on voting schemes were proposed in [79] to assist users to decide whether or not to rely on the information when the messages are in conflict with each other.

The threshold method requires message origins to be distinguishable. When a vehicle receives a number of announcements of a certain event, it needs to ensure that each message originated from a different source. However, if there is also requirement for privacy, this will directly contradict the requirement for unlinkability. If message origins cannot be distinguished then a Sybil attack [39] may be possible. In a Sybil attack, a vehicle signs the same message multiple times using different identities to deceive the receiver into accepting the fraudulent message. Hence, the threshold method used should allow distinguishability of origin. This has been achieved in some schemes [24, 36]. Meanwhile, in some other schemes, this requirement is not satisfied [18, 56, 66, 92]. Distinguishability of message origin is not be a problem to some other techniques. In schemes based on reputation system [65, 70], a receiving vehicle is only required to verify a message provided that the message generator has sufficiently high reputation. This allows computational efficiency. It also allows a vehicle to make a decision quickly and act on the message received.

Another issue associated with threshold method is a concern on how to verify numerous cryptographic signatures received by vehicles in a timely manner to allow vehicles to make decision and act upon the message quickly.

Golle et al. [45] and Schmidt et al. [99] proposed the evaluation of message reliability by modelling the network. In [45], a scheme that allows vehicles to detect and correct malicious messages in VANETs was presented. Vehicles are assumed to maintain a "model" of the VANET, which contains all the knowledge that the vehicles possess about the VANET. A vehicle can then compare the messages received against the model of the VANET. A message that is consistent and agrees with the vehicle's

model is likely to be accepted as valid. Inconsistent messages are addressed using a heuristic approach. A vehicle will search for explanations for the inconsistent messages and rank all possible explanations according to the heuristic approach. The message with the highest scoring explanation will be validated. However, requiring vehicles to possess a wide knowledge of the network may be infeasible and impractical. Schmidt et al. proposed a framework for vehicle behaviour analysis in [99]. A vehicle's behaviour refers to all observable information including its movement and position in the past and present. A receiving vehicle accumulates a sequence of messages from a broadcasting vehicle and these may provide sufficient information for behaviour analysis. The result of this analysis will help to determine a vehicle as trustworthy, neutral or untrustworthy. In this approach, vehicles are required to make observations before a decision can be made. This may not be desirable in VANETs as vehicles are not able to act quickly upon the messages received.

Several trust-based and reputation-based models, for example [38, 65, 70, 73, 84], have been presented in the literature. In [65, 70], a centralised reputation-based announcement schemes for VANETs was proposed. The reliability of a message generated by a vehicle is reflected by its reputation score. A message is considered reliable if the message generator has sufficiently high reputation. A vehicle consistently announcing reliable messages increases its reputation score. Meanwhile, the reputation score of an unreliable message generator decreases, by means of a feedback mechanism. A feedback report consists of a numerical score, which represents a receivers evaluation of the reliability of the relevant message. For these schemes, distinguishability of message origin is not a problem. A receiving vehicles is only required to verify a message provided that the message generator has sufficiently high reputation. Not only is it computationally efficient, it also allows a vehicle to make a decision quickly and act on the message received.

The schemes proposed in [38, 73, 84, 99] adopted a decentralised infrastructure. In [38], Dötzer et al. proposed a reputation system based on a mechanism called *Opinion Piggybacking*. In this approach, a vehicle generates a message and broadcast to its neighbouring vehicles. A receiving vehicle will append its own opinion about the reliability of the message that may be based on the content of the message or the aggregated opinions already appended to the message. Upon receiving a message, a vehicle is

required to compute and aggregate previous opinions appended to the message before it decides and generate its own opinion. This may cause computational burden on receiving vehicles. In addition, details of implementation such as the initialisation of the reputation system and the update of reputation score of vehicles were not discussed. Issues of revocation and robustness against possible collusion of adversaries were also not addressed.

In the scheme by Minhas et al. in [73], message reliability is evaluated by modelling the trustworthiness of the message generator. In this scheme, vehicle trustworthiness is modelled based on the combination of three trust models: role-based trust, experience-based trust and majority-based trust. *Role-based trust* exploits certain predefined roles that are enabled through the identification of vehicles. For instance, vehicles may have more trust towards traffic patrol or law enforcing authorities compared to other vehicles. To avoid impersonation attack, each vehicle is required to possess a certificate that includes its name, role and public key, issued by a trusted authority for authentication purposes. Meanwhile, *majority-based trust* is similar to the threshold method we discussed earlier. *Experience-based trust* is established based on direct interactions: a vehicle determines who to trust based on how truthful they have been in their past interactions. However, such a model requires vehicles to establish a long-term relationship with each other, which may not be practical in a big VANET environment. Furthermore, it also requires vehicles to store information regarding vehicles it has encountered in the past. This may lead to storage problem. A similar approach of experienced-based trust was proposed by Patwardhan et al. in [84].

However, most of the trust- and reputation-based schemes such as in [38, 65, 73, 84, 99] lack of privacy provision. In addition, the issue associated with schemes that adopted a decentralised infrastructure such as in [38, 73, 84, 99] is the problem of accountability.

2.4.2 Privacy

Communication in VANETs requires the receiver of a message to authenticate sender. However, such verification may reveal some information about the sender's identity and location. For example, in some signature scheme, the certificate of the signer's public

key may allow linking of activities. This is because signing a message may link the certificate of the signing vehicle. There are two aspects of privacy that we consider; anonymity and unlinkability. Anonymity means that the identity of a user is unknown to the others in the network. It must not assume that individual vehicles can always be identified by some unique code that is openly communicated. Meanwhile, unlinkability indicates that the activities cannot be linked to a source. This is to avoid profiling of a user based on their movement pattern.

2.4.2.1 Anonymity

A common approach to achieve anonymity is by using pseudonyms. In [45, 46, 51, 61, 92], randomly chosen and changing pseudonyms are used to prevent linking to real identity. In [55, 56], these pseudonyms are used as public keys in place of identity in ID-based announcement schemes. Each key may be used once for each message or used to sign multiple messages over its short lifetime, where the key change frequency varies on some factors such as vehicle's speed. The pseudonyms is updated in order to prevent linking of vehicle's activities. However, the drawback from pseudonymous technique includes secure distribution of keys, key management and complexity of storage.

Another approach to seek anonymity may be achieved by using group signature, where the group is the set of all participating cars. `3A` schemes based on group signature (GS) has been designed for the V2V safety application [24, 36, 66]. Group signature allows each group member to sign on behalf of the group. A verifier may know the signature belong to which group without being able to associate it to a signer. In certain ciarcumstances, such as revocation, the `TP` may reveal the identity of the signer. The main merit of group signatures based technique over the pseudonym approach is that the former overcomes the limitation of pre-storing a large number of anonymous certificates. However, group signatures are usually much longer than the regular signatures. This may causes an expensive storage load when messages are stored for liability purposes. It also does not provide distinction of message origin.

2.4.2.2 Unlinkability

Messages can be linked if it is signed using the same pseudonym. However, linking message will be more challenging if vehicles change and update pseudonym regularly. Pseudonyms can be preloaded or self-generated. The drawbacks of former method include key management and large storage space [61]. To eliminate these problems, [18] proposed that each vehicle generates its own pseudonyms. The rate at which pseudonyms are updated depends on various factors such as the degree of privacy required by a vehicle. However, an issue associated with this technique is the problem distinguishability of message origin as discussed in Section 2.4.1.2. The property of message unlinkability is also achieved using group signature [18, 24, 36, 66] where it is computationally hard to determine whether two messages were announced by the same group member or not.

A silent period was proposed in [17, 98] to achieve unlinkability. The level of unlinkability is dependent on the number of vehicles presents at the time the change of pseudonyms takes place. Higher velocity of vehicles present at the time of pseudonym update decreases the ability of an adversary to probabilistically determine and link pseudonyms and vice versa. During silent period, transmission of messages is temporarily disabled for a period of time. A vehicle do not receive any incoming message either. The drawback of this technique is that it restricts a vehicle from generating or receiving a message, which defeats the purpose of VANETs deployment.

2.4.3 Accountability

Accountability is achieved if it satisfies the traceability, non-repudiation and revocation requirement. The necessity for accountability in VANETs arises from the possibility of misbehaviour among users that may harm public road safety and jeopardize its future deployment. Misbehaviour in VANETs may occur as a result of hardware malfunctioning or malicious activities of users in the system. Such activities may include prevention of broadcasting messages to other vehicles; generating fake messages; injection of non-safety related message that may caused traffic in the network due to the overload of the bandwidth; or escaping from an accident. While attacks performed by outsiders can

be addressed by means of authentication, misbehaviour among legitimate senders is a more challenging problem to address. This is because they possess valid credentials by the authority and may be able to deceive receiving vehicles into trusting them.

2.4.3.1 Traceability

While traceability is desirable when dispute arise, this problem is difficult to address with the privacy requirement. Different methods have been studied to solve this problem. For instance, in scheme that uses pseudonyms (for example, [45, 46, 51, 92]), the pseudonyms can be linked to the real identity of the vehicle unique electronic license plate (ELP) to trace the misbehaved user by the authorities. Meanwhile, in group signature, some schemes allow a *tracing manager* to revoke the anonymity of malicious vehicles by *opening signatures* [24, 36]. However, some schemes revoke the misbehaved vehicles without being able to reveal the vehicles identity by any central authorities (for example, [23]).

2.4.3.2 Non-Repudiation

Another aspect of accountability is non-repudiation. A vehicle cannot deny having sent a message signed using an anonymous key that belong exclusively to the sender, assuming forgery is not possible [24, 35]. Neither could they claim that the message is replayed if a timestamp is included in each message. In some other schemes [28, 56], non-repudiation is assumed in the presence of a fully trusted party (`TP`). A challenge-response protocol is another approach to achieve non-repudiation in [24]: given a signature on a message, the challenge-response protocol determines whether a vehicle is the signer of a message.

2.4.3.3 Revocation

In the literature, the most common approach is by updating and distributing certificate revocation lists (CRLs) across the network via RSUs or other information service points.

As the authority keep records of all issued certificates, an anonymous key used to sign the malicious message can be associated to the misbehaved vehicle by matching the information stored in the database. This may occur with the aid of the TP [80, 92] or infrastructure [66, 92]. Such aid is required as the CRL is assumed to be large and the vehicle has limited storage capacity. However, such design must be constructed carefully as this may result in key management problem [92] or heavy reliance on infrastructure [66, 92] which may render the protocol inefficient. An approach to address the problem of large CRL was proposed in [66]. This hybrid method requires the unrevoked vehicles to update their private key and group public key with the group manager (GM) when the number of revoked vehicles exceed some predefined threshold. However, it leads to scalability problem where it requires an effective approach to update the parameters of remaining vehicles in the network. In reputation-based schemes [65, 70], revocation can be achieved by ceasing to provide misbehaved vehicles with their reputation credentials. A vehicle whose reputation score decreases to zero would then no longer be able to continue its future participation in the network.

Chapter 3

Literature Review

In this chapter, we review schemes based on threshold mechanism and trust- and reputation-based models. In the first part, we classify recent protocols using the threshold method according to their main credential techniques. In a similar fashion, we classify recent trust- and reputation-based models according to their main approaches. We then examine the extent to which they satisfy the properties of reliability, privacy and accountability.

Contents

3.1 Abstraction of a 3A Scheme using the Threshold Method

In this section, we present a generalization of a 3A scheme using the threshold method demonstrated in Figure 3.1. The network consists of a trusted party (TP) and vehicles; sending vehicle V_s and receiver of the message V_r as described in Section 2.1.

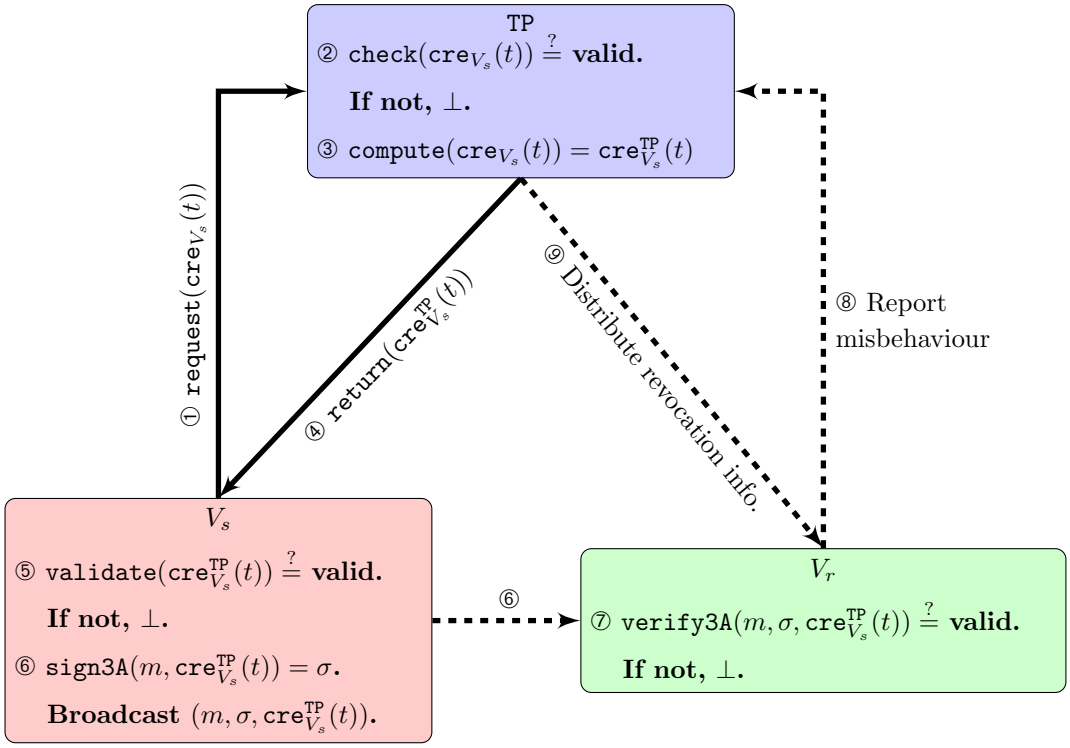

Figure 3.1: Abstraction of a Threshold Scheme.

We define a 3A scheme that satisfy the following properties. A 3A scheme must be able to prove that (i) the message m originate from a legitimate sender V_s, (ii) that the content of m has not been altered and (iii) a $\texttt{cre}^{\texttt{TP}}_{V_s}(t)$ was issued from the TP. A common 3A scheme is achieved using digital signature. The 3A is composed of sign3A() and verify3A(). The sign3A() takes input a vehicle's credential $\texttt{cre}^{\texttt{TP}}_{V_s}(t)$ and message associated with the event m and output a signature σ. The verify3A() takes input a

message m, a signature σ generated on the message and V's credential $\mathtt{cre}_{V_s}^{\mathtt{TP}}$ to verify σ.

We first present the *initialisation phase* of a 3A scheme before we describe the abstraction of a threshold scheme. The actions of each entity are described as follow:

1. Trusted Party (TP).
   (a) computation of public system parameters params. We assume the distribution of params to all entities in the network;
   (b) installation of some part of the 3A scheme. For instance, it needs verify3A() to check signed reports of misbehaviour.
2. Vehicles.
   (a) A V has some initial credential. There are 2 types of credentials. A $\mathtt{cre}_V$ may be documentation for proof of vehicle's ownership, some secret unknown to others or credentials already embedded within V which could be V's ID before it is enrolled in VANETs. The second one is the type that is issued by the TP.
   (b) installation of a secure authenticated anonymous announcement scheme 3A.

We omit the initialisation phase in Figure 3.1 as not to crowd the diagram.

3.1.1 Description of the threshold scheme

In this section, we describe each phase for a threshold scheme. There are two channels used to transmit information as depicted in Figure 3.1. The first one is called a *secure channel*, denoted by $\rightarrow$. We define secure channel that provides message authentication and confidentiality. Secondly, an authenticated and integrity protected channel, denoted by $\dashrightarrow$ is called a *public channel*. The abstraction of a threshold scheme is composed of the following phase.

A **Registration Phase.**

Step ①. Firstly V_s sends request for credentials $\texttt{request}(\texttt{cre}_{V_s}(t))$ at time t to participate in the network.

Step ②. The TP performs $\texttt{check}(\texttt{cre}_{V_s}(t))$. This verifies that the request originated from V_s and that V_s has not been revoked from the system. If the check fails the request is denied.

Step ③. Upon success verification, the TP generates credentials for V_s by executing $\texttt{compute}(\texttt{cre}_{V_s}(t)) = \texttt{cre}^{\texttt{TP}}_{V_s}(t)$ where $\texttt{cre}^{\texttt{TP}}_{V_s}(t)$ denotes credentials issued by TP for V_s at time t. The credentials $\texttt{cre}^{\texttt{TP}}_{V_s}(t)$ may be used by V_s to:

(a) make an announcement;

(b) generate other credentials;

(c) to report misbehaviour or to request new credentials.

Step ④. The TP performs $\texttt{return}(\texttt{cre}^{\texttt{TP}}_{V_s}(t))$ where the TP sends credentials it has computed to V_s.

Step ⑤. When V_s receives the credentials, it performs $\texttt{validate}(\texttt{cre}^{\texttt{TP}}_{V_s}(t))$ that verifies $\texttt{cre}^{\texttt{TP}}_{V_s}(t)$ indeed originate from the TP and the content has not been tampered. This phase is performed over a secure channel.

Periodic Credential Provision. For future participation in the network, a vehicle may periodically request credentials from the TP. We call this a *periodic credential provision*. We note that in some schemes, Steps ① to ⑤ may be repeated periodically for vehicles to obtain new credentials. In this case the frequency of retrieval will depend on the restrictions of the system. Long intervals between retrieval period (for instance, annually during vehical maintenance) mean that the vehicles will have to store a large number of credentials. Short intervals mean that vehicles store fewer credentials, but may require more frequent communications with the TP.

B **Broadcast Phase.**

Step ⑥. When V_s detects potential hazard on road, it will warn neighboring vehicles and announce the event over a public channel. It generates a signature $\sigma = \texttt{sign3A}(m, \texttt{cre}^{\texttt{TP}}_{V_s}(t))$. A vehicle V_s then broadcast $(m, \sigma, \texttt{cre}^{\texttt{TP}}_{V_s})$ to neighbouring vehicles.

C **Message Verification Phase.**

Step ⑦. A V_r performs $\texttt{verify3A}(m, \texttt{cre}_{V_s}^{\texttt{TP}}(t), \sigma)$ where it accepts a message as valid if V_s is legitimate and the integrity of the message is preserved. In a threshold scheme, this step is repeated many times and V_r will accept a message to be true if it receives a threshold number of messages of the same event reported by distinct vehicles over a short period of time

D **Revocation Phase.**

Step ⑧. If V_r experienced any misbehaviour from its encounter with V_s, it may lodge a report, sign it with its credential and send it to the TP via the wireless channel.

Step ⑨. Upon receiving reports, the TP verify V_r's authenticity and integrity of the report before arriving at a decision whether to revoke Vs from the system. The TP may also periodically update revocation information and distribute it across the network.

3.2 Reviews of 3A Techniques

In the past few years , significant interest has been displayed through the active research related to VANETs. Various cryptographic primitives have been proposed to design an efficient VANETs architectural system to solve security problems. In this section we survey some recent 3A schemes providing the three goals and classify them according to their main credential techniques. Our focus will be on vehicle-to-vehicle (V2V) communication and we shall not assume the availability of infrastructures. Each subsection focuses on a different technique used to realise a 3A.

3.2.1 Schemes based on group signatures

A group signature scheme allows each member A of the group (comprising all members registered with a particular TP) to sign a message on behalf of the group without A's identity being revealed to the verifier. In addition, two signatures of a legitimate group member cannot to linked, that is, it is impossible to tell whether two signatures

are produced by a specific signer. Hence group signature schemes provide anonymity within a group, and activities of a signer cannot be linked. Some group signature schemes (for example, [24] and [36]) allow a *tracing manager* to reveal group members' identities (by *opening* signatures) but there are also schemes where members' identities cannot be revealed by any trusted parties (for example, [23]). We review five schemes [18, 24, 36, 66, 118] based on group signatures and examine whether they achieve the goals of reliability, privacy and accountability.

3.2.1.1 GSIS: Secure Vehicular Communications with Privacy Preserving

The GSIS scheme was proposed by Lin et al. in [66]. It uses group signatures and identity-based signatures for secure and private announcement protocol in VANETs. The scheme addresses the security of communication between vehicles (V2V) and between vehicles and RSUs (V2I). For a V2I communication, an ID-based signature scheme is used. Here, we will only focus on the V2V communication. In the initialisation phase of the scheme, a vehicle has an initial credential $\texttt{ID}_V$, the TP has $\texttt{params} = \texttt{gpk}$ and 3A is the group signature scheme [11].

A **Registration Phase.**

Step ①. Each vehicle V_s with identity $\texttt{ID}_{V_s}$ sends $\texttt{request}(\texttt{cre}_{V_s}(t)) = \texttt{request}(\texttt{ID}_{V_s})$ to the TP.

Step ②. The TP $\texttt{check}(\texttt{ID}_{V_s})$ to verify the request.

Step ③. If the request proves to be valid, the TP performs $\texttt{compute}(\texttt{cre}_{V_s}(t)) = \texttt{cre}^{\texttt{TP}}_{V_s}(t) = \texttt{gsk}_{\texttt{V}_\texttt{s}}$, where $\texttt{gsk}_{\texttt{V}_\texttt{s}}$ is V_s unique group signing key. The TP stores tracing information A_{V_s} with $\texttt{ID}_{V_s}$.

Step ④. The TP $\texttt{return}(\texttt{gsk}_{\texttt{V}_\texttt{s}})$ to V_s.

Step ⑤. The V_s performed $\texttt{validate}(\texttt{gsk}_{\texttt{V}_\texttt{s}})$ to verify that it originated from the TP and integrity protected.

B **Broadcast Phase.**

Step ⑥. Given a message associated with an event m and gsk as an input to $\texttt{sign3A}(m, \texttt{cre}^{\texttt{TP}}_{V_s}(t)) = \texttt{sign3A}(m, \texttt{gsk}) = \sigma$ and broadcast (m, σ) to neigboring

vehicles V_r.

C **Message Verification Phase.**

Step ⑦. Once the message is received, V_r performs `verify3A`$(m, \texttt{gpk}, \sigma)$ where the message is accepted as valid if the signature σ is successfully verified using V_s group public key `gpk` and that V_s who generated it has not been revoked.

D **Revocation Phase.**

Step ⑧. This is not described in the scheme. We assume that misbehaviour can be reported anonymously by a vehicle V by using `sign3A`.

Step ⑨. The revocation is performed by hybrid membership revocation where the CRL–based verifier-local revocation (VLR) is utilized. Below a threshold number of revoked vehicles, revocation is similar to a traditional CRL–based revocation scheme where revocation list are distributed in the network. Once the threshold is exceeded, the `gpk` and private keys of all unrevoked vehicles are updated, leaving the revoked vehicles unable to continue generating valid signature.

Discussion. As a vehicle uses credentials distributed by the authority for signing messages, it guarantees the authenticity of the sender and integrity of the message. However, it cannot be used in threshold mechanism because in this group signature scheme, distinguishability is difficult to achieve without an online manager. This scheme achieves anonymity where the resulting signature keeps the identity of the signer secret, it also satisfy unlinkability where it is computationally hard to determine whether the valid signatures of two different group were computed by the same group member. For accountability, the authority distributes the CRL to the infrastructure points. The revocation process is then performed by the aid of the infrastructure which takes over the authority responsibility. However, this implies reliance on the infrastructure and revocation can only be performed within vicinity. Moreover, while conditional privacy preserves the anonymity of the user as long as they do not misbehave, this scheme allows the disclosure of an honest user's identity by the authority. In addition, as group signature scheme permit the issuer to create the private keys of group members, it does not achieve non-repudiation as the signer is not the sole holder of the signing key [24].

3.2.1.2 Efficient and robust pseudonymous authentication in VANET

Callandriello et al. proposed a Hybrid scheme based on the group signature proposed in [18]. In this scheme, a vehicle is initialised with an initial credential $\texttt{ID}_V$ and associated cryptographic keys. Vehicles are managed by a certification authority (CA), who plays the role as the TP which has params = gpk. The 3A is the group signature scheme based on [11].

A **Registration Phase.**

Step ①. A vehicle V_s sends request for credentials $\texttt{request}(\texttt{cre}_{V_s}(t)) = \texttt{request}(\texttt{ID}_{V_s})$ to the TP.

Step ②. The TP $\texttt{check}(\texttt{ID}_{V_s})$ to verify the request.

Step ③. The TP $\texttt{compute}(\texttt{cre}_{V_s}(t)) = \texttt{cre}^{\texttt{TP}}_{V_s}(t) = \texttt{gsk}_{\texttt{V}_\texttt{s}}$, where $\texttt{gsk}_\texttt{V}$ is V_s unique group signing key.

Step ④. The TP $\texttt{return}(\texttt{gsk}_{\texttt{V}_\texttt{s}})$ which denotes its group signing key.

Step ⑤. V_s performs $\texttt{validate}(\texttt{gsk}_{\texttt{V}_\texttt{s}})$ that it originated from the TP and integrity protected.

B **Broadcast Phase.**

Step ⑥. V_s performs $\texttt{sign3A}(m, \texttt{cre}^{\texttt{TP}}_{V_s}) = \texttt{sign3A}(m, \texttt{gsk}_{\texttt{V}_\texttt{s}})$ and output two-part signature $(\sigma_{SK^i_{V_s}}(m), \sigma_{\texttt{gsk}_{V_s}}(PK^i_{V_s}))$ where $\{PK^i_{V_s}, SK^i_{V_s}\}$ are temporary credentials generated by V_s used as input for the sign3A(). The group signing key $\texttt{gsk}_{\texttt{V}_\texttt{s}}$ is used to sign each $PK^i_{V_s}$, essentially certifying $PK^i_{V_s}$. It then broadcast the message tuple $(m, \sigma_{SK^i_{V_s}}(m), \sigma_{\texttt{gsk}_{V_s}}(PK^i_{V_s}))$.

C **Message Verification Phase.**

Step ⑦. A verifier can thus be convinced that the announcement m is sent by a legitimate group member without being able to identify V_s indicated by performing $\texttt{verify3A}(m, PK^i_{V_s}, \texttt{gpk}, \sigma) = \texttt{valid}$. Each pseudonym $PK^i_{V_s}$ is updated to $PK^{i+1}_{V_s}$ after its lifetime expires. A verifier cannot link a pseudonym with any other pseudonyms used by V_s.

D **Revocation Phase.**

Step ⑧. This step is not included in the scheme. We assume that a vehicle uses `sign3A()` to anonymously report a misbehaviour.

Step ⑨. A `TP` can identify and revoke a group member, using updated CRL distributed into the network.

Discussion. While this scheme achieves a level of reliability in that it provides assurance of the legitimacy of a sender and integrity of the message, it cannot be used in a threshold mechanism. Even though messages sent within the time period can be linked, a rogue vehicle may generate and certify many pseudonyms within any time period and thus masquerade as multiple vehicles. Without an online tracing manager, such behaviour cannot be detected. In addition, if the time period τ is short (in order to avoid linking) then messages cannot be linked and thus the scheme does not provide distinguishability of message origins. A CRL is used for revocation. This ability allows a level of accountability, but compromises privacy - a vehicle may be identified whether or not it is misbehaving. Moreover, the scheme does not provide non-repudiation, since the `TP` also holds the signing key.

3.2.1.3 Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications

Wu et al. proposed a general framework based on message–linkable group signature (MLGS) in [35]. It is a variant of group signature where a message link identifier can only be generated once for a message. This is an approach to prevent misbehaviour (i.e. vehicles sign the same message more than once) among vehicles. Vehicles signing two messages with the same content can be traced and punished by having its `ID` disclosed or by exclusion from the network. Each vehicle is registered to a vehicle administration office that acts as a group registration manager (GM). In addition, there exist tracing manager (TM) who possess some secret information that allow traceability in case of misbehaviour. The authorities are assumed to be honest and semi–trusted, which means they do not have access to the vehicles private key.

A **Registration Phase.**

Step ①. A vehicle V_s sends $\texttt{request}(\texttt{cre}_{V_s}(t)) = \texttt{request}(\texttt{pk}_{V_s}, g^{\texttt{sk}_{Vs}})$ to the TP where $\texttt{pk}_{V_s}$ and $\texttt{sk}_{V_s}$ is its self generated public and secret key pair.

Step ②. The TP $\texttt{check}(\texttt{pk}_{V_s}, g^{\texttt{sk}_{Vs}})$ to verify the request.

Step ③. If the request proven to be valid, the TP $\texttt{compute}(\texttt{cre}_{V_s}(t)) = \texttt{cre}^{\texttt{TP}}_{V_s}(t) = \sigma_{\texttt{sk}_{\texttt{TP}}}(\texttt{pk}_{V_s}) = \texttt{gc}$ where gc is V_s group certificate.

Step ④. The TP $\texttt{return}(\texttt{gc})$ to V_s.

Step ⑤. V_s performed $\texttt{validate}(\texttt{gc})$ to verify that it originated from the TP and integrity protected.

B **Broadcast Phase.**

Step ⑥. A sending vehicle V_s takes input a message m and $(\texttt{sk}_{V_s}, \texttt{pk}_{V_s}, \texttt{gc})$ to generate $\texttt{sign3A}(m, \gamma(m), \texttt{sk}_{V_s}, \texttt{pk}_{V_s}, \texttt{gc})$ which output a signature σ. A $\gamma(m)$ is a message-link identifier that can only be produced once for the same message. An identical $\gamma(m)$ is produced if V_s attempt to sign the same message more than once. A vehicle can be trivially linked by comparing two signatures on the same message. V_s then broadcast $(m, \gamma(m), \sigma)$.

C **Message Verification Phase.**

Step ⑦. Upon receiving the message, receiving vehicle V_r will validate the gc using the TP's public key and later verify the signature. If such verification holds for all n signatures received from n distinct vehicles which exceed certain threshold, V_r is likely to accept the message as valid.

D **Revocation Phase.**

Step ⑧. This is not described in the scheme. We assume that misbehaviour can be reported anonymously by a vehicle V by using sign3A.

Step ⑨. If a vehicle V is found to act maliciously (e.g. signing a message more than once), V can be traced. The validity of σ and m is first verified. The TP who possess some trapdoor information of V_s public key will look up its local database to match it with V's identity for revocation.

Discussion. This scheme satisfies all requirement for a reliable announcement. A V_s who possesed valid credentials issued the by TP assures user authenticity and message

integrity. Sybil attacks in VANETs can be thwarted with this technique as a vehicle is traceable if it signs a message more than once. Therefore, a threshold method can be adopted. This scheme achieves anonymity where the resulting signature keeps the identity of the signer secret, it also satisfy unlinkability where it is computationally hard to determine weather the valid signatures of two different group were computed by the same group member. For accountability, they face the same adverse conditions in group signature-based protocol in which the verification time grows linearly with the number of revoked vehicles and every remaining vehicle need to update its private key and group public key when the number of revoked vehicles exceed some predefined threshold.

3.2.1.4 Threshold Anonymous Announcement in VANET

A threshold anonymous announcement (TAA) scheme was proposed by Chen et al. in [24]. The protocol uses direct anonymous attestation technique [23] and k-time anonymous [105]. The DAA scheme is used as a method to assure the verifier that the anonymous signer possesses valid credentials by the TPs. It can also be seen as a group signature schemes without the facility to trace the signature to its signer [24]. Meanwhile, a k-time anonymous signature scheme allows a signer identity to be recovered by the TP if he signs the message more than k times ($k = 1$ in an announcement scheme).

A **Registration Phase.**

Step ①. A V_s sends a $\texttt{request}(\texttt{comm}_{V_s})$ to the TP where $\texttt{comm}_{V_s}$ is a commitment that binds a secret value f_{V_s} generated by V_s and its private signing key $\texttt{sk}_{V_s}$ embedded within V_s prior to the system set up.

Step ②. The TP $\texttt{check}(\texttt{comm}_{V_s})$ to verify if the request holds to be valid.

Step ③. If it verifies correctly, the TP $\texttt{compute}(\texttt{cre}_{V_s}) = \texttt{cre}_{V_s}^{\texttt{TP}} = (A, B, C)$. It stores a trapdoor information $\texttt{comm}_{V_s}$ associated with f_{V_s}.

Step ④. The TP $\texttt{return}(A, B, C)$ to V_s.

Step ⑤. The V_s verifies the correctness of the credentials by performing $\texttt{validate}(A, B, C)$.

B **Broadcast Phase.**

Step ⑥. A V_s $\texttt{sign3A}(m,(A,B,C)) = \sigma$ and broadcast (m,σ).

C **Message Verification.**

Step ⑦. A receiving vehicle V_r perform $\texttt{verify3A}(m,\sigma,\texttt{gpk})$. In this scheme, a V_r can link two signatures and the identity of V_s can be revealed if V_s announce the same message more than once.

D **Revocation Phase.**

Step ⑧. Each V_r maintains a list β of l events and associated information. It created a new event if it hasn't been reported before. If the event exist in β, the signature σ is checked against the list of σ already received.

Step ⑨. When a revocation list gets longer, the TP update its key pair $(\texttt{sk}_{\texttt{TP}}, \texttt{pk}_{\texttt{TP}})$. It then update (A,B,C) to (A,B,C') of unrevoked vehicles. The revoked vehicles will not have their credentials updated and hence they would not be able to generate a valid signature under the new TP public key $\texttt{pk}'_{\texttt{TP}}$.

Discussion. The requirement of message reliability is satisfied in this scheme. The assurance of message authentication and data integrity is provided by using credentials issued by the TP. Distinguishability of message origin is achieved, where it can determine whether two signatures for the same event were generated by the same signer of not. This permits the adoption of a threshold method. A vehicle can anonymously sign on behalf its group without being identified as the message generator, which preserves user's anonymity. The property of unlinkability is satisfied where its computationally hard to determine whether two valid signatures was generated by the same group member or not. For accountability, non-repudiation is achieved as the signer is the sole holder its secret key. The TP holds V's trapdoor information that allows traceability when misbehaviour issue arise. To address the problem of long rogue list commonly occur in group signature schemes, this scheme proposed permanent revocation. The TP's key pairs and signer's credentials cre are updated, preventing it to continue participating in the network.

3.2.2 Schemes based on pseudonyms

In these schemes, pseudonyms are anonymous public keys certified by a TP that does not contain any identifying information to associate it with a user. Each pseudonym may be used once or has a short lifetime before it is updated to prevent linkability of vehicle's activities. There are a few schemes proposed using pseudonyms which we shall review [27, 34, 92, 115] in this section. We then analyse the extent of security goals achieved.

3.2.2.1 Securing vehicular ad hoc networks

To achieve authentication and conditional privacy, Raya and Hubaux proposed the use of public key cryptography in [92].

A **Registration Phase.**

Step ①. Each vehicle V_s with identity $\mathtt{ID}_{V_s}$ sends $\mathtt{request}(\mathtt{cre}_{V_s}, t) = \mathtt{request}(\mathtt{ID}_{V_s})$ to the TP.

Step ②. The TP $\mathtt{check}(\mathtt{ID}_{V_s})$ to verify the request.

Step ③. If the request proven to be valid, the TP compute a set of credentials as follows: $\mathtt{compute}(\mathtt{cre}_{V_s}(t)) = \mathtt{cre}^{\mathtt{TP}}_{V_s}(t) = (\mathtt{pk}_{\mathtt{V_s}}, \mathtt{sk}_{\mathtt{V_s}}, Cert^{\mathtt{TP}}_{V_s})$. This corresponds to V_s's public and private key, and its corresponding public key certificate, which is TP's signature on V_s public key.

Step ④. The TP $\mathtt{return}(\mathtt{pk}_{\mathtt{V_s}}, \mathtt{sk}_{\mathtt{V_s}}, Cert^{\mathtt{TP}}_{V_s})$ to V_s.

Step ⑤. V_s $\mathtt{validate}(\mathtt{pk}_{\mathtt{V_s}}, \mathtt{sk}_{\mathtt{V_s}}, Cert^{\mathtt{TP}}_{V_s}))$ to verify the correctness of the credentials provided before they are stored.

Periodic Credential Provision.

Periodic credential provision is performed over a long interval between retrieval period (for instance, semi-annual or annually) where the credentials are transmitted over a secure channel. This can be done during regular vehicle maintenance or

renewal vehicle's registration. The reason being is that a large number of credentials for longer term usage may not be feasible to be transmitted over the wireless medium. In some countries, periodic vehicle inspection are mandatory to allow vehicles operate on public road [31]. These occasion can be used to update software, perform system consistency check, and upload new cryptographic materials. In this scheme, Step ① to Step ⑤ as described in Registration Phase above is performed to retrieve credentials.

B **Broadcast Phase.**

Step ⑥. To broadcast a message, V_s takes input m and a randomly selected $\mathtt{sk}_{\mathtt{V_s}}$ to generate $\mathtt{sign3A}(m, \mathtt{sk}_{\mathtt{V_s}})$ which output σ on m. It then broadcast $(m, \sigma, Cert_{V_s}^{\mathtt{TP}})$ where $Cert_{V_s}^{\mathtt{TP}}$ is its corresponding certificate.

C **Message Verification Phase.**

Step ⑦. A receiver V_r $\mathtt{verify3A}(m, \sigma, Cert_{V_s}^{\mathtt{TP}})$ where $\mathtt{pk}_{V_s}$ is extracted and verified using $Cert_{V_s}^{\mathtt{TP}}$. It then verify V_s signature σ on the message using $\mathtt{pk}_{V_s}$.

D **Revocation Phase.**

Step ⑧. This is not described in the scheme. We assume that a vehicle can anonymously report a misbehaviour using `sign3A`().

Step ⑨. Identity resolution in this scheme is preformed by the `TP` who maintains a mapping between long term identity $\mathtt{ID}_{V_s}$ and credentials issued. To revoke a vehicle from the network, three revocation protocols were designed. Revocation protocol of tamper-proof device (RTPD) relays revocation message via the infrastructures to the misbehaving vehicle V_m. All stored keys will be erased once the message which is encrypted with the V_m's public key is received and decrypted by the TPD. When locating a vehicle is infeasible and partial revocation is desired, the revocation protocol using compressed certificate revocation lists (RCCRL), which is based on traditional CRL, is adopted. It reduced communication and storage overhead by employing a compression technique to the CRL. Slightly different from the above two protocols, distributed revocation protocol (DRP) uses a detection malicious technique similar to [45] for revocation. Neighbouring vehicles will report an accumulated accusation against V_m once they reach an infrastructure point. The CA will then update and distribute the CRL within the network.

Discussion. This scheme achieves reliability in sense of authenticity and data integrity. However, their scheme do not prevent Sybil attacks as, for the same message, a signing vehicle can disguise as multiple vehicles. Therefore, threshold mechanism can not be adopted. For signing purpose, each key can only be used once to achieve the need for privacy. In case of dispute, these keys have to be traceable which requires an exhaustive search in the certificate database by the TP. Moreover, it raise manufacturing cost as an advanced storage for key pairs must be issued to maintain privacy over a significant amount of time. This subsequently results in substantial amount of communication overhead to the TP who needs to manage many certificates per vehicle. Associated with revocation techniques, the RTPD protocol is only employed when revoking the keys of V_m is required as it does not allow partial revocation. It also relies heavily on the infrastructures and require the TP to locate and trace the current location of V_m where the message will be send through infrastructures until it is reachable. Similar to RTPD, the RCCRL protocol also depends on the availability of infrastructures to distribute CRL, which may lead to scalability problem. While these three protocols works well with conventional public key infrastructure, using anonymous credentials for preserving privacy whilst achieving traceability and revocation may results in large CRL managed by the TP. This is because each vehicle has many anonymous public key and revoking a vehicle requires revoking all its anonymous keys.

While this scheme achieves authenticity of the sender and integrity of the message, in case where vehicles collude to lie, it is difficult to distinguish and trace misbehaviour as a group of vehicles is assigned with the same key material. Non-repudiation is also not achieved as the VM also possess a copy of the r shares of the signature scheme. All these problems subsequently leads to the problem of irrevocable anonymity.

3.2.2.2 Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication

Xiong et al. proposed a VANET announcement scheme based on revocable ring signatures in [115]. To compare the properties between group signature and ring signature, the anonymity of the signer in group signature is revocable by a trusted party called the group manager. The group manager is also responsible for the formation of groups

of users and distribute specially designed keys to their members. Meanwhile, these ring signatures schemes [96] are simplified group signatures which only have users and no group manager. It does not allow anyone to revoke the signer anonymity, while allowing the actual signer to form a set of possible signers including himself, and sign a message by using his secret key and other's public keys without getting their approval or assistant. Another variant of ring signature called *revocable ring signature* [67] allows a real signer to form a ring arbitrarily while allowing revocable anonymity of the actual signer by the trusted party.

A **Registration Phase.**

Step ①. A vehicle V_s with identity $\mathtt{ID}_{V_s}$ sends $\mathtt{request}(\mathtt{cre}_{V_s}(t)) = \mathtt{request}(\mathtt{ID}_{V_s})$ to the TP.

Step ②. The TP $\mathtt{check}(\mathtt{ID}_{V_s})$ to verify the request.

Step ③. The TP then compute a set of credentials as follows: $\mathtt{compute}(\mathtt{cre}_{V_s}(t)) = \mathtt{cre}^{\mathtt{TP}}_{V_s}(t) = (\mathtt{pk}_{\mathtt{V_s}}, \mathtt{sk}_{\mathtt{V_s}}, Cert^{\mathtt{TP}}_{V_s})$. This denotes V_s's public and private key, and its corresponding public key certificate respectively. The TP stores $(\mathtt{ID}_{V_s}, \mathtt{pk}_{V_s})$ in its database.

Step ④. The TP $\mathtt{return}(\mathtt{cre}^{\mathtt{TP}}_{V_s}(t)) = (\mathtt{pk}_{\mathtt{V_s}}, \mathtt{sk}_{\mathtt{V_s}}, Cert^{\mathtt{TP}}_{V_s})$ to V_s.

Step ⑤. V_s then verify the validity of the credentials received.

B **Broadcast Phase.**

Step ⑥. The sending vehicle V_s dynamically has a set of public keys, say $P = \{\mathtt{pk}_1, \cdots, \mathtt{pk}_n\}$ collected from other vehicles it encounter along its way, where $\mathtt{pk}_{V_s} \in P$. The set P is updated to avoid from being traced and it defines the ring of unrevoked public keys. V_s generate $\mathtt{sign3A}(P, \mathtt{sk}_s, \mathtt{pk}_{GTA}, m)$, output σ and broadcast it.

C **Message Verification Phase.**

Step ⑦. Upon receiving the message, V_r performs $\mathtt{verify3A}(m, P)$. A message is accepted only if σ is validated. Otherwise it is rejected.

D **Revocation Phase.**

Step ⑧. This is not described in the scheme. We assume that a vehicle can anonymously report a misbehaviour using $\mathtt{sign3A}()$.

Step ⑨. Given the signature σ, the TP can determine and trace the real identity of malicious V_s which is stored in its database. The TP broadcast $(\mathtt{pk}_{V_s}, \mathtt{ID}_{V_s})$ to all vehicles in the network. Each vehicle will then add $\mathtt{pk}_{V_s}$ into their local revocation list.

Discussion. The scheme achieves the authenticity of the sender and integrity of the message as the ring signature can only be generated by a valid ring member. However, the message is indistinguishable due to the changing public key set P and therefore, a threshold mechanism cannot be adopted in this scheme. While anonymity is achieved, it does not achieve unlinkability as the vehicle public key $\mathtt{pk}_{V_s}$ is always the same despite changing and updating the other public keys in the set P. For accountability, once a signature is disputed, as only the TP knows their private key, the TP have the ability to trace and revoke the anonymity of misbehaving vehicle. However, non-repudiation is not achieve as the TP also hold V_s's private key.

3.2.2.3 A Security Framework with Strong Non-Repudiation and Privacy in VANETs

A security framework for an announcement scheme using identity-based public key cryptography (ID-PKC) was presented in [27]. This scheme proposed an approach to solve the inherent key escrow problem in ID-PKC. The essence of the idea is to use the identity of the trusted party as a verifier of vehicles' identity.

A **Registration Phase.**

Step ①. The V_s sends $\mathtt{request}(\mathtt{cre}_{V_s}, t) = \mathtt{request}(\mathtt{ID}_{V_s}, \mathtt{pk}_{V_s})$ to the TP where $\mathtt{pk}_{V_s}$ is the self-generated public key $\mathtt{pk}_{V_s}$ by V_s while keeping its corresponding secret key $\mathtt{sk}_{V_s}$ private.

Step ②. The TP $\mathtt{check}(\mathtt{ID}_{V_s}, \mathtt{pk}_{V_s})$ to verify the request.

Step ③. If the request proven to be valid, the TP compute a set of credentials as follows: $\mathtt{compute}(\mathtt{cre}_{V_s}(t)) = \mathtt{cre}^{\mathtt{TP}}_{V_s}(t) = (\mathtt{PID}_{V_s}, Cert^{\mathtt{TP}}_{V_s})$. The $\mathtt{PID}_{V_s}$ is V_s's anonymous identity which is generated using the TP's secret value. Meanwhile $Cert^{\mathtt{TP}}_{V_s}$ is V_s public key certificate, which is TP's signature on $\mathtt{PID}_{V_s}$ and the self-generated public key by V_s.

Step ④. The TP return($\mathtt{PID}_{V_s}, Cert_{V_s}^{\mathtt{TP}}$) to V_s.

Step ⑤. V_s validate($\mathtt{PID}_{V_s}, Cert_{V_s}^{\mathtt{TP}}$) to verify the correctness of the credentials provided before they are stored.

Periodic Credential Provision.

The periodic credential phase for this scheme is similar to the scheme in [92] described earlier.

B **Broadcast Phase.**

Step ⑥. When V_s wishes to broadcast a message, V_s takes input m and a randomly selected $\mathtt{sk}_{\mathtt{V_s}}$ to generate sign3A($m, \mathtt{sk}_{\mathtt{V_s}}$) which output σ on m. It then broadcast $(m, \sigma, \mathtt{pk}_{V_s}, Cert_{V_s}^{\mathtt{TP}}, \mathtt{PID}_{V_s})$.

C **Message Verification Phase.**

Step ⑦. A receiver V_r verify3A($m, \sigma, \mathtt{pk}_{V_s}, Cert_{V_s}^{\mathtt{TP}}, \mathtt{ID}_{\mathtt{TP}}$).

D **Revocation Phase.**

Step ⑧. This is not described in the scheme. We assume that a vehicle can anonymously report a misbehaviour using sign3A().

Step ⑨. Identity resolution in this scheme is preformed by the TP who maintains a mapping between long term identity $\mathtt{ID}_{V_s}$ and credentials issued. To revoke a vehicle from the network, three revocation protocols were designed. Revocation protocol of tamper-proof device (RTPD) relays revocation message via the infrastructures to the misbehaving vehicle V_m. All stored keys will be erased once the message which is encrypted with the V_m's public key is received and decrypted by the TPD. When locating a vehicle is infeasible and partial revocation is desired, the revocation protocol using compressed certificate revocation lists (RCCRL), which is based on traditional CRL, is adopted. It reduced communication and storage overhead by employing a compression technique to the CRL. Slightly different from the above two protocols, distributed revocation protocol (DRP) uses a detection malicious technique similar to [45] for revocation. Neighbouring vehicles will report an accumulated accusation against V_m once they reach an infrastructure point. The TP will then update and distribute the CRL within the network.

Discussion. The TP signs self-generated $\mathtt{pk}_{V_s}$ from V_s, essentially certifying V_s. Messages signed using valid credentials satisfies message authentication and data integrity. However, it cannot adopt the threshold method as message origin is indistinguishable. In terms of privacy, anonymity is achieved using pseudonyms that does not contain any identifying information that associates it to V_s. Messages sign using the same pseudonym is linkable over it's short lifetime. For accountability, non-repudiation is achieved as the vehicle is the sole holder of its secret key. In case of misbehaviour, a vehicle is traceable using the database maintained by the TP and revoked from future participation in the system.

3.2.3 Others

3.2.3.1 Balancing Auditability and Privacy in Vehicular Networks

Choi et al. proposed the use of symmetric cryptosystem for a VANET security architecture design in [28]. The security mechanism is of two types: between vehicles (V2V) and between a vehicle and an infrastructure (V2I). Symmetric key technique is used in a V2V communication, while public/private key for the V2I communication. The infrastructure is responsible for the issuance of pseudonyms which are used to generate anonymous communication in a V2V network.

Initialisation Phase. The TP initializes the system by issuing V's long term pseudonym $\mathtt{PK}_V^x$, for $x = \{1, \cdots, m\}$. The long term pseudonym provides a way to correlate an identity based on a short term pseudonym that will be issued by the infrastructure, also known as the roadside unit (RSU), to V. The uses of the two tiers are used to obscure the vehicles privacy. The TP then creates a database for every vehicle admitted into the network. Each vehicle then perform a preliminary handshake with the RSU whenever it enter new area or switch to a new RSU to obtain its set of short term pseudonyms $\mathtt{pk}_V^i$ and its corresponding session key $\mathtt{KS}_V^i$ for $i = \{1, \cdots, n\}$.

Broadcast Message. To broadcast an event, a sending vehicle V_s randomly choose a pseudonym $\mathtt{pk}_{V_s}^i$ and the corresponding session key $\mathtt{KS}_{V_s}^i$ to compute MAC_i. Once the MAC_i is generated, V_s broadcast the message M_i. A receiving vehicle V_r will store

M_i in its database and send to a nearby RSU. The RSU will run pseudonym lookup to match the session key corresponding to the V_s pseudonym attached to M_i. Once the message is verified, RSU will send M_i back to V_r.

Revocation. Three revocation protocols are proposed in the scheme. Pseudonym auditing (PA) is used to determine the location at a certain time of a vehicle of a given identity. Basic identity auditing (BIA) determine the identity of a vehicle by linking pseudonyms and only the TP can reveal the identity of the vehicle. Meanwhile, application of identity auditing (AIA) aim to find vehicle at a certain time or certain place by querying its database.

Discussion. While the scheme achieves user authenticity and data integrity, it could not distinguish whether two message were signed by the same vehicle or not. This imply threshold mechanism cannot be used in this scheme. For decryption and verification of each message, V_r is required to contact RSU. This may not be ideal and feasible taking into account the real time demand and high mobility of vehicles in the network. To revoke a vehicle, the scheme relies heavily on the infrastructure for revocation computation. Even though symmetric primitives are efficient in terms of computation overhead, it requires preliminary handshake between communicating parties. In a VANET pervasive environment, this is challenging. Furthermore, due to the nature of key symmetric, non-repudiation could not be achieved.

3.2.3.2 Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks

Daza et al. proposed group-based (t, n)-threshold signature schemes in [34]. A (t, n)-threshold signature distributes the signing operation among a group of n participants. Each participant in a distributed signature scheme is given a share $\mathtt{sk}_i$ of the secret key sk in such a way that to sign a message, every participant computes a partial signature $\sigma_i(m)$ using his share of the secret key. Then, any set of at least t participants can compute a valid signature $\sigma(m)$ on the message by combining their partial signatures. This essentially implies that a valid signature $\sigma(m)$ could only be computed if at least t participants participated before a message is announced. This is a different technique

compared to the threshold method in our work, where in a threshold method, a message is considered reliable if at least t messages of the same content were announced by at least t distinctive legitimate participants within a certain time interval. In their paper in [34], three variants of privacy-preserving schemes were proposed, namely group-based private protocol (GBPP), extended group-based private protocol (E-GBPP) and semiprivate protocol for sparse VANETs (SPSV). Here, we only focus on SPSV as it is the most relevant for comparison purposes.

Initialisation Phase. In a group of n participants, the trusted parties TPs sets up d' different (t, n)-threshold signature schemes. The TPs partitioned n vehicles into d' sub-range, each assign to a TP. For $k = 1, \cdots, d'$, the k^{th} scheme consists of a public key $\mathtt{pk}^k$ and n shares secret $\mathtt{sk}_i^k$, where $i = 1, \cdots, n$. Each vehicle V is assigned with the public keys $(\mathtt{pk}^1, \cdots, \mathtt{pk}^{d'})$ and the secret key shares $(\mathtt{sk}_i^1, \cdots, sk_i^{d'})$ which assures legitimacy of users.

Broadcast Phase. To send a message m, V_i randomly select one of the d' threshold signature schemes and compute its partial signature $\sigma_i^k(m)$ using $\mathtt{sk}_i^k$. It then broadcasts $\sigma_i^k(m)$ and m, which includes signature scheme k that was being used. Upon receiving the message, V_y uses the k^{th} threshold scheme to compute its partial signature $\sigma_y^k(m)$ on m. It then broadcasts $\sigma_y^k(m)$ and $H(m)$, where $H(m)$ is the hash of the message input. If exist at least t different partial signatures on m, V_i can compute the signature $\sigma^k(m)$ and broadcast it, along with m. The announcement m will be considered as valid if it can be verified by neighbouring vehicles using the public key $\mathtt{pk}^k$.

Revocation. This scheme did not address revocation techniques for accountability purposes.

Discussion. While this scheme achieves authenticity of the sender and integrity of the message, it does not achieve distinguishability of message origin. Hence, the threshold method cannot be adopted. The other downfall of this scheme is that a valid signature $\sigma(m)$ could not be computed if less than t participants participated, hence a vehicle would not be able to announce a message, rendering the scheme to fall apart. In terms of privacy, the property of anonymity and unlinkability is satisfied. However, the

level of unlinkability is dependent on the value of d' where unlinkability improves by choosing a large value d'. This scheme lack discussion on accountability where the issue of revocation was not addressed. Non-repudiation is also not achieved as the vehicle is not the sole holder of their secret key.

3.3 Conclusion

In Section 3.1 and 3.2, we started our contributions in the area by giving construction of a generic abstraction for `3A` scheme using threshold method. To our knowledge, this is the *first* construction of such abstraction proposed in the literature that systematically studies and generalise threshold-based `3A` schemes. We classified them according to their main credentials techniques which are (i) group signature, (ii) pseudonyms and (iii) for other schemes. We then presented an extensive research of different cryptographic approaches for `3A` schemes in VANETs. We thoroughly analyse the advantages and shortcomings of these schemes. Our analysis cast light on one of the main problems of VANET security where we deduced that the problems of conflicting security goals is a non-trivial matter. This can be seen from Table 3.1 that shows only a small number of schemes which are prevalent to be a secure privacy-preserving system.

In Table 3.1 below, the "✓" indicates the security objective is achieved while the "×" implies the security requirement is not satisfied. Meanwhile, the "✓*" in the unlinkability column implies the scheme achieve partial unlinkability, where messages signed using the same pseudonym are linkable over its short lifetime. The summary of the security goals achieved by the schemes we have reviewed is depicted in Table 3.1 below.

1. **Group signature.** In a group signature, all group members are assigned with the same group public key while possessing their own individual secret key to sign a message. A verifier can verify that the message was signed by a group member without able to determine the signature generator. The properties of group signature satisfy the privacy requirement deemed by most VANETs applications. However, most group signature does not allow indistinguishability of

Security Analysis								
Sec. goals / Schemes	Reliability			Privacy		Accountability		
	Auth.	Int.	Thres.	Anony.	Unlink.	Trace.	Revoke.	Non-Rep.
GSIS [66]	✓	✓	×	✓	✓	✓	✓	×
Hybrid [18]	✓	✓	×	✓	✓*	✓	✓	×
MLGS [35]	✓	✓	✓	✓	✓	✓	✓	✓
TAA [24]	✓	✓	✓	✓	✓	✓	✓	✓
Raya [92]	✓	✓	×	✓	✓*	✓	✓	×
Ring signature [115]	✓	✓	×	✓	×	✓	✓	×
ID-PKC [27]	✓	✓	×	✓	✓*	✓	✓	✓
Symmetric [28]	✓	✓	×	✓	✓	✓	✓	×
Daza et al. [34]	✓	✓	×	✓	✓	✓	×	×

Table 3.1: Comparison of Security Analysis.

message origin without the presence of an online group manager. This may not be feasible in practise. Furthermore, group signature often involves expensive computation and incur considerable signature size.

2. **Public Key Cryptography.** In a public key cryptography (PKC), each user has a pair of keys; one called the public key and the other is called the private key. The public key is made public while the private kept is kept secret. The public key is associated to the user in a trusted manner. This is achieved using a certificate issued by a trusted party (`TP`), which vouching for the fact that a given public key belongs to its rightly owner. Inevitably, this causes the `TP` to require large amount of storage and computing time managing the certificates.

3. **Symmetric Cryptography.** Approaches based on symmetric cryptography requires an establishment of pairwise symmetric key during authentication phase before a message is transmitted. Relying on a key establishment phase is problematic in most VANETs scenarios due to their high velocity and thus, short communication span. This is one of the challenges to deploy symmetric-based techniques in VANETs, as a secure and efficient mechanism to distribute symmetric keys into wireless nodes needs to be well-devised. Some schemes (such as in [28]) requires communication with the `TP` before a secret key is shared between two communicating parties. This may cause the scheme to fall apart with an

offline TP as the shared secret key could not be established, hence hinder communication to take place. On the other hand, distributing symmetric keys in the absence of an online TP (such as in [15]) introduces security concerns. Indeed message authenticated using symmetric techniques can be verified efficiently and involves cheaper computation cost. However, it often occur at the expense of delayed message authentication. This may not be desirable for safety applications in VANETs where messages needs to be processed quickly to allow vehicles utilize and responds to the event announced. Another inherent problem of symmetric cryptography is that it does not support non-repudiation and would need to be extended accordingly to achieve the accountability requirement.

4. **Secret Sharing.** A secret sharing scheme, known as threshold cryptography, requires the participation of at least t of n entities to announce a message. Each entity generates a partial signature and t partial signatures computed on a message will construct a full signature before a message can be broadcasted. The issue associated with this techniques is that the scheme falls apart if less than t entities participates. Therefore, the message could not be broadcasted and utilized.

5. **Ring Signature.**

   Ring signature is a form of group signature. It allows a ring of possible signers to sign messages on behalf of the group without revealing whose signature it belongs to. In contrast to a group signature, the formation of group members in a ring signature is completely ad hoc and it does not require a centralized group manager. However, the drawback of this technique is the lack of accountability. This raises the question on how to revoke misbehaved vehicles in the absence of a trusted party. Most schemes [18, 24, 27, 28, 34, 35, 65, 66, 70, 92] assigned the trusted party to be the sole authority to revoke a vehicle off the network, rather than delegating the task to a group of vehicles. This choice of design is to safeguard the scheme against collusion attack and retain accountability.

6. **Identity-based Public Key Cryptography.**

   In identity-based public key cryptography (ID-PKC), the public key of a user is some unique information associated to its identity, such as their email address or phone number. The direct derivation of its public key in ID-PKC eliminates the

necessity of certificates. However, its inherent problem is that it suffers the key escrow problem. A trusted party, commonly known as the key generator center (KGC) has access to a user's private key as it manages and distributes users' private keys in the system.

3.4 Reviews of Trust- and Reputation-based Models

In this section, we review some recent trust- and reputation-based system for a secure anonymous announcement scheme in VANETs. We extract the essence of their work and summarize them.

3.4.1 Schemes based on Trust and Reputation Models

Mármol et al. [72] proposed a trust and reputation infrastructure-based protocol for VANETs called TRIP. In their scheme, a vehicle generates a message and broadcast it to neighboring vehicles. To evaluate the reliability of the message, the receiving vehicle V_r computes the reputation score of the sending vehicle V_s. The reputation score is the combination of three different sources; its direct previous experience with the sending vehicle, recommendation by surrounding vehicles, and recommendation from the trusted party. For instance, the roadside unit who maintains a database of malicious vehicles in the network. The results of the reputation score will assist the V_r to determine whether a V_s vehicle is untrustworthy, partially trusted or fully trusted. In order for a reputation score to be computed, the proposed scheme requires communication with the trusted party and neighboring vehicles to obtain their recommendation about V_s. This may not be ideal for a time-constraint safety application in VANETs. Furthermore, it requires a vehicle to establish a long term relationship, which may not be feasible in a fast moving and large scale of VANETs. A vehicle is also required to store its past encounters with other vehicles. This may lead to a storage problem. It also does not address details of the scheme main operations such as the initialisation phase, message announcement and verification, and revocation of misbehaved vehicles.

The schemes proposed in [38, 73, 84, 99] adopted a decentralised infrastructure. In [38], Dötzer et al. proposed a reputation model using an approach called *opinion piggybacking*. Upon receiving a message, each receiving vehicle appends its opinion about the reliability of the message before it forwards the message to neighboring vehicles. The opinion may be based on the content of the message or previous aggregated opinions attached to the message. To generate an opinion, a receiving vehicle has to verify, compute and aggregate all previous opinions appended to the message. This may cause significant computational burden on receiving vehicles. Issues of revocation and robustness against possible collusion of adversaries were also not addressed. In addition, details of implementation such as the initialisation of the reputation system and the update of reputation score of vehicles were not discussed.

A multifaceted trust modelling framework for VANETs was developed by Minhas et al. in [73]. The scheme employs three variation of trust models to evaluate the reliability of a message: *role-based trust*, *majority-based trust* and *experience-based trust*. *Role-based* trust assumes vehicles with certain predefined role, such as the traffic patrol or law enforcing authorities, have higher trust value compared to other vehicles. Each vehicle possesses a certificate from a trusted authority, for identification and authentication purposes. Meanwhile, *majority-based* trust is similar to the threshold method. In *experience-based* trust, the trustworthiness of a vehicle is evaluated based on how truthful they were in their past direct interaction. Such a model requires a vehicle to establish long term relationship with other vehicles. Similar to the problem encounter in [72], this may not be practical in a large VANET environment. This also implies that a vehicle is required to store information of other vehicles encountered in the past, which may cause storage problem. A similar approach of experience-based trust was proposed by Patwardhan et al. in [84].

In [65, 70], a centralised reputation-based announcement scheme for VANETs was proposed. The reliability of a message is evaluated based on the *reputation* of the vehicle who generates the message. A message is considered reliable if the message generator has sufficiently high reputation. The reputation of a vehicle reflects the extend it has broadcasted reliable messages in the past. It is computed and updated by means of a feedback mechanism. A feedback report consists of a numerical score, which represents a receivers evaluation of the reliability of the relevant message. The

reputation score of all vehicles are managed and certified by a trusted party. During a message broadcast, a vehicle attaches its reputation certificate to the message it intends to announce, which allows a receiving vehicle to determine the reliability of the message. A misbehaved vehicle whose reputation score decreases to 0 will be revoke from the system by the trusted party who no longer provides it with new reputation certificate in the future. These schemes are computationally efficient as evaluation of message reliability only requires a receiving vehicle to verify one signature provided that the message generator has sufficient high reputation. This will allow a vehicle to make a decision quickly and act on the message received.

3.4.2 Schemes based on Network Modelling

Golle et al. [45] and Schmidt et al. [99] proposed the evaluation of message reliability by modelling the network. In [45], a scheme that allows vehicles to detect and correct malicious messages in VANETs was proposed. Vehicles are assumes to maintain a "model" of the VANET where it contains all the knowledge that the vehicle possess about the VANET. The vehicle can then compare the messages received against the model of the VANET. A message which is consistent and agrees with the vehicles model is likely to be accepted as valid. Inconsistent messages is addressed by a heuristic approach termed adversarial parsimony. The parsimony assumes a small fraction of adversaries is more likely than a large number of colluding vehicles. A vehicle will search for explanantions for the inconsistent messages based on the possible presence of malicious vehicles and rank all possible explanations according with the parsimony heuristic. The message with the highest scoring explanation will be validated. However, a strong assumption is drawn where it requires vehicles to construct a model of the VANET. This requires vehicles to possess a wide knowledge of the network, which may be infeasible and render the scheme to be impractical.

Schmidt et al. proposed a framework for vehicle behaviour analysis in [99]. The behaviour is referred to all observable information on a vehicle that includes its movement and position in the past, present and (predicting) future movements. Their scheme requires receiving vehicles to accumulate multiple messages from a vehicle that may provide sufficient information for behaviour analysis. The result of this analysis will

help to determine a vehicle as trustworthy, neutral or untrustworthy. In this approach, vehicles are required to make observations before a decision can be made. This may not be desirable in VANETs as vehicles are not able to act quickly upon the messages received and be aware of the situation ahead of them.

However, the schemes in [38, 45, 72, 73, 84, 99] does not address the matter of privacy. In addition, the issue associated with decentralised infrastructure for the schemes in [38, 45, 73, 84, 99] is that robustness is often not guaranteed.

3.5 Conclusion

In Section 3.4, we have reviewed and analysed some recent trust- and reputation-based announcement scheme in VANETs. While trust- and reputation-based system has been widely deployed in computer interactions [89], the application of this mechanism is still at a preliminary stage for an announcement scheme in VANETs. Our survey proves the lack of proposal in the area. Nevertheless, this implies there are more rooms for research and this is where our work steps in.

Chapter 4

Reputation-based VANETs

In this chapter we design a secure authenticated anonymous reputation-based announcement scheme. It allows evaluation of message reliability that is practical, efficient while preserving privacy of vehicles in the network.

Contents

4.1 Introduction

Mechanism for reputation system has been widely deployed in computer interactions (for example, e-commerce) that focused on building trust in specific entities over a series of interactions [89]. However, this existing notion of trust establishment is not suitable to be adopt in VANETs. This is because the large number of vehicles moving around and encountering each other perhaps only for a brief moments making it not possible to build a long term relationship with each other. This means that building reputation system for a large scale system is excessively complex.

In the thesis, we adopt reputation system for vehicular ad hoc network. For a message announcement scheme in VANETs, the reliability of a message is evaluated according to the *reputation* of the vehicle that generates this message. The reputation system computes the reputation score for an entity that allows evaluation of its trustworthiness to other entities. A message is considered reliable if the vehicle that generates the message has sufficiently high reputation. The reputation of a vehicle is represented by a numerical score. This reflects the extent to which the vehicle has announced reliable messages in the past. It is computed based on feedback reported by other vehicles. Feedback contains a numerical score representing the feedback-reporting vehicles evaluation of the reliability of the message. These feedback accumulate to a vehicle's reputation score. The score is collected, updated, and certified by a trusted party. The reputation score evolves, as time elapses, based on the reliability of messages that the vehicle announces. Vehicles tend to give positive feedback for reliable messages. This increases the reputation score. Meanwhile, a reputation score decreases when negative feedback is reported. Hence, short term encounter leads to a long term trust, represented by a vehicle's reputation score.

To determine the reliability of messages in VANETs, a majority of the announcement schemes in the literature such as [18, 24, 27, 28, 34, 35, 66, 92, 115] adopted the threshold method. In a threshold method, a message is likely to be reliable if it has been announced by a number of distinct vehicles within a time interval. However, as depicted in Table 3.1 in Section 3.3 of Chapter 3, it shows that most schemes [18, 27, 28, 34, 66, 92, 115] does not achieve message reliability. This is because distinguishability of message origin is not achieved, which is a prerequisite property for

the threshold method.

Another approach to evaluate the reliability of messages is trust- and reputation-based system. There have been several other announcement schemes based on reputation systems [38, 73, 84, 99]. However, these schemes does not provide a comprehensive construction that efficiently address the three security requirements for a secure announcement scheme. Discussion on robustness against colluding adversaries was also not included.

Our scheme do not rely on multiple messages to evaluate reliability. We also do not require distinguishability of message origin. Indeed our scheme only require a vehicle to verify one message, provided that the message reporter has sufficiently high reputation. Not only this is computationally efficient, this also enables a vehicle to quickly determine the reliability of the message, make decision accordingly and act upon the message.

4.2 The Reputation System

In [65], we proposed a robust reputation-based announcement scheme for VANETs that achieves message reliability and accountability. The reliability of a message is evaluated according to the reputation of the sending vehicle who announce the message. A message is consider to be reliable if the vehicle that generates the message has a sufficiently high reputation. The reputation of a vehicle reflects the extent to which the vehicle has announced reliable messages in the past, which may reflect the likelihood it will announce reliable messages in the future. A vehicle periodically retrieves its reputation credentials from a trusted party who certifies and manages the reputation scores of all vehicles in the system. A vehicle attaches its reputation credential when it announce a message, which will assist receiving vehicles to evaluate the reliability of the message based on its reputation score. A vehicle whose reputation score decreases below a certain threshold is revoke from the system by the trusted party who no longer provides it with new reputation credentials in the future. However, this scheme does not provide much privacy since the identities of all sending and reporting vehicles are made public. The provision of privacy in a reputation system is a nontrivial matter.

In this chapter, we provide an abstraction for a 3A scheme using reputation system based on [65]. We then construct a secure 3A scheme based on this abstraction that also provides privacy for vehicles.

The adoption of the reputation system in our schemes requires the installation of protocols and algorithms as follows.

- The Aggr. The Aggr algorithm is used by the RS to compute and update reputation scores for vehicles based on the feedback received. We will discuss it in more detail in Section 4.5.7.1;
- the TimeDiscount. The TimeDiscount is a non-increasing function that takes input a non-negative value representing a time difference, and output a number between 0 and 1. For example, it can be defined as:

$$\mathsf{TimeDiscount}(t) = \begin{cases} 1 - t/\Psi_{TD} & \text{if } t < \Psi_{TD}; \\ 0 & \text{if } t \geq \Psi_{TD}, \end{cases}$$

  where Ψ_{TD} is a positive constant. In our schemes, the TimeDiscount algorithm is used to determine the freshness of a vehicle's reputation score. We take the absolute value of the difference between the current time when a message is received and the time the reputation certificate was retrieved. This difference value is directly proportional to the freshness of the reputation certificate used. Larger difference value indicates older reputation certificate was used, which results in lower value of discounted reputation score. In a similar fashion, smaller difference value between these two times imply updated reputation certificate was used, which results in a higher value of discounted reputation score. A receiving vehicle will accept a message from a sending vehicle whose discounted reputation score is above $\Psi_{\mathtt{RS}}$, where $\Psi_{\mathtt{RS}}$ is a reputation threshold that deem whether a vehicle is reputable or not. The purpose to determine the freshness of a vehicle's reputation score is to prevent them from abusing the system. For instance, a vehicle may continue to announce messages using its old reputation credential with higher reputation score in order to avoid retrieving its latest reputation credentials that may have lower reputation score after knowingly misbehaved. The TimeDiscount is incorporated in the scheme to ensure that even if this is the case, the use of

old reputation score will results in a higher value of discounted reputation score;

- three configurable public parameters $\Psi_{\texttt{RS}}$, Ψ_t and $\mathbb{T}$. The parameter $\Psi_{\texttt{RS}}$ acts as a threshold and is used by a vehicle to determine whether or not another vehicle is reputable. It is a constant between 0 and 1. The parameter Ψ_t also acts as a threshold and used to determine whether or not a message tuple is sufficiently fresh for feedback reporting. Feedback needs to be generated within short period of time below the threshold Ψ_t. Any feedback generated after that will be considered invalid. This prevent attackers generating fake feedback after a while once they get hold of the message. The assumption is the message propagation is slow, so attackers can get a message after a while once it is broadcast. The parameter $\mathbb{T}$ is a large time interval, over which a *sufficiently large* number of vehicles report feedback relating to a vehicle. Large interval is to ensure there are sufficient number of feedback for most of vehicles. The system needs enough feedback to calculate accurate reputation. If the interval is too short, then there will not be many feedback. This may caused the reputation not be accurate.

4.3 Abstraction of a Reputation System Scheme

In this section, we present an abstract scheme for a reputation system. The network consists of vehicles as discussed in Section 2.1. In this abstract scheme, we rely on the presence of two fully trusted parties: a *reputation server* and a *management server*. Communication between entities is performed over two channels: a *secure* and a *public channel*. We define a secure channel, denoted by "$\longrightarrow$", that provides message authentication and confidentiality. Meanwhile, an authenticated and integrity protected channel is define as the public channel, denoted by "$\dashrightarrow$". The reputation server (RS) computes and aggregates feedback to produce reputation scores for vehicles. The management server (MS) is responsible for the distribution and management of identities and cryptographic credentials of the vehicles. They also collect feedback from vehicles. The MS is also responsible for revoking vehicles. A secure confidential communication takes place between the RS and the MS. Periodic communication takes place between the MS and vehicles for reputation score retrieval via the secure channel and for feedback reporting via the public channel. The MS does not need to be online otherwise.

We also assume that the MS is equipped with a secure clock. There is also an access point (AP) as the roadside unit. An AP is a physical device located at fixed locations. Such locations include along the highways, roads, intersections, roundabouts or traffic lights. An AP is equipped with at least a network device for short-range wireless communication. Access points are connected with the reputation server, acting as a communication interface between vehicles and the MS. The purpose of access points is to allow vehicles to communicate with the MS in a convenient and frequent manner.

We begin with the description of the *initialisation phase* of a reputation system scheme. We describe the initialisation phase of each entity accordingly as follows.

1. Management server (MS).
   (a) computation of system parameters params which is made available to all entities in the network;
   (b) issuance of cryptographic keys, referred to as credentials, to all entities in the network;
   (c) the MS creates a database;
   (d) installation of a secure authenticated anonymous announcement scheme 3A algorithm. The properties of 3A are described below:
      - the message m originate from a message generator V_s that possesses valid credentials issued by the MS;
      - the message m is integrity protected.

      A common 3A scheme is achieved using digital signature. The 3A is composed of sign3A() and verify3A() which can be used when a vehicle wishes to send and verify a message. We utilise 3A during message broadcast and feedback reporting phase;
   (e) installation of the Ψ_t and $\mathbb{T}$.
2. Reputation server (RS).
   (a) installation of the Aggr;
   (b) the RS maintains a database that stores a vehicle's reputation score. In our scheme, we assign that the initial reputation score of a new vehicle is zero.

This configuration often causes a bootstrapping problem in a reputation system, where a newcomer has difficulty establishing its reputation. However, in our scheme, a new vehicle with zero initial reputation score is still able to establish its reputation. This is because, although messages broadcast by the new vehicle will not be considered as reliable, the receiving vehicles are still able to report feedback for these messages. Gradually, the new vehicle will be able to establish its own reputation. It is also worth noting that assigning zero initial reputation score to a new vehicle, as described in our scheme, is conservative. The purpose of this is to discourage a vehicle with bad reputation from whitewashing its reputation by rejoining the system with a new identity. This is useful when the cost of rejoining the system with a new identity is negligible. However, in a VANET, it is often difficult or costly for a vehicle to reenter the system with a different identity. In this case, a new vehicle could be initialized with a positive reputation, thus alleviating the bootstrapping problem.

3. Vehicles.

   (a) Each vehicle is assigned with a unique identity $\texttt{ID}_V \in \{0,1\}^*$;

   (b) the MS installs 3A;

   (c) the MS installs TimeDiscount, $\Psi_{\texttt{RS}}$, and Ψ_t onto V;

   (d) generate and send credentials to be used by V.

The initialisation phase is conducted during registration phase but we do not include the description in Figure 4.1 as not to crowd the diagram.

4.4 Description of a Reputation System Scheme

The abstraction of a reputation system scheme is composed of the following phases.

1. **Registration Phase.**

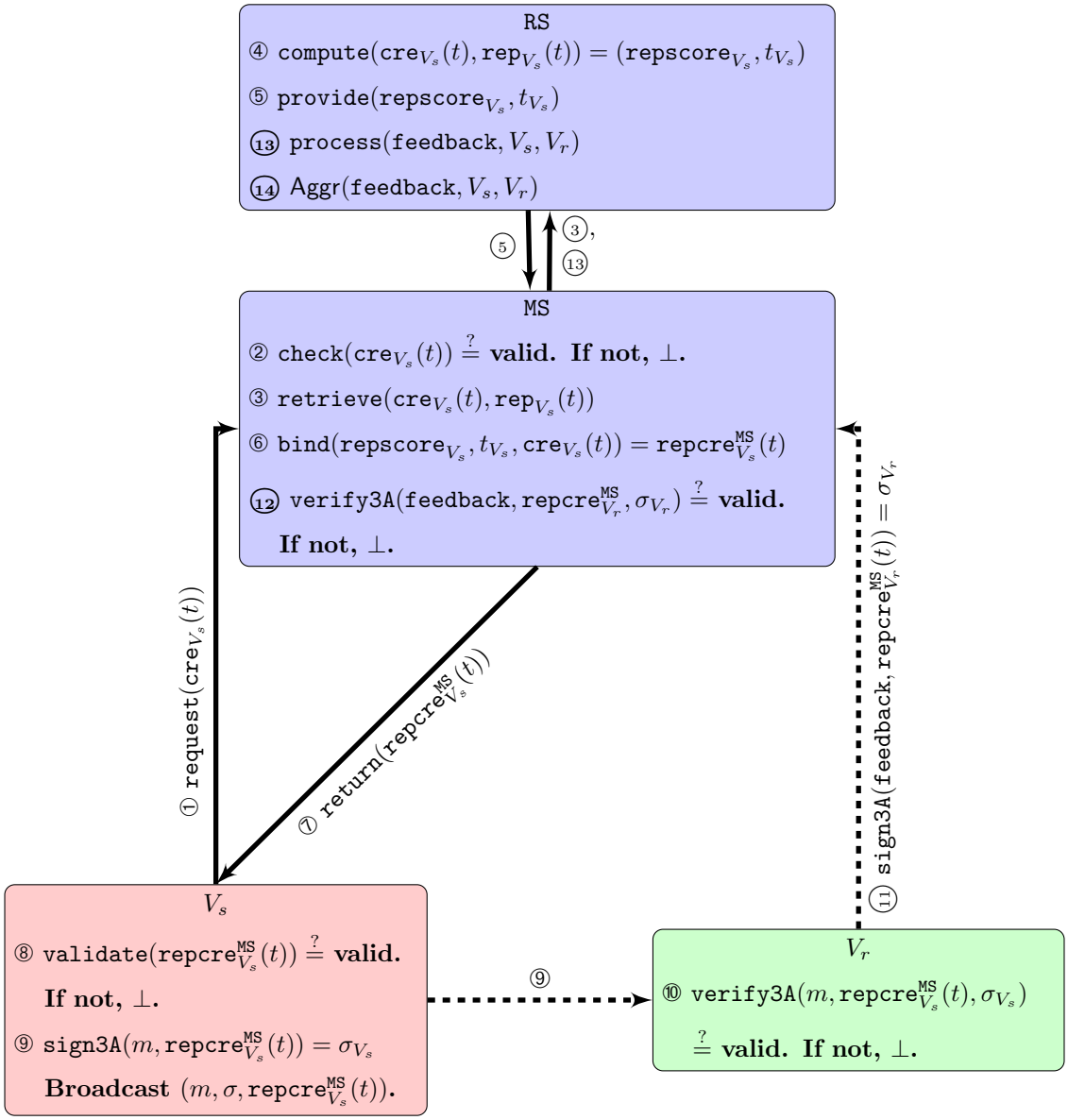

Figure 4.1: Abstraction of a Reputation System Scheme.

The registration of a new vehicle V_s is performed by the MS as follows.

Step ①. A V_s sends request for its reputation credentials $\texttt{request}(\texttt{cre}_{V_s}(t))$ at time t to join the network.

Step ②. The MS performs $\texttt{check}(\texttt{cre}_{V_s}(t)) = \texttt{check}(\texttt{ID}_{V_s})$. This ascertain that the request was sent unmodified from an unrevoked vehicle V_s. The request is denied otherwise.

Step ③. Upon success verification, the $\texttt{MS}$ acquire V_s's reputation score by sending the $\texttt{RS}$ $\texttt{retrieve}(\texttt{cre}_{V_s}(t), \texttt{rep}_{V_s}(t))$.

Step ④. The $\texttt{RS}$ generates reputation score for V_s by executing $\texttt{compute}(\texttt{cre}_{V_s}(t), \texttt{rep}_{V_s}(t)) = (\texttt{repscore}_{V_s}, t_{V_s})$ where $\texttt{repscore}_{V_s}$ denotes reputation score issued for V_s at time t_{V_s}.

Step ⑤. The $\texttt{RS}$ securely sends the $\texttt{MS}$ with V_s reputation information as requested by performing $\texttt{provide}(\texttt{repscore}_{V_s}, t_{V_s})$.

Step ⑥. The $\texttt{MS}$ ties $\texttt{cre}_{V_s}(t)$ to $(\texttt{repscore}_{V_s}, t_{V_s})$ by performing $\texttt{bind}(\texttt{repscore}_{V_s}, t_{V_s}, \texttt{cre}_{V_s}(t)) = \texttt{repcre}_{V_s}^{\texttt{MS}}(t)$ and creates a database for V_s that stores these information. The bind of V's reputation score to its credential essentially certifying that the authenticity and integrity of its reputation score is protected.

Step ⑦. The $\texttt{MS}$ performs $\texttt{return}(\texttt{repscore}_{V_s}^{\texttt{MS}}(t))$ that securely sends V_s with its reputation credentials.

Step ⑧. When V_s receives the credentials, it performs $\texttt{validate}(\texttt{repcre}_{V_s}^{\texttt{MS}}(t))$ that verifies $\texttt{repcre}_{V_s}^{\texttt{MS}}(t) = (\texttt{repscore}_{V_s}, t_{V_s}, \texttt{cre}_{V_s}(t))$ originate from the $\texttt{MS}$ and the content has not been tampered.

The registration phase is performed over a secure channel.

2. **Reputation Score Retrieval.**

   When V_s intend to retrieve its reputation credentials, Step ① to Step ⑧ described in Figure 4.1 is performed. The $\texttt{cre}_{V_s}$ used may be V_s long term key or previous reputation credential $\texttt{repcre}_{V_s}^{\texttt{MS}}$ obtained from $\texttt{MS}$.

3. **Broadcast Phase.**

   Step ⑨. When V_s wishes to announce a message, it takes a message associated with the event m and reputation credential $\texttt{repcre}_{V_s}^{\texttt{MS}}(t)$ as input to generate $\texttt{sign3A}(m, \texttt{repcre}_{V_s}^{\texttt{MS}}(t))$ and outputs a signature σ as below:

   $$V_s \rightarrow V_r : \texttt{sign3A}(m, \texttt{repcre}_{V_s}^{\texttt{MS}}(t)) = \sigma \text{ and send } (m, \sigma, \texttt{repcre}_{V_s}^{\texttt{MS}}(t)).$$

4. **Message Verification Phase.**

   Step ⑩. A V_r performs $\texttt{verify3A}(m, \texttt{repcre}_{V_s}^{\texttt{MS}}(t), \sigma)$ to verify the validity of the signature. It then compute the time-discounted reputation $\texttt{repscore}'_{V_s} = \texttt{repscore} \cdot \mathsf{TimeDiscount}(t_r - t_b)$, where t_r and t_b denotes time the message was

received and announced respectively. If $\texttt{repscore}'_{V_s} \geq \Psi$, then V_s is considered to be reputable.

5. **Feedback Reporting Phase.**

   Step (11) When V_r has its own experience about the event m announced by V_s, it would be able to judge the reliability of m and rate the experience it has encountered with V_s. It takes input `feedback` and its reputation credential $\texttt{repcre}^{\texttt{MS}}_{V_r}(t)$, where the `feedback` consist of it's feedback rate about V_s and associated information about V_s. It outputs a signature σ_{V_r} and sends $(\texttt{feedback}, \texttt{repcre}^{\texttt{MS}}_{V_r}(t), \sigma_{V_r})$ to the `MS`.

   Step (12) The `MS` then perform $\texttt{verify3A}(\texttt{feedback}, \texttt{repcre}^{\texttt{MS}}_{V_r}(t), \sigma_{V_r})$ that determines whether the feedback sent is valid or not.

   Step (13) Upon successful verification, the `MS` sends information associated to the feedback to be $\texttt{process}(\texttt{feedback}, V_s, V_r)$ to the `RS` to update V_s reputation score.

   Step (14) The `RS` uses Aggr that computes and updates V_s latest reputation.

6. **Revocation Phase.**

   A vehicle whose reputation decreases to 0 will be revoked from the system. The `MS` will stop issuing reputation credentials to malicious vehicles and therefore, would not be able to continue to participate in the network.

4.5 An Anonymous Authenticated Reputation-Based Announcement Scheme in VANETs

4.5.1 Scheme Overview

We propose a new authenticated anonymous announcement scheme in vehicular ad hoc networks (VANETs) based on techniques used in public key cryptography [92] and reputation system [65]. In [65], the scheme does not provide much privacy since the identities of all sending and reporting vehicles are made public. The provision of privacy in a reputation system is a nontrivial matter. Here, we present an extension to our previous work in [65] where the matter of privacy is addressed. To achieve privacy,

we uses randomly chosen anonymous public key bind to its reputation score, which is certified by the management server MS.

The management server MS initialises the system by installing a secure digital signature scheme DS, together with a secure signature scheme SS, a secret key encryption scheme SKE and a public key encryption scheme PKE. The MS computes and distribute its public system parameters to all entities in the network. The installation of the various schemes and associated keys onto vehicles is performed during the admission of vehicles into the network. Operation of the scheme composed of *setup*, *reputation score retrieval*, *message broadcast*, *message verification*, *feedback reporting*, *reputation update* and *revocation*.

To communicate in the network, a vehicle V periodically retrieves a set of anonymous reputation certificates from the MS via its nearest access point. The retrieval period varies, depends on how often a vehicle would like to obtain its latest reputation score or before it runs out of its certificates. A message signed with its reputation certificate attached satisfy the requirement of sender's authenticity and message integrity. Upon receiving a message, a receiving vehicle $V_r$verifies the message based on the validity of the signature and the reputation of V. A V_r may or may not provide a feedback about V. If it chooses to, V_r provides a feedback score to rate its experience with V and signs a feedback to report to the MS. The MS verifies the report based on V_r's signature and timing of the feedback reported. These information associated to the feedback is then sent to the reputation server RS who computes the latest reputation of V and updates its database. In our scheme, revocation is achieved without the need of an explicit revocation mechanism to address the issue of accountability. This is because the revocation technique is "embedded" within our scheme. Once a vehicle whose reputation score decreases to 0, the authority will no longer provides new reputation credentials. This is an act of revocation where these vehicles will not be able to participate in future communication in the network.

4.5.2 The Setup

We present the setup phase into two compartments: initialisation phase and registration phase. The initialisation phase is performed during registration phase but is not included in Figure 4.1 as not to crowd the diagram.

4.5.2.1 Initialisation Phase

The initialisation phase requires the installation of:

1. secure signature schemes, namely:
   (a) a secure digital signature scheme $\texttt{DS} = (\texttt{KGen}_{\texttt{DS}}, \texttt{DSsign}, \texttt{DSverify})$. We will use DS to realise a 3A;
   (b) a secure signature scheme, defined by $\texttt{SS} = (\texttt{KGen}_{\texttt{SS}}, \texttt{SSsign}, \texttt{SSverify})$ where $\texttt{KGen}_{\texttt{SS}}, \texttt{SSsign}$ and SSverify denotes key generation, signing and verifying operation for a signature scheme respectively. The SS is used to allow V_s to authenticate itself during reputation credential retrieval.

   We use two signature schemes because they will be used for different purposes and hence, different requirements for each scheme.
2. A secure symmetric key encryption scheme, defined by $\texttt{SKE} = (\texttt{KGen}_{\texttt{SKE}}, \texttt{SKEnc}, \texttt{SKDec})$ where $\texttt{KGen}_{\texttt{SKE}}, \texttt{SKEnc}$ and SKDec denotes symmetric key generation, encryption and decryption respectively.
3. A secure public key encryption scheme, defined by $\texttt{PKE} = (\texttt{KGen}_{\texttt{PKE}}, \texttt{PKEnc}, \texttt{PKDec})$ where $\texttt{KGen}_{\texttt{PKE}}, \texttt{PKEnc}$ and PKDec denotes public key generation, encryption and decryption respectively.

Each entity is then initialised as follows.

1. Management server (MS). In addition to Step 1e of the initialisation phase for the MS depicted in Section 4.1, the MS then runs:

   (a) the algorithm DSverify() to validate feedback reported by vehicles;

   (b) the $\mathtt{KGen}_{\mathtt{PKE}}$ to generate a key pair $(\mathtt{PK}_{\mathtt{MS}}, \mathtt{SK}_{\mathtt{MS}})$ used to encrypt and decrypt session keys (please refer to Section 4.5.3) ;

   (c) the $\mathtt{KGen}_{\mathtt{SS}}$ to generate a key pair $(\mathtt{pk}_{\mathtt{MS}}, \mathtt{sk}_{\mathtt{MS}})$ used to sign V long term keys;

   (d) selects another secure hash function $\mathcal{H} : \{0,1\}^n \rightarrow \mathbb{Z}_q^*$;

   (e) publishes $\mathtt{params} = \langle \mathcal{H}, \mathtt{PK}_{\mathtt{MS}}, \mathtt{pk}_{\mathtt{MS}} \rangle$.

2. Reputation server (RS). The RS is initialised as described in Section 4.1, which are as follows.

   (a) Installation of the Aggr;

   (b) the RS maintains a database that stores a vehicle's reputation score.

3. Vehicles. In addition to Step 3a and Step 3c of the initialisation phase for vehicles in Section 4.1, vehicles are initialised as follows.

   (a) The MS installs DS, SS, SKE and PKE schemes onto each vehicle V;

   (b) a V generates a pair of unique long term key pair (pk_V, sk_V) using $\mathtt{KGen}_{\mathtt{SS}}$. The authentication process to validate pk_V to the MS takes place during the V's registration before it is admitted into the system;

   (c) The MS creates a database that will store the following data for every vehicle in the system: a vehicle's identity $\mathtt{ID}_V$, a unique long term public key pk_V, a set of pseudonyms $\mathtt{pk}_V^i$, reputation scores $\mathtt{repscore}_V^i$, timestamps t_V^i on $(\mathtt{pk}_V^i, \mathtt{repscore}_V^i)$, and all feedback reported for the vehicle (see Section 4.5.6).

4.5.2.2 Registration Phase

Step ① A V sends a request to the MS for its reputation credentials and to authenticate its self-generated pk_V and a a set of pseudonyms $\mathtt{pk}_V^i$ $\mathtt{request}(\mathtt{ID}_V, pk_V, \mathtt{pk}_V^i)$. A pk_V is V self-generate credential associate to its identity $\mathtt{ID}_V$ assigned by the MS. Meanwhile,

$\mathtt{pk}_V^i$ is its set of pseudonyms generated by V, with its corresponding set of secret keys $\mathtt{sk}_V^i$, where these key pairs are generated using $\mathtt{KGen}_{\mathtt{DS}}$. To run this step, a V first generate a signature $\sigma = \mathtt{SSsign}_{sk_V}(\mathtt{ID}_V, pk_V, \mathtt{pk}_V^i)$ while keeping its corresponding secret key sk_V private. A random session key $\mathtt{skey}_V$ is generated using $\mathtt{KGen}_{\mathtt{SKE}}$ to encrypt the request $\mathtt{req}_V = \mathtt{SKEnc}_{\mathtt{skey}_V}(\mathtt{ID}_V, pk_V, \mathtt{pk}_V^i, \sigma)$. It encrypts the session key $\mathtt{key}_V = \mathtt{PKEnc}_{\mathtt{PK}_{\mathtt{MS}}}(\mathtt{skey}_V)$ and sends $\{\mathtt{req}_V; \mathtt{key}_V\}$ to the MS via the secure channel.

Step ② The MS $\mathtt{check}(\mathtt{ID}_V, pk_V, \mathtt{pk}_V^i)$ to authenticate V. To do this, it first decrypts $\mathtt{key}_V$ by using $\mathtt{PKDec}_{\mathtt{SK}_{\mathtt{MS}}}$. The session key obtained is used to decipher $\mathtt{req}_V$ using $\mathtt{SKDec}_{\mathtt{skey}_V}$. This will allow the MS to verify σ on $(\mathtt{ID}_V, pk_V, \mathtt{pk}_V^i)$ using SSverify.

Step ③ If the check succeed, the MS securely communicate with the RS to obtain V's reputation score by running $\mathtt{retrieve}(\mathtt{cre}_{V_s}(t), \mathtt{rep}_{V_s}(t))$.

Step ④ Upon receiving request from the MS, the RS $\mathtt{compute}(\mathtt{cre}_{V_s}(t), \mathtt{rep}_{V_s}(t)) = (\mathtt{repscore}_{V_s}, t_{V_s})$. The computation of $\mathtt{repscore}_V$ to be used at time beginning t_V^i is done by calculating $\mathtt{repscore}_V^i = \mathtt{repscore} \cdot \mathsf{TimeDiscount}(t_c - t_V^i)$, where t_c denotes the current time, until $\mathtt{repscore}_V^i$ goes below the reputation threshold $\Psi_{\mathtt{MS}}$.

Step ⑤ The RS performs $\mathtt{provide}(\mathtt{repscore}_{V_s}, t_{V_s})$ that sends back the generated reputation score to the MS.

Step ⑥ The MS ties the reputation score to V's credential by performing $\mathtt{bind}(\mathtt{repscore}_{V_s}, t_{V_s}, \mathtt{cre}_{V_s}(t)) = \mathtt{repcre}_{V_s}^{\mathtt{MS}}(t) = \mathtt{repcert}_{V_s}^i(t) = (\mathtt{pk}_{V_s}^i, \mathtt{repscore}_{V_s}^i, t_{V_s}^i, \mathtt{Cert}(\mathtt{pk}_{V_s}^i, \mathtt{repscore}_{V_s}^i, t_{V_s}^i))$. The certificate Cert() is a signature generated by the MS on the tuple $(\mathtt{pk}_{V_s}^i, \mathtt{repscore}_{V_s}^i, t_{V_s}^i)$. This essentially binds vehicle's reputation to its credential. The MS also generate a signature $\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V)$ that informed V that pk_V has been certified by the MS. The MS then creates a database that will store the following data for every vehicle in the system: a vehicle's identity $\mathtt{ID}_V$, a unique long term public key pk_V and a set of pseudonym $\mathtt{pseu}_V^i$ and its reputation score $\mathtt{repscore}_V^i$ issued to V.

Step ⑦ The MS encrypts $(\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), \mathtt{repcre}_V^{\mathtt{MS}}(t)) = (\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), \mathtt{repcert}_{V_s}^i(t))$ with the session key $\mathtt{skey}_V$ using the secret key encryption algorithm SKEnc and sends the ciphertext to V by running $\mathtt{return}(\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), \mathtt{repcert}_{V_s}^i(t))$ to V_s.

Step ⑧ A V decrypts the ciphertext acquired using $\texttt{SKDec}$ with $\texttt{skey}_V$. It then performs $\texttt{validate}(\sigma_{\texttt{sk}_{\texttt{MS}}}(pk_V), \texttt{repcert}^i_{V_s}(t))$, where $\sigma_{\texttt{sk}_{\texttt{MS}}}()$ is verified using $\texttt{pk}_{\texttt{MS}}$.

4.5.3 Reputation Score Retrieval

In this phase, a vehicle V retrieves from the $\texttt{MS}$ a set of its credentials $\texttt{repcre}^{\texttt{MS}}_V(t) = \texttt{repcert}^i_V(t) = \{(\texttt{pk}^i_V, \texttt{repscore}^i_V, t^i_V, \texttt{Cert}(\texttt{pk}^i_V, \texttt{repscore}^i_V, t^i_V)) : i = 1, \cdots, n\}$, where $\texttt{pk}^i_V$ is a random string, $\texttt{repscore}^i_V$ is a reputation score, t^i_V is a timestamp when $\texttt{repscore}^i_V$ were generated, and $\texttt{Cert}()$ is its corresponding certificate.

When it drives into the wireless communication range of an access point, the communication takes place as follow.

Step ① A V first generate a set of key pairs $(\texttt{pk}^i_V, \texttt{sk}^i_V)$ using $\texttt{KGen}_{\texttt{DS}}$. A request for reputation credentials is made by V by sending $\texttt{request}(pk_V, \texttt{pk}^i_V)$ to the $\texttt{MS}$. To identify itself to the $\texttt{MS}$, a V generate a signature $\sigma = \texttt{SSsign}_{sk_V}(pk_V, \texttt{pk}^i_V)$. A random session key $\texttt{skey}_V$ is generated using $\texttt{KGen}_{\texttt{SKE}}$ to encrypt the request $\texttt{req}_V = \texttt{SKEnc}_{\texttt{skey}_V}(pk_V, \texttt{pk}^i_V, \sigma)$. It encrypts the session key $\texttt{key}_V = \texttt{PKEnc}_{\texttt{PK}_{\texttt{MS}}}(\texttt{skey}_V)$ and sends $\{\texttt{req}_V; \texttt{key}_V\}$ to the $\texttt{MS}$ via the secure channel.

Step ② The $\texttt{MS}$ $\texttt{check}(pk_V, \texttt{pk}^i_V)$ to authenticate V. A V first decrypts $\texttt{key}_V$ by using $\texttt{PKDec}_{\texttt{SK}_{\texttt{MS}}}$. The session key obtained is used to decipher $\texttt{req}_V$ using $\texttt{SKDec}_{\texttt{skey}_V}$. This will allow the $\texttt{MS}$ to verify σ on $(pk_V, \texttt{pk}^i_V)$ using $\texttt{SSverify}$.

Step ③Upon successful verification, the $\texttt{MS}$ securely communicate with the $\texttt{RS}$ to obtain V's reputation score by running $\texttt{retrieve}(\texttt{cre}_{V_s}(t), \texttt{rep}_{V_s}(t))$.

Step ④ The $\texttt{RS}$ $\texttt{compute}(\texttt{cre}_{V_s}(t), \texttt{rep}_{V_s}(t)) = (\texttt{repscore}_{V_s}, t_{V_s})$ upon receiving request from the $\texttt{MS}$. The computation of $\texttt{repscore}_V$ to be used at time beginning t^i_V is done by calculating $\texttt{repscore}^i_V = \texttt{repscore} \cdot \mathsf{TimeDiscount}(t_c - t^i_V)$, where t_c denotes the current time, until $\texttt{repscore}^i_V$ goes below the reputation threshold $\Psi_{\texttt{MS}}$.

Step ⑤ The $\texttt{RS}$ runs $\texttt{provide}(\texttt{repscore}_{V_s}, t_{V_s})$ that sends back the generated reputation

score to the MS.

Step ⑥ The MS binds the reputation score to V's credential by performing $\texttt{bind}(\texttt{repscore}_{V_s}, t_{V_s}, \texttt{cre}_{V_s}(t)) = \texttt{repcre}_{V_s}^{\texttt{MS}}(t) = \texttt{repcert}_V^i(t) = (\texttt{pk}_V^i, \texttt{repscore}_V^i, t_V^i, \texttt{Cert}(\texttt{pk}_V^i, \texttt{repscore}_V^i, t_V^i))$.

Step ⑦ The MS encrypts $\texttt{repcre}_V^{\texttt{MS}}(t) = \texttt{repcert}_V^i(t) = \{\texttt{pk}_V^i, \texttt{repscore}_V^i, t_V^i, \texttt{Cert}(\texttt{pk}_V^i, \texttt{repscore}_V^i, t_V^i)\}$ with the session key $\texttt{skey}_V$ using the secret key encryption algorithm SKEnc and sends the ciphertext to V by running $\texttt{return}(\texttt{repcert}_V^i(t))$ to V_s.

Step ⑧ A V decrypts the ciphertext received using SKDec with $\texttt{skey}_V$. It then runs $\texttt{validate}(\texttt{repcert}_V^i(t))$. The secret keys are stored within a V's black box while the public keys and its corresponding certificates are kept within its onboard unit.

The retrieval period varies, depends on how often a vehicle would like to obtain its latest reputation score or before it runs out of keys. A vehicle is likely to retrieve its credentials when its time-discounted reputation value $\texttt{repscore}_V^i \cdot \mathsf{TimeDiscount}(t_c - t_V^i)$, where t_c denotes the current time, is approaching or below the reputation threshold $\Psi_{\texttt{MS}}$. There is a tradeoff between the frequency a vehicle retrieves its keys from the MS and the efficiency of the scheme. Long interval between retrieval period may be desirable as it may ease management to the MS who does not need to generate certificates for a vehicle frequently. However, it will lead to storage problem to a vehicle that needs to preload a lot of keys over a long period of time.

Meanwhile, a shorter interval between retrieval period solves the storage problem as a vehicle only needs to store fewer keys for a shorter time duration. It also provides a simpler means of revocation. Once it runs out of keys, a misbehaved vehicle would not be able to obtain the next set of certificates from the MS. However, it implies frequent interaction between the MS and a vehicle.

4.5.4 Broadcast Phase

An announcing vehicle, say V_s generates a road-related message $\texttt{msg}$ and broadcasts it to its neighbouring vehicles. This is described as follows.

1. V_s forms a $\texttt{MSG} = (h = \mathcal{H}(\texttt{msg}), t_b)$ where $h = \mathcal{H}(\texttt{msg})$ is a hash of the message and t_b is the time when the message was announced.
2. V_s perform Step ⑨ where the $\texttt{SSsign}()$ takes as input hash of the message $h = \mathcal{H}(\texttt{msg})$, the current time t_b and a user's signing key $\texttt{sk}^i_{V_s}$. It returns a signature θ_{V_s}.

$$\theta_{V_s} \leftarrow \texttt{DSsign}_{\texttt{sk}^i_{V_s}}(\mathcal{H}(\texttt{msg}), t_b)$$

3. V_s forms a *message tuple* $M = (\texttt{msg}, t_b, \theta_{V_s}, \texttt{repcert}^i_{V_s})$ and broadcasts M to its neighbouring vehicles.

4.5.5 Message Verification Phase

Upon receiving the message tuple M, a receiving vehicle, say V_r, performs the following procedure:

1. it determine whether it is interested in the message $\texttt{msg}$. If it is, it computes $h = \mathcal{H}(\texttt{msg})$;
2. V_r inputs θ_{V_s} into its trusted hardware. The trusted hardware retrieves the current time t_r from its embedded clock, and then stores the tuple (θ_{V_s}, t_r) within the trusted hardware. The trusted hardware outputs t_r to V_r.
3. V_r performs Step ⑩ where it first determines whether the broadcasting vehicle is reputable, that is, $\texttt{repscore}^i_{V_s} \cdot \mathsf{TimeDiscount}(t_r - t^i_{V_s}) \geq \Psi_{\texttt{MS}}$;
4. V_r then determines message freshness. A message is considered to be fresh if $t_r - t_b \leq \Psi_t$ where Ψ_t is very short time period after a sending vehicle announced a message.

5. whether the certificate $\texttt{Cert}()$ generated by the $\texttt{MS}$ is valid; and

6. V_r runs $\texttt{DSverify}(\texttt{msg}, t_b, \theta_{V_s}, \texttt{pk}^i_{V_s})$. If it returns **accept**, then the signature θ_{V_s} is considered valid. Otherwise V_r **rejects** the message.

The message $\texttt{msg}$ is considered reliable if all the above requirements are satisfied. The message tuple M is kept for future feedback reporting. If it does not fulfill the requirements, V_s is not considered as trustworthy and $\texttt{msg}$ is not considered as reliable and will not be taken into consideration. In the latter case, if Steps 1, 4 and 6 are positive, then the message tuple M is still stored for future feedback reporting. Otherwise it is discarded.

4.5.6 Feedback Reporting Phase

In this phase, when vehicle V_r, has its own experience about the event that the message $\texttt{msg}$ describe, it is able to judge the trustworthiness of the message. Then if V_r wants to report feedback to the reputation server, it performs Step (11) elaborated by the following procedures.

1. V_r generates a feedback rating $\texttt{feedrate} \in \{0, 1\}$ where $\texttt{feedrate} = 1$ if $\texttt{msg}$ is reliable and $\texttt{feedrate} = 0$ if $\texttt{msg}$ is not reliable.

2. V_r forms a $\texttt{feedback} = (\texttt{feedrate}, h, t_r, t_b, \theta_{V_s}, \texttt{pk}^i_{V_s})$.

3. V_r runs the $\texttt{DSsign}()$ that takes as input a $\texttt{feedback}$, a feedback reporter's signing key $\texttt{sk}^j_{V_r}$ and V_r's public key $\texttt{pk}^j_{V_r}$. It returns a signature θ_{V_r}.

$$\theta_{V_r} \leftarrow \texttt{DSsign}(\texttt{feedback}, \texttt{sk}^j_{V_r}, \texttt{pk}^j_{V_r})$$

4. V_r casts a $\texttt{feedback report} = (\texttt{feedback}, \theta_{V_r}, \texttt{repcert}^j_{V_r})$.

When V_r drives into the wireless communication range of a AP, it sends the $\texttt{feedback report}$ to the $\texttt{MS}$ via the AP.

4.5.7 Reputation Update Phase

In this phase, the reputation server updates the reputation score $\texttt{repscore}_{V_s}$ of vehicle V_s. The MS first verifies the feedback received from other vehicles as in Step ⑫. This is further elaborated as below.

1. it determine whether $t_r - t_b \leq \Psi_t$ where Ψ_t is small. This is performed to ensure that a receiving vehicle cannot forward this message to other colluding vehicles and together launch an attack to manipulate the reputation of the broadcasting vehicle;
2. runs $\texttt{DSverify}(\texttt{feedback}, \theta_{V_r}, \texttt{repcert}^j_{V_r})$. If it returns **accept**, then the signature θ_{V_r} is considered valid. Otherwise MS **rejects** the feedback.
3. runs $\texttt{DSverify}(\texttt{msg}, \theta_{V_s}, \texttt{repcert}^i_{V_s})$. If it returns **accept**, then the signature θ_{V_s} is considered valid. Otherwise MS **rejects** the feedback.
4. If the checks pass then the reputation server considers the `feedback report` as valid and stores it in the database.

The MS sends the RS $(\texttt{feedback}, V_s, V_r)$ to be processed to the RS as shown in Step ⑬, who stores these information into its database. The RS then execute Step ⑭ which applies the reputation aggregation algorithm Aggr (Section 4.5.7.1) on all stored feedback relating to V_s in order to compute the latest reputation score for vehicle V_s. It then replaces the previous reputation score in the database with its latest reputation score.

4.5.7.1 The Reputation Aggregation Algorithm

In this section, we describe the reputation aggregation algorithm Aggr from [65]. The Aggr computes the latest reputation score for a vehicle V based on all stored feedback, as follows:

1. The Aggr selects all feedback reported for V whose corresponding message tuple was broadcast from $\mathbb{T}$ time ago up to now. Any feedback whose corresponding message was broadcast earlier than $\mathbb{T}$ time ago is ignored, and deleted if necessary for data storage efficiency. We denote t_a as the time when this aggregation is running.

2. Multiple feedback reported by a vehicle V_z for V is aggregated into one intermediate value $\hat{r}_{V_z}$. Let $\mathcal{F}_{V_z}$ denote the set of feedback reported by V_z for V and whose corresponding message was broadcast from $\mathbb{T}$ time ago up to now. Each entry in $\mathcal{F}_{V_z}$ has feedback rating $\texttt{feedrate}_b$ corresponds to the message broadcasted at time t_b. The value $\hat{r}_{V_z}$ is aggregated using weighted average as follows:

$$\hat{r}_{V_z} = \frac{\sum\limits_{\texttt{feedback} \in \mathcal{F}_{V_z}} \texttt{feedrate}_b \cdot \big(\mathbb{T} - (t_a - t_b)\big)}{\sum\limits_{\texttt{feedback} \in \mathcal{F}_{V_z}} \big(\mathbb{T} - (t_a - t_b)\big)}. \tag{4.1}$$

   This gives more recent feedback a greater weight than less recent feedback. Let $\mathcal{V}$ denote the set of vehicles that each has reported at least one feedback for V in the past $\mathbb{T}$ time. The value $\hat{r}_{V_z}$ is computed for each vehicle $V_z \in \mathcal{V}$.

3. Let $\mathcal{V}^-$ denote the set of vehicles reporting at least one negative feedback for V in the past $\mathbb{T}$ time. The latest reputation score $\texttt{repscore}_V$ is computed as follows:

$$\texttt{repscore}_V = \begin{cases} \frac{\sum\limits_{V_z \in \mathcal{V}} \hat{r}_{V_z}}{|\mathcal{V}|} & \text{if } |\mathcal{V}^-| < \Psi_{nf}; \\ 0 & \text{otherwise,} \end{cases} \tag{4.2}$$

   where Ψ_{nf} is a configurable public parameter. The intuition of this equation is that $\texttt{repscore}_V$ is computed as the average of $\hat{r}_{V_z}$ if not too many vehicles reported negative feedback for V in the past $\mathbb{T}$ time; otherise $\texttt{repscore}_V$ decreases to 0, indicating that V has conducted message fraud attack.

4.5.8 Revocation Phase

A vehicle whose reputation score decreases to 0 will be revoked from the system. If a vehicle is revoked, the MS will stop issuing its reputation certificates. Feedback reported by the revoked vehicle will also not be considered as valid. We note that the previously

issued reputation certificate will gradually expire as time elapses. A misbehaved vehicle would then not be able to participate in future communication in the network.

4.6 Analysis

In this section, our scheme is compared with threshold schemes, which have been the mainstream announcement schemes. We first compare the security of our scheme with pseudonymous public key (PPK) [92] and TAA [24]. We then evaluate and compare the performance of these schemes in terms of communication cost, computational cost of signing and verifying a signature, signature length and storage cost.

4.6.1 Security Analysis

We compare the schemes based on three main security requirements of reliability, privacy and accountability. These are further divided into eight security requirements as discussed in Section 2.3. We summarised our finding in Table 4.1 below.

4.6.1.1 Reliability

In all three schemes, the property of sender authenticity and message integrity are satisfied, provided that the digital signature schemes used are secure. This also applies for feedback reporting phase where reporter authenticity and report integrity are assured provided that the digital signature used are secure. The signature, public and symmetric key encryption used during reputation score retrieval phase in Section 4.5.3 are also required to be secure. This will enable the `MS` to issue the correct credentials after proven the authenticity of a requesting vehicle.

Message truthfulness is not achieved in PPK as a receiving vehicle could not distinguish the origin of the message. Hence a threshold method could not be adopted. In TAA, a misbehaved vehicle who attempt to sign two messages of the same content can be

detected, as these two signatures can be linked to each other. This allows a receiving vehicle to distinguish the origin of messages, and therefore, allows the adoption of the threshold method. In our scheme, a message is considered truthful provided that the message generator has sufficiently high reputation. To lie successfully, an adversary may attempt to manipulate the content of an announcement (message fraud) or it manipulate the reputation score of the sending vehicle.

To evaluate the robustness of our scheme against message fraud, neither an external or internal adversary can modify the content of a message if the digital schemes used are secure. On the other hand, an internal adversary whose reputation is greater than the threshold $\Psi_{\texttt{MS}}$ may be able to deceive neighbouring vehicles into accepting a fake message as valid. However, if it persistently broadcast false messages over a long time period, then the negative feedbacks reported with respect to the announced event will decreases its reputation score. If it continues to act maliciously, this will results in its reputation score decreasing to 0 and thus, it will be revoked from the system.

With respect to robustness against reputation manipulation, our scheme is secure against external adversary. An external adversary who attempt to perform reputation manipulation attack may be motivated to impersonate as a legitimate vehicle V_r to forge and report a feedback for a target vehicle V_t with its own choice of feedback score. However, an external adversary who is not in the possession of a valid credentials would not be able to generate a valid signature as the secret key is determined by the feedback reporter's public key. Meanwhile, an internal adversary performing reputation manipulation may intentionally report a fake feedback upon receiving a message M from a target vehicle V_t. An internal adversary who acts on its own can only report a false feedback for each announced event by V_t. However, this only has a small impact on V_t's reputation score. In the worst case, it collude with a group of adversaries to magnify the impact on V_t's reputation score. However, the impact on V_t's reputation score remain small if the number of colluding adversaries are small relative to the number of all vehicles that have reported at least one feedback related to V_t.

4.6.1.2 Privacy

Anonymity is satisfied in all schemes. In TAA, the group signature allows the group member to sign on behalf of the group without the ability to tell who produced the signature. The use of randomly chosen public keys that does not contain any identifying information associating it to its user, also known as pseudonyms, allow anonymous communication in PPK. In our scheme, this is similar for message broadcast and feedback reporting phase. Communication during reputation score retrieval is guarded by means of signature and encryption. A vehicle and its credentials remain anonymous provided that these schemes are secure. Therefore, anonymity is satisfied in reputation score retrieval, message announcement and feedback reporting phase.

Only TAA achieves complete unlinkability. In our scheme and PPK, pseudonyms technique adopted allows messages to be linkable over its short lifetime. We call this partial unlinkability, denoted by a "✓*" in Table 4.1. This applies to both message announcement and feedback reporting phase in our scheme. This is a tradeoff between privacy and storage and communication cost. However, the lifetime of a pseudonym can be adjusted corresponds to the level of privacy required. Communication during reputation score retrieval phase is also unlinkable using the public and symmetric key encryption schemes, provided that these schemes are secure.

4.6.1.3 Accountability

All schemes addresses the issue of revocation. In PPK, the `TP` maintain a pseudo-identity mapping that will assist it to find the matching identity of misbehaved vehicles in its huge database. In our scheme, the `MS` revokes malicious vehicles by no longer providing them with their reputation credentials in the future. In TAA, a verifier must check against a list of compromised vehicles to determine whether the message generator has been revoked or not. Message verification takes longer as the revocation list grows. To avoid the inefficiency of long revocation list, a permanent revocation mechanism was proposed. The `TP`'s key pairs and vehicles' credentials are updated. Vehicles to be revoked will not have their credential updated and hence their signature will be able to be verified correctly under the new `TP`'s public key.

Traceability is fulfilled in all schemes. In PPK and our scheme, a vehicle is traceable via the database maintained by the TP. In TAA [24], a misbehaved vehicle who attempt to sign messages of the same content more than once can be traced and its identity can be revealed.

The requirement of non-repudiation is not satisfied in PPK. The TP is responsible for the generation of secret keys for vehicles in the system. Hence, non-repudiation is not achieved as the vehicle is not the sole holder of the secret key. In TAA, the TP do not possess the knowledge of the secret f, which is an important element of the signing key. In addition, a challenge-response protocol was also proposed to assure a receiving vehicle that the sending vehicle is indeed the message generator. Our scheme provide non-repudiation as vehicles self-generate their own secret keys, and thereby, the sole holder of the signing key.

Security Analysis				
Security goals	Security components	PPK [92]	TAA [24]	Our scheme
Reliability	Sender's Authenticity	✓	✓	✓
	Message Integrity	✓	✓	✓
	Message truthfulness	×	✓	✓
Privacy	Anonymity	✓	✓	✓
	Unlinkability	✓*	✓	✓*
Accountability	Non-repudiation	×	✓	✓
	Revocation	✓	✓	✓
	Traceability	✓	✓	✓

Table 4.1: Comparison of security analysis

4.6.2 Performance Analysis

This section presents comparison of performance efficiency between our scheme with PPK [92] and TAA [24]. We choose to employ ECDSA (elliptic curve digital signature algorithm) [14, 52, 54] as the signature algorithm to sign messages in PPK and our scheme. We set security level $l = 80$ bits for message signatures and $l = 128$ bits for certificates in these schemes. We summarise our finding in Table 4.2 below.

Computational cost. We evaluate the computational cost of signature generation and verification in broadcast of message, as they are among the factors that determines the performance of a secure vehicle-generated announcement protocol. As observed in [23, 24], the two most expensive operations are multiplications in $\mathbb{G}_1$ and pairing evaluation, which we shall consider here. We compare the cost between our scheme with PPK [92] and TAA [24] for $t = 1$, as our scheme require only one message provided that the message generator has sufficiently high reputation.

A similar signature technique is adopted in PPK and our scheme, resulting in similar computational cost. In both schemes, the signing operation requires two scalar multiplications and the verification requires four scalar multiplications. Our scheme has additional operations where V_r may choose to provide a feedback to rate its experience with the message generator. In this case, the computational cost is that of a signature. The verification of feedback requires two signatures verifications. This is performed by the MS and can be done offline. In TAA, the signing operation requires nine scalar multiplications and one pairing operation. Meanwhile, the verification operation consume eight scalar multiplications and five pairing operations.

Signature length. The signature in our scheme and PPK is generated using elliptic curve digital signature algorithm (ECDSA)[14, 52, 54]. It comprises of two elements of $\mathbb{G}_1$. To provide a security level 2^{80}, we can set q to be 190-bit long and the element in $\mathbb{G}_1$ is 191-bit long by choosing an appropriate curve such as NIST curve [14]. Thus, the length of signature generated on a message is 48 bytes in our scheme and PPK. In TAA, the size of the signature comprise of seven elements of $\mathbb{G}_1$ and three elements of q. This results in the length of 238 bytes for a group signature in TAA.

Communication cost. An announcement message M in PPK consists of: $(\theta_{\mathtt{sk}}(\mathtt{msg}), \mathtt{msg}, \mathtt{cert}_{\mathtt{TP}}(\mathtt{pk}), \mathtt{pk}, t)$, which denotes signature generated on an announced message, a message announced, its certificate which essentially is the signature of the TP on a vehicle's public key, a vehicle's public key and a timestamp to specify signature generation time respectively. To provide a security level of 2^{80}, we can set q to be 190-bit long and the element in $\mathbb{G}_1$ is 191-bit long. According to [7] the size of safety messages

is 100 bytes and we choose 8 bytes for timestamp, using the unix 64-bit timestamp. Based on the implementation in [14, 60], the size of the public key is 25 bytes, message signature is 48 bytes and TP certificate is 64 bytes. Hence the length of the message in PPK is $L = 48 + 100 + 25 + 64 + 8 = 245$ bytes.

In our scheme, a message is composed of: $(\theta_{V_s}(\mathtt{msg}), \mathtt{msg}, \mathtt{pk}^i_{V_s}, \mathtt{Cert}(\mathtt{pk}^i_{V_s}, \mathtt{repscore}^i_{V_s}, t^i_{V_s}), \mathtt{repscore}^i_{V_s}, t^i_s, t_b)$, where $\theta_{V_s}(\mathtt{msg}), \mathtt{msg}, \mathtt{pk}^i_{V_s}, \mathtt{Cert}(), \mathtt{repscore}^i_{V_s}, t^i_s$ and t_b denotes a signature generated on an announced message, a message announced, a vehicle's public key, its certificate, its reputation score and a timestamp on the reputation score and message broadcasted respectively. The size of the public key is 25 bytes, message signature is 48 bytes and MS certificate is 64 bytes, each timestamp is of 8 bytes and reputation score of size 1 byte. Therefore the size of the message size is $L = 48 + 100 + 25 + 64 + 1 + 8 + 8 = 254$ bytes.

In TAA, a message consists of: $(\theta_{\mathtt{sk}}(\mathtt{msg}), \mathtt{msg}, t, \mathtt{group}_{\mathtt{ID}})$, where $\theta_{\mathtt{sk}}(\mathtt{msg})$ is the signature generated on the announced event, msg is the event anounced, t is the timestamp when the message was generated and the group ID ($\mathtt{group}_{\mathtt{ID}}$) is used to identify which group does the vehicle belongs to. The length of the signature is 238 bytes, the size of the message is 100 bytes, 2 bytes for the group ID and 8 bytes for the timestamp. Hence, the size of the message is $L = 238 + 100 + 2 + 8 = 348$ bytes.

Storage and Generation costs. We compute the storage and generation costs of preloading credentials in PPK and our scheme. We note that the TAA scheme does not require storage of credentials, hence is not included in this discussion. For each credential retrieval period, PPK preloads a large set of key pairs $(\mathtt{sk}, \mathtt{pk})$, its corresponding anonymous certificate $\mathtt{cert}_{\mathtt{TP}}(\mathtt{pk})$ onto each vehicle, for its usage over a long period of time (i.e. a year). The next retrieval may occur during periodical vehicle maintenance visits, for instance. The public and private key is 25 bytes and 24 bytes respectively, using ECDSA-192 and a TP certificate is 64 bytes using ECDSA-256. This sums up to storage space of $25 + 24 + 64 = 113$ bytes per key. If a vehicle uses his car 2 hours per day on average, as assumed in [91], where the lifetime of each key is one minute, then the number of required keys per year is approximately 43800. This amounts to storage space of 4.95 MBytes on each vehicle. Given the long credential period in PPK, we consider heaviest car usage of 8 hours per day to ensure each vehicle has sufficient

credentials until the next retrieval session. This would sum up to 19.80 MBytes storage cost.

In our scheme, a vehicle retrieves four credentials from the `MS`; a set of its certificates `Cert`(), pseudonyms `pk`, reputation scores `repscore` and timestamp on the reputation score t_s. The `Cert` is of 64 bytes, `pk` is of 25 bytes, `repscore` is of 1 bytes, and t_s is of 8 bytes. The sum of storage space is of $25 + 64 + 1 + 8 = 98$ bytes per key, which is more efficient as it is less compared to PPK for each key. The retrieval period in our scheme is shorter and flexible, depends on whether a vehicle would like to obtain its latest reputation score or when it runs out of credentials.

Performance Analysis					
Scheme	Communication cost	Sign	Verify	Sig. length	Storage cost
PPK	245 bytes	$2 \cdot \mathbb{G}_1$	$4 \cdot \mathbb{G}_1$	$2\|\mathbb{G}_1\|$	113 bytes/key
TAA	348 bytes	$9 \cdot \mathbb{G}_1 + 1 \cdot P$	$8 \cdot \mathbb{G}_1 + 5 \cdot P$	$7\|\mathbb{G}_1\| + 3\|q\|$	-
Ours	254 bytes	$2 \cdot \mathbb{G}_1$	$4 \cdot \mathbb{G}_1$	$2\|\mathbb{G}_1\|$	98 bytes/key

Table 4.2: Comparison of performance analysis

Regarding the network modelling approach [45, 99] and the trust- and reputation-based approaches [38, 73, 84] that were discussed in Chapter 2, these schemes are still at a conceptual level and lack technical details and performance evaluation. We thus cannot provide a detailed security performance comparison between our schemes and these schemes.

4.6.3 Simulation Evaluation

In this section, we show some simulation results to examine the efficiency and performance of the scheme proposed in this chapter. This is evaluated from the following aspects.

1. Message drop rates: the average that reliable messages are rejected by a receiving vehicle due to low reputation scores of the announcing vehicles.

2. The percentage of attack success, as this is important for security context.
3. Temporary unavailability of the reputation server: The average increase of message drop rate due to the temporary unavailability of the reputation server.
4. Temporary unavailability of access points: The average increase of message drop rate due to the temporary unavailability of some access points.

In order to fully estimate the real world implementation of vehicular network, we use an event-based real street map vehicular network simulator called GrooveNet [71]. The road network used in the simulations is an urban area chosen from the city of Pittsburgh, PA. This simulation makes use of the publicly available TIGER (Topologically Integrated Geographical Encoding and Referencing) database obtained from the U.S. Census Bureau [109].

The simulations were carried out with conditions and configurations in line with other studies in the literature, for example [36, 65, 89]. Since the reputation system deployed here is based on the previous work in [65], similar configurations and values of parameters were used in the simulations to standardize the results.

1. Access points are generated and populated randomly over the selected road network.
2. Vehicles are generated, populated randomly, and move in the selected road network. We consider the participation of legitimate vehicles who are in possession of valid credentials issued by the trusted party. Their mobility models are as follows: A vehicle follows the vehicle in front, and a vehicle moves at the speed limit of a street when it is leading on the street. Their trip models are as follows: a vehicle randomly moves until it is 10 km from its starting point; the vehicle then takes the shortest path back to the starting point and starts again along a different path.
3. Road events randomly occur in the road network throughout the experiment. The time that an event will last is set randomly from 1 to 120 s.
4. Each vehicle broadcasts periodic messages every 300 ms over a range of approximately 100 m, in line with the DSRC specification [40].

5. A vehicle broadcasts a message regarding an event that it experiences, along with its latest reputation certificate.

6. A message receiving vehicle determines whether it accepts the received message by evaluating the reputation of the broadcasting vehicle, as specified in Section 4.5.5. The reputation threshold parameter $\Psi_{\texttt{RS}}$ is set conservatively to 0.8. The time discount parameter Ψ_{TD} is set conservatively to 1 hour. Note that Ψ_{TD} in a real-world implementation should be much longer than 1 hour, perhaps a few days or even longer. The purpose of setting it to 1 hour is to make the effect of the time discount function more visible during the experiments as well as to make it in line with 30 minutes of experiment time.

7. A message receiving vehicle may report feedback if it later experiences the event described by the message within the time when the event still exists. The probability that the vehicle will report a feedback is set conservatively to 0.1.

8. When a vehicle moves into communication range of an access point, it retrieves and then updates its latest reputation certificate and reports all feedback that it has generated and not yet reported.

9. The reputation server updates the reputation of each vehicle based on feedback received from all vehicles and generates a new reputation certificate accordingly, as specified by Sections 4.5.7 and 4.5.7.1. The time interval $\mathbb{T}$ is set to 10 min. Note that $\mathbb{T}$ in a real-world implementation should be much longer than 10 min: perhaps weeks or even longer. The purpose of setting such a short time interval $\mathbb{T}$ in the experiments is, again, to make it in line with 30 min of experiment time.

4.6.3.1 Effects of the Credential Retrieval Period

In this experiment, we deployed 600 vehicles whom are uniformly assigned with reputation score of 0.6, 0.8 and 1.0 respectively. Figure 4.2 shows the simulation results of message drop rate with respect to the credential retrieval period. As seen from the graph, the result shows that the message drop increases as the retrieval period increases. This is reasonable since longer period between retrieval phase implies a higher discounted reputation score. As a result, vehicles tend to broadcast messages with less

"fresh" reputation certificates, and the reputation scores tend to be more discounted by receiving vehicles using the discount function TimeDiscount. This results in higher rejection of reliable messages and thus an increase in the message drop rate.

The reputation score of vehicles also impacts on the message drop rate. We observe a slight increase for vehicles whose reputation score is 0.8 and 1.0. Meanwhile, the message drop rate for vehicles whose reputation score is 0.6 is bigger. This is reasonable as the reputation threshold Ψ_{RS} is set to 0.8. Therefore, for vehicles whose reputation is below Ψ_{RS} will become lesser reputable than it already is due to its discounted reputation score as the credential retrieval period increases .

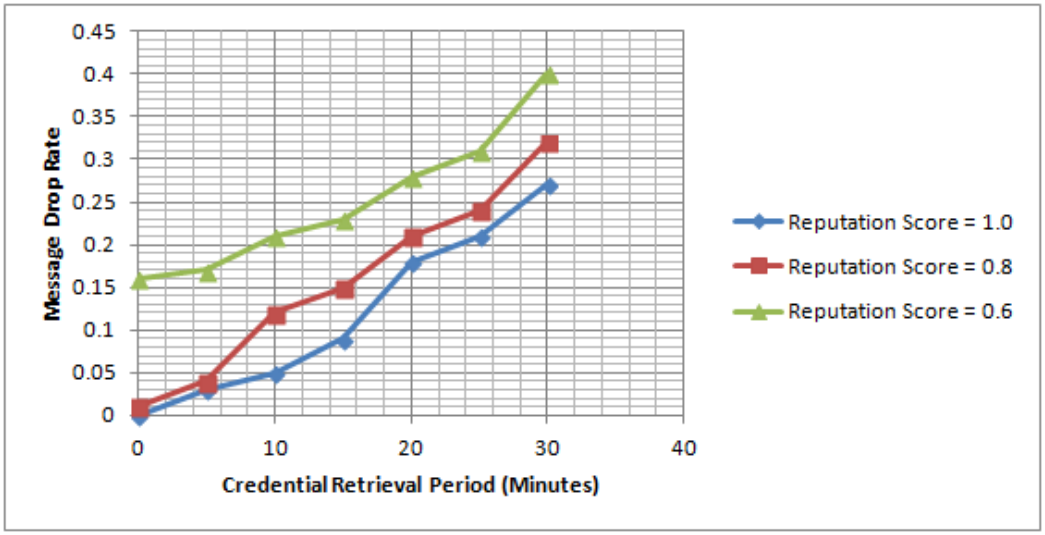

Figure 4.2: Effects of the Credential Retrieval Period

4.6.3.2 Effects of the Reputation Scores

Figure 4.3 shows the simulation results on the effects of the reputation score relative to the message drop rate. As seen from the graph, a decrease of message drop is observed as the reputation score of the announcing vehicle increases. This is natural as message broadcasted by vehicles with higher reputation is more likely to be reliable, hence decreases the message drop rate.

The density of vehicles also impacts on the message drop rate. We observe a decrease

of message drop rate when the density of vehicles increases. A modest but noticeable decrease is seen when the density of vehicles increases from 200 to 600 vehicles in the selected road network of 10 km^2. This is reasonable because more feedback tends to be reported for a vehicle in a vehicle-dense road network. Consequently, it is more likely that feedback whose corresponding message tuple was broadcast within the past $\mathbb{T}$ time is reported for a vehicle, and thus, a reputation certificate becomes available for the vehicle. This results in the reliable messages broadcast subsequently by the vehicle being accepted by the receiving vehicles, given that the broadcasting vehicle has a sufficiently high reputation score. Hence, we observe a decrease in the message drop rate.

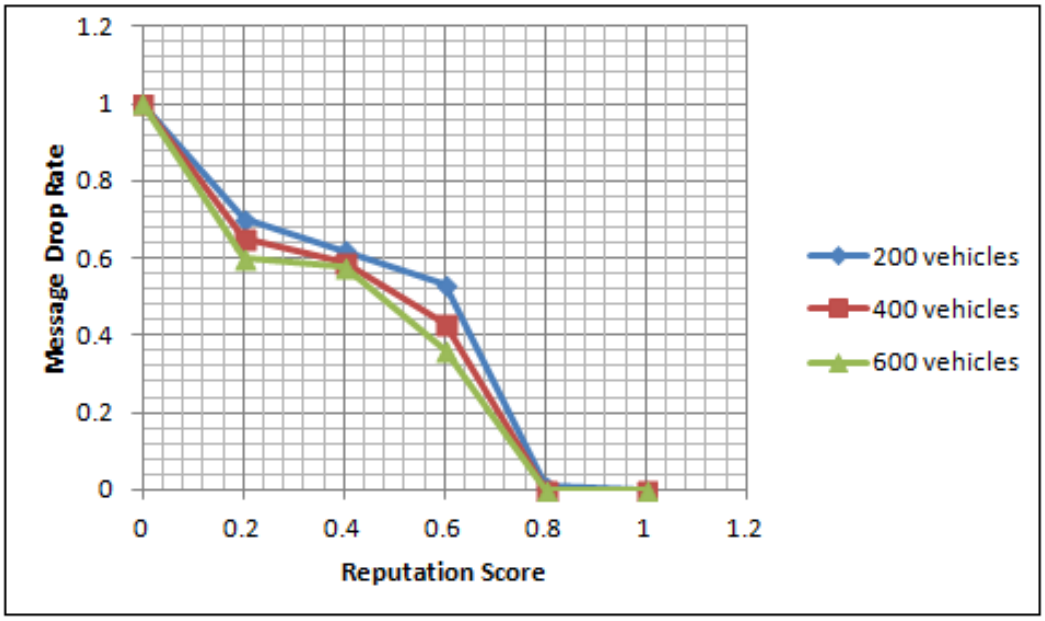

Figure 4.3: Effects of the Reputation Scores

4.6.3.3 Impact of Misbehaving Vehicles with Good Reputation Score

In Figure 4.4, we observe the impact of misbehaving vehicles with good reputation relative to the percentage of a success attack. In this scenario, we assume these misbehaved vehicles to conduct message fraud attack, where it broadcasted false information to neighbouring vehicles. We only consider this attack as a misbehaved vehicle with good reputation score has little impact to its target's vehicle reputation score if it acts

on itself. The impact of reputation manipulation attack is more obvious if these misbehaved vehicles act together in a group. We shall consider a reputation manipulation attack in the next experiment.

In this simulation, we deployed 600 vehicles who are uniformly assigned with a reputation score of 0.6, 0.8 and 1.0 respectively. The attack is 100% successful at $t = 0$ minutes for vehicles whose reputation score are 0.8 and 1.0. This is straightforward as an adversary with a time-discounted reputation score greater than $\Psi_{\mathtt{RS}}$ can deceive its neighboring vehicles into believing that a false message is reliable. If these vehicles continue to actively misbehaved, as time increases, the chances of an attack to be successful decreases. This is because the number of negative feedbacks reported for it will results in its reputation score decreasing, as shown in the graph.

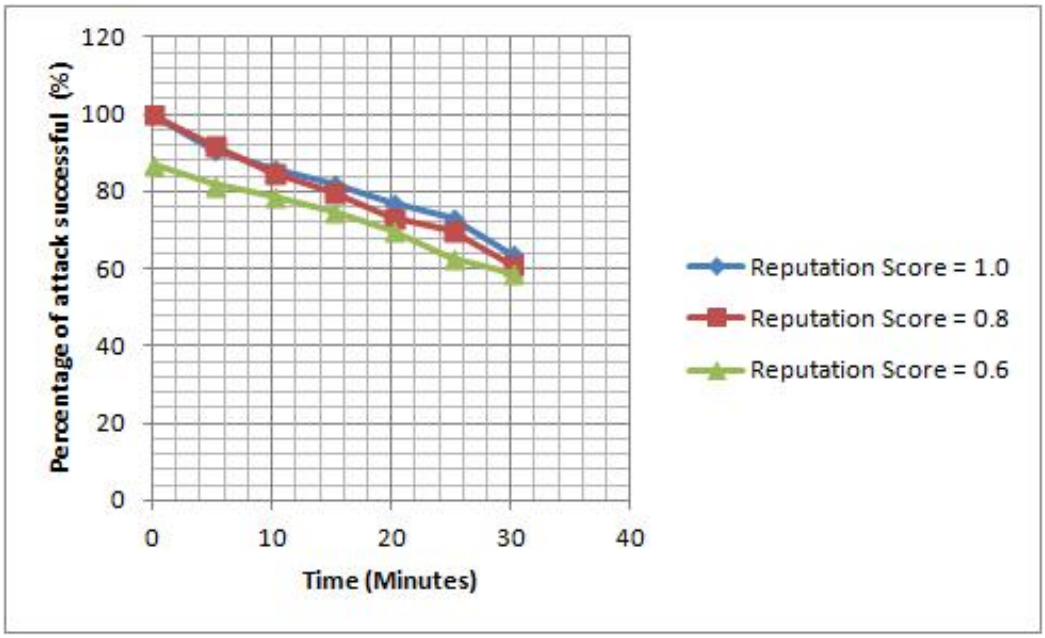

Figure 4.4: Impact of Misbehaving Vehicles with Good Reputation Score

4.6.3.4 Effects of Colluding Misbehaved Vehicles

In this experiment, we determine the effects of colluding misbehaved vehicles relative to the percentage of a success attack. As our scheme only require a vehicle to verify one message provided that the message generator has sufficiently high reputation, the

message fraud attack is not consider here. Rather, we focus on reputation manipulation attack. In this attack, an adversary unfairly inflates or deflates the reputation score of a target vehicle. This target vehicle can be the adversary itself. The attack has also more impact when it is performed in a group of colluding vehicles. Note that reputation manipulation may lead to message fraud, since an adversarial vehicle can get its reputation unfairly inflated by a reputation manipulation attack and only then launch a message fraud attack.

We consider the worst situation where all adversaries collude together to attack the same target vehicle with the same goal (to inflate or deflate the reputation score of a vehicle). If we set $\psi_t \leq 1.0\ s$ (ψ_t is denoted by t in the Figure 4.5), we observe that as the presence of colluding misbehaved vehicles increases, the percentage of an attack success increases as well. This is inevitable as the group of colluding vehicles increases and ψ_t increases (below the permitted threshold), it gives the colluding vehicles sufficient time to send a number of false feedback to manipulate its target vehicle's reputation score. This increases the percentage for an attack to be successful, as illustrated in the Figure 4.5.

If the number of adversaries is relatively small compared with the size of vehicles in the network, then the maximum unfair impact of internal adversaries conducting reputation manipulating attack is still small. In this case, the adversaries only adds a small noise into the reputation score of the target vehicle. It is reasonable to assume that in a VANET, there is only a small proportion of internal adversaries compared with the entire population of vehicles. This is consistent with the assumption we adopt in the thesis. Hence, the unfair impact of internal adversaries conducting reputation manipulating attack remains small.

4.6.3.5 Effect of temporary unavailability of `MS` and AP

The question of how usable the system is measured in terms of message drop rate and the effect of the availability of the `MS` and AP is demonstrated in simulation results in [65]. We will summarise the findings here (Section 4.6.3)and refer the reader to [65] for details.

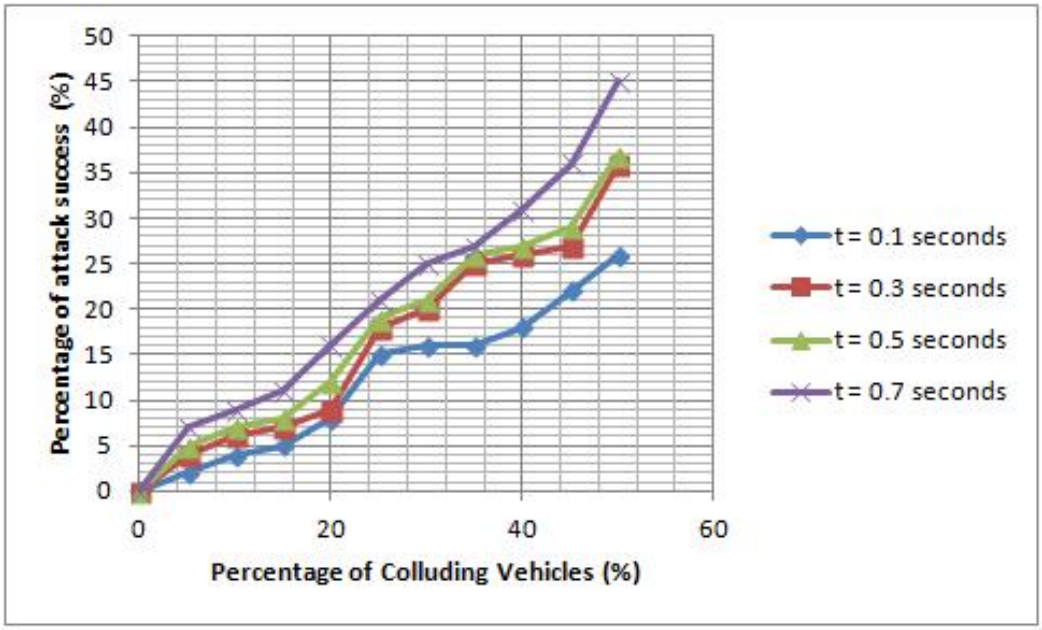

Figure 4.5: Effects of Colluding Misbehaved Vehicles

If MS and AP are all functioning continuously, the message drop rate depends (obviously) on the density of the vehicles and the density of APs. It appears that the message drop rates decreases drammatically when the density of AP is increased from very low. Subsequent increases have much smaller effect. For example, if there are 2 APs per km^2, the message drop rate is 0.1 if the density of vehicles is 500 per 10 km^2, while the message drop rate is less than 0.05 if there are 4 APs per km^2. This also confirms that even with initial reputation score of 0, a new vehicle will be able to establish its own reputation fairly reasonably. This is because a receiving vehicle may still provide a feedback even if it considered a message unreliable due to low reputation.

Temporary unavailability of MS. With 2 to 5 APs per km^2, the message drop rates increases proportionally as the length of unavailability of MS, until a certain point where the message drop rate is 1. This point is dependent upon the time discount parameter Ψ_{TD} and the reputation threshold $\Psi_{\texttt{MS}}$. If Ψ_{TD} and $\Psi_{\texttt{MS}}$ are set conservatively to 1 hour and 0.8 respectively (and the experiment time is only 30 minutes) then the message drop rate reaches 1 in 12 minutes. It is expected that in a real-world implementation with a much longer Ψ_{TD} the time to reach message drop rate 1 would be much longer.

Temporary unavailability of APs. The simulation result shows that for 5 APs per km^2 with the density of 500 vehicles per 10 km^2, even the unavailability of up to 50% of APs for 25 minutes contribute only slightly to the increase in message drop rate. Again, this is not unexpected, since a vehicle can always retrieve its reputation score and report feedback when it comes across another functioning AP.

4.7 Conclusion

In this chapter, we have presented an abstraction of a reputation system for a broadcast scenario in VANETs. Based on this construction, we presented a novel reputation-based announcement scheme for VANETs. We have shown that our scheme is robust, practical and efficient while satisfying the requirement of reliability, privacy and accountability.

Chapter 5

Certificateless-based VANETs

In this chapter, we construct two schemes using a certificateless signature scheme (CLS) based on (i) reputation systems and (ii) a threshold mechanism. The adoption of CLS does not require the use of certificates, which can be unwieldy in a large VANET environment, and yet does not have the inherent key escrow problem of identity-based signature. This allows for an efficient as well as secure and anonymous announcement scheme for VANETs.

Contents

5.1 Cryptographic Background

In this section, we review some fundamental background for a certificateless signature scheme.

5.1.1 Certificateless Cryptography

Public Key Cryptography. In public key cryptography (PKC), each user has a public and a private key. The private key is kept secret while the public key is published. A public key of a user is associated with the user by a certificate, that is, a signature of a trusted Certificate Authority (CA) on the public key. This allows the receiver to be sure that the public key that they have is the correct public key for the sender. A receiver who wants to use the public key must verify the corresponding certificate for the validity of the key. Hence, we require a public key infrastructure - a series of trusted third parties that can be relied upon to vouch for the connection between an identity and a particular public key. Inevitably this feature causes a CA to require a large amount of storage and computing time managing the certificates.

Identity-based Cryptography. To avoid the certificate management problem, Shamir [101] introduced the concept of identity-based public key cryptography (ID-PKC). The idea was then practically deployed by Boneh and Franklin in [12]. An identity-based scheme removes the need for a public key infrastructure by setting an entity's public key to be equal to its digital identity. A key generator center (KGC) generates the entity's

private key using a master secret. An inherent problem of ID-PKC is thus the "key escrow" problem: the KGC knows the user's private keys and has to be complete trusted.

Certificateless Cryptography. In 2003, Al-Riyami and Paterson [5] introduced the concept of certificateless public key cryptography (CL-PKC) which eliminates the use of certificates in PKC and solves the key escrow problem in ID-PKC. The basic idea of CL-PKC is that the user constructs a public/private key pair by combining a value generated by a TP using its master key with a random secret value generated by the user. We describe such a signature scheme in the next section.

5.1.2 A Certificateless Signature Scheme

5.1.2.1 Pairings and Computational Problems

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ and be an additive group and a multiplicative group, respectively, of the same prime order q. Let P denote a random generator of $\mathbb{G}_1$ and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ denote a bilinear map which is typically constructed by Weil or Tate pairing with properties:

1. Bilinearity: $e(Q, W + Z) = e(Q, W) \cdot e(Q, Z)$ and $e(Q + W, Z) = e(Q, Z) \cdot e(W, Z)$ $\forall\ Q, W, Z \in \mathbb{G}_1$. Consequently, we have $e(aP, bQ) = e(P, Q)^{ab}, \forall\ P, Q \in \mathbb{G}_1$ and $\forall a, b \in \mathbb{Z}_q^*$.
2. Non-degeneracy: $\exists\ P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
3. Computability: there exists an efficient algorithm to compute $e(aP, bQ)$ $\forall\ P, Q \in \mathbb{G}_1$.

We assume that the discrete logarithm problem (DLP) is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$. The DLP is defined as follows: Given a generator P of a cyclic additive group $\mathbb{G}$ with order q, and $Q \in \mathbb{G}^*$, find an integer $a \in \mathbb{Z}_q^*$ such that $Q = aP$. In addition, we assume the computational Diffie-Hellman problem (CDHP) in $\mathbb{G}_1$. The CDHP is defined as follows: Given a generator P of a cyclic additive group $\mathbb{G}$ with order q, and given (aP, bP) for unknown $a, b \in \mathbb{Z}_q^*$, compute abP.

5.1.2.2 Certificateless Signature Scheme

The certificateless signature scheme (CLS) from [117] initialises the system by running the set up algorithm $\texttt{CLSsetup}(1^k)$ where 1^k is a security parameter. $\texttt{CLSsetup}()$ chooses the groups $\langle \mathbb{G}_1, \mathbb{G}_2, e \rangle$, where $\mathbb{G}_1, \mathbb{G}_2$ are groups of prime order q and e is a bilinear pairing, $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. It also selects 3 cryptographic hash functions $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$, each of which maps from $\{0,1\}^*$ to $\mathbb{G}_1$. It chooses an integer $s \in_R \mathbb{Z}_q^*$ (where $s \in_R \mathbb{Z}_q^*$ denotes choosing an element s uniformly at random from the set $\mathbb{Z}_q^*$) as its master secret key. It sets $P_0 = s \cdot P \in \mathbb{G}_1$ as the master public key. $\texttt{CLSsetup}()$ outputs $\langle s, \texttt{CLSparams} = \langle \mathbb{G}_1, \mathbb{G}_2, e, q, P, P_0, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 \rangle \rangle$. The master secret key s is kept confidential while CLSparams is published as system parameters. From now on we will assume the availability of CLSparams in the description of the remaining protocols and algorithms.

During the enrolment of an entity V with an identifier $\texttt{ID}_V \in \{0,1\}^*$, the enrolment protocol $\texttt{CLSenrol}(\texttt{ID}_V)$ is performed by the TP and V in a secure environment. This protocol consists of two parts: $\texttt{CLSenrol}_{\texttt{TP}}(\texttt{ID}_V)$ and $\texttt{CLSenrol}_V(x_V)$ as below.

$\texttt{CLSenrol}(\texttt{ID}_V)$
- TP runs $\texttt{CLSenrol}_{\texttt{TP}}(\texttt{ID}_V)$
  - computes $Q_V = \mathcal{H}_1(\texttt{ID}_V)$;
  - computes $x_V = sQ_V$;
  - outputs a partial private key x_V.
- TP sends x_V securely to V.
- V runs $\texttt{CLSenrol}_V(x_V)$
  - selects a secret value $y_V \in_R \mathbb{Z}_q^*$;
  - sets $\texttt{sk}_V = (x_V, y_V)$;
  - sets $\texttt{pk}_V = y_V P$;
  - outputs $(\texttt{sk}_V, \texttt{pk}_V)$.

To sign and verify a message M, the singing and verifying algorithms, denoted by $\texttt{CLSsign}()$and $\texttt{CLSverify}()$ respectively, are performed as follows.

$\texttt{CLSsign}(M, \texttt{sk}_V = (x_V, y_V), \texttt{ID}_V, \texttt{pk}_V)$
computes $U = u \cdot P$ for $u \in_R \mathbb{Z}_q^*$;
sets $v = x_V + u \cdot \mathcal{H}_2(M, \texttt{ID}_V, \texttt{pk}_V, U) + y_V \cdot \mathcal{H}_3(M, \texttt{ID}_V, \texttt{pk}_V)$;
outputs signature $\theta_V = (U, v)$.

$\texttt{CLSverify}(M, (U, v), \texttt{ID}_V, \texttt{pk}_V)$
computes $Q_V = \mathcal{H}_1(\texttt{ID}_V)$;
checks if the equality $e(v, P) = e(Q_V, P)e(\mathcal{H}_2(M, \texttt{ID}_V, \texttt{pk}_V, U), U)e(\mathcal{H}_3(M, \texttt{ID}_V, \texttt{pk}_V), \texttt{pk}_V)$ holds. If it does, outputs **valid**, otherwise outputs $\perp$.

We will use this scheme $\texttt{CLS} = (\texttt{CLSsetup}, \texttt{CLSenrol}, \texttt{CLSsign}, \texttt{CLSverify})$ in our announcement scheme in Section 5.2.2.

5.2 A Certificateless Anonymous Authenticated Announcement Scheme in VANETs

5.2.1 Scheme Overview

The management server MS initialises the system by installing a secure certificateless signature scheme CLS adopted from [117], along with a secure signature scheme SS, a secret key encryption scheme SKE and a public key encryption scheme PKE. The MS generates and publishes system parameters to vehicles in the network. The installation of the various schemes and associated keys onto vehicles is conducted during the admission of vehicles into the network. Operation of the scheme consists of *setup*, *reputation score retrieval*, *message broadcast*, *message verification*, *feedback reporting*, *reputation update* and *revocation*.

To communicate in the network, a vehicle V periodically retrieves a set of credentials from the MS via its nearest access point. To announce a safety related message, V anonymously sign the message with its reputation score attached and broadcast to neighboring vehicles. Each signing key key is valid over a short period. A receiving vehicle V'verifies the message based on the validity of the signature and the reputation

of V. It may or may not provide a feedback about V. If it chooses to, V' provides a feedback score to rate its experience with V and signs a feedback to report to the MS. Upon receipt of the feedback, the MS validates the report based on V''s signature and timing of the feedback reported. These information associated to the feedback is then sent to the reputation server RS who computes the latest reputation of V and updates its database.

5.2.2 Scheme Operation

We describe our scheme by showing how reputation of a vehicle is formed, propagated, updated and utilised to determine the trustworthiness of vehicles. We note that the CLSsetup(), CLSenrol(), CLSsign() and CLSverify() used in this section has been presented in Section 5.1.2.2. We further note that the description of our scheme will be presented based on the abstraction of a reputation system discussed in Section 4.4 of Chapter 4.

The operation of the scheme consists of the following phases: *setup*, *reputation score retrieval*, *message broadcast*, *message verification*, *feedback reporting*, *reputation update* and *revocation*.

The *setup* phase composed of the setup of the reputation server (RS), management server (MS) and admission of new vehicles Vs into the network. Such setup include generation of required cryptographic keys, installation of algorithms, regulation of their clocks and creation of database that stores V's information. To communicate in the network, a vehicle V periodically retrieves its latest reputation credentials from the MS when it drives into the proximity of a wireless communication range. We call this a *reputation score retrieval* phase. A V then generates a set of its secret and public key pairs $(\mathtt{sk}_V, \mathtt{pk}_V)$ after receiving its reputation scores and partial keys from the MS. During a *message broadcast* phase, a sending vehicle V_s anonymously sign the message and attach its reputation score before announcing the message to neighboring vehicles. Upon receiving the message, a receiving vehicle V_r performs *message verification* check to determine the reliability of a message. When V_r has its own experience about the event described by the message, it is able to judge the reliability of the message and

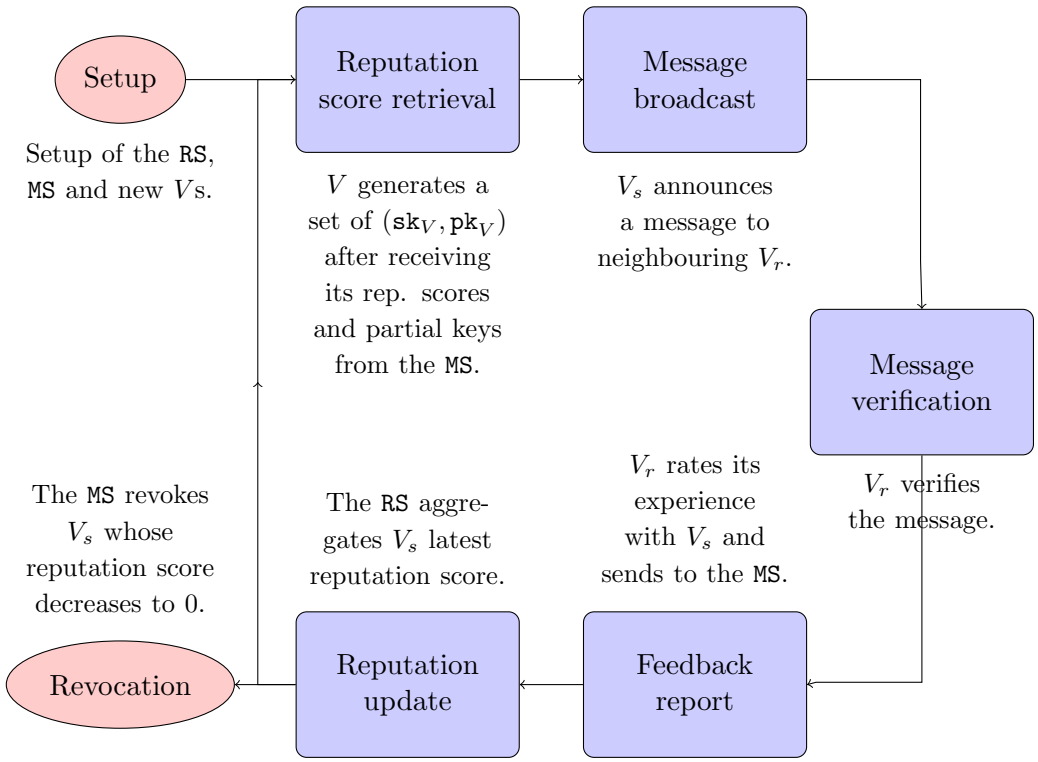

Figure 5.1: Flowchart of the scheme operation.

lodge a *feedback report* to the MS regarding its encounter with V_s. The validity of the feedback reported is determined before the RS aggregate and update the reputation score of V_s during the *reputation update* phase. A V repeats the cycle of retrieving its credentials to obtain its latest reputation score or when it needs to reload its credentials. Otherwise, it is *revoked* from the system by the MS if its reputation score decreases to 0.

5.2.3 The Setup

We present the setup phase into two compartments: initialisation phase and registration phase. The initialisation phase is performed during registration phase but is not included in Figure 4.1 as not to crowd the diagram.

5.2.3.1 Initialisation Phase

The initialisation phase requires the installation of:

1. a secure certficateless signature scheme $\texttt{CLS} = (\texttt{CLSsetup}, \texttt{CLSenrol}, \texttt{CLSsign}, \texttt{CLSverify})$ as described in Section 5.1.2.2. We will use CLS to realise a 3A.
2. a secure signature scheme, defined by $\texttt{SS} = (\texttt{KGen}_{\texttt{SS}}, \texttt{SSsign}, \texttt{SSverify})$ where $\texttt{KGen}_{\texttt{SS}}, \texttt{SSsign}$ and SSverify denotes key generation, signing and verifying operation for a signature scheme respectively.
3. a secure symmetric key encryption scheme, defined by $\texttt{SKE} = (\texttt{KGen}_{\texttt{SKE}}, \texttt{SKEnc}, \texttt{SKDec})$ where $\texttt{KGen}_{\texttt{SKE}}, \texttt{SKEnc}$ and SKDec denotes symmetric key generation, encryption and decryption respectively.
4. a secure public key encryption scheme, defined by $\texttt{PKE} = (\texttt{KGen}_{\texttt{PKE}}, \texttt{PKEnc}, \texttt{PKDec})$ where $\texttt{KGen}_{\texttt{PKE}}, \texttt{PKEnc}$ and PKDec denotes public key generation, encryption and decryption respectively.

Each entity is then initialised as follows.

1. Management server (MS). In addition to Step 1e of the initialisation phase for the MS depicted in Section 4.1, the MS then runs:
   (a) the algorithm $\texttt{CLSsetup}(1^k)$ as in section 5.1.2.2 to get $\langle s, \texttt{CLSparams} = \langle \mathbb{G}_1, \mathbb{G}_2, e, q, P, P_0, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 \rangle \rangle$;
   (b) the algorithm CLSenrol() to admit new vehicles into the system and the algorithm CLSverify() to validate feedback reported by vehicles;
   (c) the $\texttt{KGen}_{\texttt{PKE}}$ to generate a key pair $(\texttt{PK}_{\texttt{MS}}, \texttt{SK}_{\texttt{MS}})$ used to encrypt and decrypt session keys (please refer to Section 5.2.4) ;
   (d) the $\texttt{KGen}_{\texttt{SS}}$ to generate a key pair $(\texttt{pk}_{\texttt{MS}}, \texttt{sk}_{\texttt{MS}})$ used to sign V long term keys;
   (e) selects another secure hash function $\mathcal{H}_4 : \{0,1\}^n \rightarrow \mathbb{Z}_q^*$;
   (f) publishes $\texttt{params} = \langle \texttt{CLSparams}, \mathcal{H}_4, \texttt{PK}_{\texttt{MS}}, \texttt{pk}_{\texttt{MS}} \rangle$.

2. Reputation server (RS). The RS is initialised based on Step 2a and Step 2b of the initialisation phase for the reputation server in Section 4.3 of Chapter 4, which are as follows.

   (a) Installation of the Aggr;

   (b) the RS maintains a database that stores a vehicle's reputation score.

3. Vehicles. In addition to Step 3a and Step 3c of the initialisation phase for vehicles in Section 4.1, vehicles are initialised as follows.

   (a) The MS installs $\mathtt{CLS}, \mathtt{SS}, \mathtt{SKE}$ and PKE schemes onto each vehicle V;

   (b) A V generates a pair of unique long term key pair (pk_V, sk_V) using $\mathtt{KGen}_{\mathtt{SS}}$. The authentication process to validate pk_V to the MS takes place during the V's registration before it is admitted into the system;

   (c) The MS creates a database that will store the following data for every vehicle in the system: a vehicle's identity $\mathtt{ID}_V$, a unique long term public key pk_V, a set of pseudonyms $\mathtt{pseu}_V^i$, reputation scores $\mathtt{repscore}_V^i$, timestamps t_V^i on $(\mathtt{pseu}_V^i, \mathtt{repscore}_V^i)$, and all feedback reported for the vehicle (see Section 5.2.7).

5.2.3.2 Registration Phase

Step ① A V sends a request to the MS for its reputation credentials and to authenticate its self-generated pk_V $\mathtt{request}(\mathtt{ID}_V, pk_V)$. A pk_V is V self-generate credential associate to its identity $\mathtt{ID}_V$ assigned by the MS. This allows V to identify itself to the MS. To run this step, a V first generate a signature $\sigma = \mathtt{SSsign}_{sk_V}(\mathtt{ID}_V, pk_V)$ while keeping its corresponding secret key sk_V private. A random session key $\mathtt{skey}_V$ is generated using $\mathtt{KGen}_{\mathtt{SKE}}$ to encrypt the request $\mathtt{req}_V = \mathtt{SKEnc}_{\mathtt{skey}_V}(\mathtt{ID}_V, pk_V, \sigma)$. It encrypts the session key $\mathtt{key}_V = \mathtt{PKEnc}_{\mathtt{PK_{MS}}}(\mathtt{skey}_V)$ and sends $\{\mathtt{req}_V; \mathtt{key}_V\}$ to the MS via the secure channel.

Step ② The MS $\mathtt{check}(\mathtt{ID}_V, pk_V)$ to authenticate V. To do this, it first decrypts $\mathtt{key}_V$ by using $\mathtt{PKDec}_{\mathtt{SK_{MS}}}$. The session key obtained is used to decipher $\mathtt{req}_V$ using $\mathtt{SKDec}_{\mathtt{skey}_V}$. This will allow the MS to verify σ on $(\mathtt{ID}_V, pk_V)$ using SSverify.

Step ③ If the check succeed, the $\mathtt{MS}$ securely communicate with the $\mathtt{RS}$ to obtain V's reputation score by running $\mathtt{retrieve}(\mathtt{cre}_{V_s}(t), \mathtt{rep}_{V_s}(t))$.

Step ④ Upon receiving request from the $\mathtt{MS}$, the $\mathtt{RS}$ $\mathtt{compute}(\mathtt{cre}_{V_s}(t), \mathtt{rep}_{V_s}(t)) = (\mathtt{repscore}_{V_s}, t_{V_s})$. The computation of $\mathtt{repscore}_V^i$ to be used at time beginning t_V^i is done by calculating $\mathtt{repscore}_V^i = \mathtt{repscore} \cdot \mathsf{TimeDiscount}(t_c - t_V^i)$, where t_c denotes the current time, until $\mathtt{repscore}_V^i$ goes below the reputation threshold $\Psi_{\mathtt{MS}}$.

Step ⑤ The $\mathtt{RS}$ performs $\mathtt{provide}(\mathtt{repscore}_{V_s}, t_{V_s})$ that sends back the generated reputation score to the $\mathtt{MS}$.

Step ⑥ The $\mathtt{MS}$ ties the reputation score to V's credential by performing $\mathtt{bind}(\mathtt{repscore}_{V_s}, t_{V_s}, \mathtt{cre}_{V_s}(t)) = \mathtt{repcre}_{V_s}^{\mathtt{MS}}(t)$. To do this, the $\mathtt{MS}$ runs $\mathtt{CLSenrol}_{\mathtt{MS}}(\{\mathtt{pseu}_V^i, \mathtt{repscore}_V^i, t_V^i\})$ to obtain x_V^i for each i. This essentially binds vehicle's reputation to its credential. The $\mathtt{MS}$ also generate a signature $\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V)$ that informed V that pk_V has been certified by the $\mathtt{MS}$. The $\mathtt{MS}$ then creates a database that will store the following data for every vehicle in the system: a vehicle's identity $\mathtt{ID}_V$, a unique long term public key pk_V and a set of pseudonym $\mathtt{pseu}_V^i$ issued to V.

Step ⑦ The $\mathtt{MS}$ encrypts $(\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), \mathtt{repcre}_V^{\mathtt{MS}}(t)) = \{\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), (\mathtt{pseu}_V^i, \mathtt{repscore}_V^i, t_V^i, x_V^i)\}$ with the session key $\mathtt{skey}_V$ using the secret key encryption algorithm $\mathtt{SKEnc}$ and sends the ciphertext to V by running $\mathtt{return}(\mathtt{ID}_V, \sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), \mathtt{pseu}_V^i, \mathtt{repscore}_V^i, t_V^i, x_V^i)$ to V_s.

Step ⑧ A V decrypts the ciphertext acquired using $\mathtt{SKDec}$ with $\mathtt{skey}_V$. It then performs $\mathtt{validate}(\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V), \mathtt{pseu}_V^i, \mathtt{repscore}_V^i, t_V^i, x_V^i)$ where $\sigma_{\mathtt{sk}_{\mathtt{MS}}}(pk_V)$ is verified using $\mathtt{pk}_{\mathtt{MS}}$. It then runs $\mathtt{CLSenrol}_V(x_V^i)$ that generate its set of secret value y_V^i and compute a set of its key pairs $(\mathtt{pk}_V^i, \mathtt{sk}_V^i)$. The secret key is stored within a V's black box while the public key is kept within its onboard unit.

5.2.4 Reputation Score Retrieval

In this phase, a vehicle V retrieves from the $\texttt{MS}$ a set of its credentials $\texttt{repcre} = \{(\texttt{pseu}_V^i, \texttt{repscore}_V^i, t_V^i, x_V^i) : i = 1, \cdots, n\}$, where $\texttt{pseu}_V^i$ is a random string, $\texttt{repscore}_V^i$ is a reputation score, t_V^i is a timestamp when $(\texttt{pseu}_V^i, \texttt{repscore}_V^i)$ were generated, and x_V^i is a partial secret key.

When it drives into the wireless communication range of an access point, the communication takes place as follow.

Step ① A request for reputation credentials is made by V by sending $\texttt{request}(pk_V)$ to the $\texttt{MS}$. To identify itself to the $\texttt{MS}$, a V generate a signature $\sigma = \texttt{SSsign}_{sk_V}(pk_V)$. A random session key $\texttt{skey}_V$ is generated using $\texttt{KGen}_{\texttt{SKE}}$ to encrypt the request $\texttt{req}_V = \texttt{SKEnc}_{\texttt{skey}_V}(pk_V, \sigma)$. It encrypts the session key $\texttt{key}_V = \texttt{PKEnc}_{\texttt{PK}_{\texttt{MS}}}(\texttt{skey}_V)$ and sends $\{\texttt{req}_V; \texttt{key}_V\}$ to the $\texttt{MS}$ via the secure channel.

Step ② The $\texttt{MS}$ $\texttt{check}(\texttt{ID}_V, pk_V)$ to authenticate V. A V first decrypts $\texttt{key}_V$ by using $\texttt{PKDec}_{\texttt{SK}_{\texttt{MS}}}$. The session key obtained is used to decipher $\texttt{req}_V$ using $\texttt{SKDec}_{\texttt{skey}_V}$. This will allow the $\texttt{MS}$ to verify σ on $(\texttt{ID}_V, pk_V)$ using $\texttt{SSverify}$.

Step ③Upon successful verification, the $\texttt{MS}$ securely communicate with the $\texttt{RS}$ to obtain V's reputation score by running $\texttt{retrieve}(\texttt{cre}_{V_s}(t), \texttt{rep}_{V_s}(t))$.

Step ④ The $\texttt{RS}$ $\texttt{compute}(\texttt{cre}_{V_s}(t), \texttt{rep}_{V_s}(t)) = (\texttt{repscore}_{V_s}, t_{V_s})$ upon receiving request from the $\texttt{MS}$. The computation of $\texttt{repscore}_V^i$ to be used at time beginning t_V^i is done by calculating $\texttt{repscore}_V^i = \texttt{repscore} \cdot \mathsf{TimeDiscount}(t_c - t_V^i)$, where t_c denotes the current time, until $\texttt{repscore}_V^i$ goes below the reputation threshold $\Psi_{\texttt{MS}}$.

Step ⑤ The $\texttt{RS}$ runs $\texttt{provide}(\texttt{repscore}_{V_s}, t_{V_s})$ that sends back the generated reputation score to the $\texttt{MS}$.

Step ⑥ The $\texttt{MS}$ binds the reputation score to V's credential by performing $\texttt{bind}(\texttt{repscore}_{V_s}, t_{V_s}, \texttt{cre}_{V_s}(t)) = \texttt{repcre}_{V_s}^{\texttt{MS}}(t)$. To do this, the $\texttt{MS}$ runs $\texttt{CLSenrol}_{\texttt{MS}}(\{\texttt{pseu}_V^i, \texttt{repscore}_V^i, t_V^i\})$ to obtain x_V^i for each i.

Step ⑦ The MS encrypts $\texttt{repcre}_V^{\texttt{MS}}(t) = \{\texttt{pseu}_V^i, \texttt{repscore}_V^i, t_V^i, x_V^i\}$ with the session key $\texttt{skey}_V$ using the secret key encryption algorithm SKEnc and sends the ciphertext to V by running $\texttt{return}(\texttt{pseu}_V^i, \texttt{repscore}_V^i, t_V^i, x_V^i)$ to V_s.

Step ⑧ A V decrypts the ciphertext received using SKDec with $\texttt{skey}_V$. It then runs $\texttt{validate}(\texttt{pseu}_V^i, \texttt{repscore}_V^i, t_V^i, x_V^i)$. A V execute $\texttt{CLSenrol}_V(x_V^i)$ that generate its set of secret value y_V^i and compute a set of its key pairs $(\texttt{pk}_V^i, \texttt{sk}_V^i)$. The secret key is stored within a V's black box while the public key is kept within its onboard unit.

The retrieval period varies, depends on how often a vehicle would like to obtain its latest reputation score or before it runs out of keys. A vehicle is likely to retrieve its credentials when its time-discounted reputation value $\texttt{repscore}_V^i \cdot \mathsf{TimeDiscount}(t_c - t_V^i)$, where t_c denotes the current time, is approaching or below the reputation threshold $\Psi_{\texttt{RS}}$. There is a tradeoff between the frequency a vehicle retrieves its keys from the RS and the efficiency of the scheme. Long interval between retrieval period may be desirable as it may ease management to the MS who does not need to compute the keys for a vehicle frequently. However, it will lead to storage problem to a vehicle that needs to preload a lot of keys over a long period of time.

Meanwhile, a shorter interval between retrieval period solves the storage problem as a vehicle only needs to store fewer keys for a shorter time duration. It also provides a simpler means of revocation. Once it runs out of keys, a misbehaved vehicle would not be able to obtain the next set of keys from the MS. However, it implies frequent interaction between the MS and a vehicle.

5.2.5 Broadcast Phase

An announcing vehicle, say V_s generates a road-related message msg and broadcasts it to its neighbouring vehicles. This is described as follows.

1. V_s forms a $\texttt{MSG} = (h = \mathcal{H}_4(\texttt{msg}), t_b)$ where $h = \mathcal{H}_4(\texttt{msg})$ is a hash of the message and t_b is the time when the message was announced.

2. V_s perform Step ⑨ where the $\texttt{CLSsign}()$ takes as input $\texttt{MSG}$, V_s's signing key $\texttt{sk}^i_{V_s}, \{\texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{V_s}\}$ and V_s's public key $\texttt{pk}^i_{V_s}$. It returns a signature $\theta_{V_s} = (U, v)$.

$$\theta_{V_s} \leftarrow \texttt{CLSsign}(\texttt{MSG}, \texttt{sk}^i_{V_s}, \{\texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{V_s}\}, \texttt{pk}^i_{V_s})$$

3. V_s forms a *message tuple* $M = (\texttt{msg}, t_b, \theta_{V_s}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{V_s})$ and broadcasts M to its neighbouring vehicles.

5.2.6 Message Verification Phase

Upon receiving the message tuple M, a receiving vehicle, say V_r, performs the following procedure:

1. it determine whether it is interested in the message $\texttt{msg}$. If it is, it computes $h = \mathcal{H}_4(\texttt{msg})$;
2. V_r inputs θ_{V_s} into its trusted hardware. The trusted hardware retrieves the current time t_r from its embedded clock, and then stores the tuple (θ_{V_s}, t_r) within the trusted hardware. The trusted hardware outputs t_r to V_r.
3. V_r performs Step ⑩ where it first determines whether the broadcasting vehicle is reputable, that is, $\texttt{repscore}^i_{V_s} \cdot \mathsf{TimeDiscount}(t_r - t^i_{V_s}) \geq \Psi_{\texttt{MS}}$;
4. V_r determines message freshness. A message is considered to be fresh if $t_r - t_b \leq \Psi_t$ where Ψ_t is very short time period after a sending vehicle announced a message.
5. V_r runs $\texttt{CLSverify}(\texttt{MSG}, \theta_{V_s}, \{\texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{V_s}\}, \texttt{pk}^i_{V_s})$. If it returns **accept**, then the signature θ_{V_s} is considered valid. Otherwise V_r **rejects** the message.

The message $\texttt{msg}$ is considered reliable if all the above requirements are satisfied. The message tuple M is kept for future feedback reporting. If it does not fulfill the requirements, V_s is not considered as trustworthy and $\texttt{msg}$ is not considered as reliable and will not be taken into consideration. In the latter case, if Steps 2 and 3 are positive,

then the message tuple M is still stored for future feedback reporting. Otherwise it is discarded.

5.2.7 Feedback Reporting Phase

In this phase, when vehicle V_r, has its own experience about the event that the message `msg` describe, it is able to judge the trustworthiness of the message. Then if V_r wants to report feedback to the management server, it performs Step (11) elaborated by the following procedures.

1. V_r generates a feedback rating $\texttt{feedrate} \in \{0, 1\}$ where $\texttt{feedrate} = 1$ if `msg` is reliable and $\texttt{feedrate} = 0$ if `msg` is not reliable.
2. V_r forms a $\texttt{feedback} = (\texttt{feedrate}, h, t_r, t_b, \theta_{V_s}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s})$.
3. V_r runs the `CLSsign`() that takes as input a `feedback`, a feedback reporter's signing key $\texttt{sk}^j_{V_r}, \{\texttt{pseu}^j_{V_r}, \texttt{repscore}^j_{V_r}, t^j_{V_r}\}$ and V_r's public key $\texttt{pk}^j_{V_r}$. It returns a signature $\theta_{V_r} = (U', v')$.

$$\theta_{V_r} \leftarrow \texttt{CLSsign}(\texttt{feedback}, \texttt{sk}^j_{V_r}, \{\texttt{pseu}^j_{V_r}, \texttt{repscore}^j_{V_r}, t^j_{V_r}\}, \texttt{pk}^j_{V_r})$$

4. V_r casts a $\texttt{feedback report} = (\texttt{feedback}, \theta_{V_r}, \texttt{pk}^j_{V_r})$.

When V_r drives into the wireless communication range of a AP, it sends the `feedback report` to the `MS` via the AP.

5.2.8 Reputation Update Phase

The `MS` first verifies the feedback received from other vehicles as in Step (12). It retrieves $(\texttt{repscore}^i_{V_s}, t^i_{V_s}, \texttt{repscore}^j_{V_r}, t^j_{V_r})$ from its database based on $(\texttt{pseu}^i_{V_s}, \texttt{pseu}^j_{V_r})$ for V_s and V_r respectively in order to carry out the verification describe as follows.

1. It determine whether $t_r - t_b \leq \Psi_t$ where Ψ_t is small. This is performed to ensure that a receiving vehicle cannot forward this message to other colluding vehicles and together launch an attack to manipulate the reputation of the broadcasting vehicle;

2. runs $\texttt{CLSverify}(\texttt{feedback}, \theta_{V_r}, \{\texttt{pseu}^j_{V_r}, \texttt{repscore}^j_{V_r}, t^j_{V_r}\}, \texttt{pk}^j_{V_r})$. If it returns **accept**, then the signature θ_{V_r} is considered valid. Otherwise MS **rejects** the feedback.

3. runs $\texttt{CLSverify}(\texttt{MSG}, \theta_{V_s}, \{\texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{V_s}\}, \texttt{pk}^i_{V_s})$. If it returns **accept**, then the signature θ_{V_s} is considered valid. Otherwise MS **rejects** the feedback.

4. If the checks pass then the reputation server considers the `feedback report` as valid and stores it in the database.

Upon successful verification, the MS sends the RS $(\texttt{feedback}, V_s, V_r)$ to be processed as shown in Step (13). The RS then execute Step (14) which applies the reputation aggregation algorithm Aggr (Section 5.2.8.1) on all stored feedback relating to V_s. It then replaces the previous reputation score in the database with its latest reputation score.

5.2.8.1 The Reputation Aggregation Algorithm

In this section, the reputation aggregation algorithm Aggr used for this scheme is similar as described in Section 4.5.7.1 of Chapter 4. The function of Aggr is to compute the latest reputation score for a vehicle V based on all stored feedback.

5.2.9 Revocation Phase

In our paper, a vehicle retrieves a set of credentials $\texttt{repcre} = (\texttt{pseu}^i_V, \texttt{repscore}^i_V, t^i_V, x^i_V)$ from the MS. The design of our scheme allows a shorter interval of credentials retrieval. Frequent credentials retrieval allows a vehicle to obtain its latest reputation score as the reputation score of a vehicle evolves, based on the reliability of messages that the vehicle announces. A vehicle whose reputation score decreases to 0 will be revoked from

the system. The MS will stop issuing pseudonyms, reputation scores, timestamps and the partial keys. A misbehaved vehicle would then not be able to compute its secret and its public key. Therefore, it would not be able to participate in future communication in the network.

5.3 A Threshold-based Certificateless Anonymous Authenticated Announcement Scheme in VANETs

In this section, a modification of the CLS scheme presented in Section 5.2.2 is described. We adopt the threshold method as another means to evaluate the reliability of messages. The modification mainly affects the *initialisation phase*, *periodic credential retrieval*, *broadcast phase*, *message verification phase* and *revocation phase*.

In this CLS threshold-based scheme, we assume the presence of the key generator center (KGC) who plays the role as the trusted party. We note that the CLSsetup(), CLSenrol(), CLSsign() and CLSverify() used in this section has been presented in Section 5.1.2.2. This scheme will be presented based on the steps of the abstraction scheme in Figure 3.1 located in Section 3.1 of Chapter 3.

Initialisation Phase

The initialisation phase of the scheme requires the installation of:

1. a secure certficateless signature scheme CLS = (CLSsetup, CLSenrol, CLSsign, CLSverify) as described in Section 5.1.2.2. We will use CLS to realise a 3A.
2. a secure signature scheme, defined by SS = (KGen_{SS}, SSsign, SSverify) where KGen_{SS}, SSsign and SSverify denotes key generation, signing and verifying operation for a signature scheme respectively.
3. a secure symmetric key encryption scheme, defined by SKE = (KGen_{SKE}, SKEnc, SKDec) where KGen_{SKE}, SKEnc and SKDec denotes symmetric key generation, encryption and decryption respectively.

4. a secure public key encryption scheme, defined by $\mathtt{PKE} = (\mathtt{KGen}_{\mathtt{PKE}}, \mathtt{PKEnc}, \mathtt{PKDec})$ where $\mathtt{KGen}_{\mathtt{PKE}}, \mathtt{PKEnc}$ and $\mathtt{PKDec}$ denotes public key generation, encryption and decryption respectively.

The KGC then runs:

1. the algorithm $\mathtt{CLSsetup}(1^k)$ as in section 5.1.2.2 to get $\langle s, \mathtt{CLSparams} = \langle \mathbb{G}_1, \mathbb{G}_2, e, q, P, P_0, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3 \rangle \rangle$;
2. the $\mathtt{KGen}_{\mathtt{PKE}}$ to generate a key pair $(\mathtt{PK}_{\mathtt{KGC}}, \mathtt{SK}_{\mathtt{KGC}})$ used to encrypt and decrypt session keys (please refer to Section 5.2.4) ;
3. the $\mathtt{KGen}_{\mathtt{SS}}$ to generate a key pair $(\mathtt{pk}_{\mathtt{KGC}}, \mathtt{sk}_{\mathtt{KGC}})$ used to sign V long term keys;
4. selects another secure hash function $\mathcal{H}_4 : \{0,1\}^n \rightarrow \mathbb{Z}_q^*$;
5. installation of the CLS;
6. publishes $\mathtt{params} = \langle \mathtt{CLSparams}, \mathcal{H}_4, \mathtt{pk}_{\mathtt{KGC}}, \mathtt{PK}_{\mathtt{KGC}} \rangle$.

When a new vehicle is admitted into the network, it is initialised as follows.

1. Each vehicle is assign with a unique identity $\mathtt{ID}_V \in \{0,1\}^*$.
2. The KGC installs $\mathtt{CLS}, \mathtt{SS}, \mathtt{SKE}$ and PKE schemes onto each vehicle V.
3. A V generates a pair of unique long term key pair (pk_V, sk_V) using $\mathtt{KGen}_{\mathtt{SS}}$.
4. We require a configurable public parameter Ψ_t. The parameter Ψ_t acts as a threshold and used to determine whether or not a message tuple is sufficiently fresh.

The authentication process to validate pk_V to the KGC takes place during the V's registration before it is admitted into the system. This is performed in Section 5.3.1 below.

5.3.1 Registration Phase

Step ① A V sends a request to the KGC for its credentials and to authenticate its self-generated pk_V $\texttt{request}(\texttt{ID}_V, pk_V)$. A pk_V is V self-generate credential associate to its identity $\texttt{ID}_V$ assigned by the KGC. To perform this step, a V first generate a signature $\sigma = \texttt{SSsign}_{sk_V}(\texttt{ID}_V, pk_V)$ while keeping its corresponding secret key sk_V private. A random session key $\texttt{skey}_V$ is generated using $\texttt{KGen}_{\texttt{SKE}}$ to encrypt the request $\texttt{req}_V = \texttt{SKEnc}_{\texttt{skey}_V}(\texttt{ID}_V, pk_V, \sigma)$. It encrypts the session key $\texttt{key}_V = \texttt{PKEnc}_{\texttt{PK}_{\texttt{KGC}}}(\texttt{skey}_V)$ and sends $\{\texttt{req}_V; \texttt{key}_V\}$ to the KGC via the secure authenticated channel.

Step ② The KGC $\texttt{check}(\texttt{ID}_V, pk_V)$ to authenticate V. To do this, it first decrypts $\texttt{key}_V$ by using $\texttt{PKDec}_{\texttt{SK}_{\texttt{KGC}}}$. The session key obtained is used to decipher $\texttt{req}_V$ using $\texttt{SKDec}_{\texttt{skey}_V}$. This will allow the KGC to verify σ on $(\texttt{ID}_V, pk_V)$ using SSverify.

Step ③ Upon successful verification of σ, the KGC $\texttt{compute}(\texttt{cre}_V(t)) = \texttt{cre}_V^{\texttt{KGC}}(t) = (\texttt{ID}_V, \sigma_{\texttt{sk}_{\texttt{KGC}}}(pk_V), \texttt{pseu}_V^i)$. The signature generated on pk_V essentially informed V that pk_V has been certified by the KGC. The KGC then creates a database that will store the following data for every vehicle in the system: a vehicle's identity $\texttt{ID}_V$, a unique long term public key pk_V and a set of pseudonym $\texttt{pseu}_V^i$ issued to V.

Step ④ The KGC $\texttt{return}(\texttt{ID}_V, \sigma_{\texttt{sk}_{\texttt{KGC}}}(pk_V), \texttt{pseu}_V^i)$ to V_s.

Step ⑤ A V performs $\texttt{validate}(\sigma_{\texttt{sk}_{\texttt{KGC}}}(pk_V), \texttt{pseu}_V^i)$ using $\texttt{pk}_{\texttt{KGC}}$. A V then stores pk_V and $\texttt{pseu}_V^i$ after successful verification.

Periodic Credential Provision

In this phase, a vehicle V retrieves from the KGC a set of its pseudonyms $\texttt{pseu}_V^i$. When it drives into the wireless communication range of an access point, the communication takes place as follow.

Step ① To request for credentials $\texttt{request}(\texttt{cre}_V(t)) = \texttt{request}(pk_V)$, a V first identifies itself to the KGC. It signs a request message $\sigma = \texttt{SSsign}_{sk_V}(pk_V)$. A random session key $\texttt{skey}_V$ is generated using $\texttt{KGen}_{\texttt{SKE}}$ to encrypt the request $\texttt{req}_V = \texttt{SKEnc}_{\texttt{skey}_V}(pk_V, \sigma)$.

A V then encrypts the session key $\texttt{key}_V = \texttt{PKEnc}_{\texttt{PK}_{\texttt{KGC}}}(\texttt{skey}_V)$ and sends $\{\texttt{req}_V; \texttt{key}_V\}$ to the KGC via the wireless channel.

Step ② To $\texttt{check}(\texttt{cre}_V(t)) = \texttt{check}(pk_V)$, the KGC first decrypts $\texttt{key}_V$ by using $\texttt{PKDec}_{\texttt{SK}_{\texttt{KGC}}}$. The session key obtained is used to decipher $\texttt{req}_V$ using $\texttt{SKDec}_{\texttt{skey}_V}$.

Step ③ Upon verification of σ using SSverify, the KGC generates a set of pseudonyms $\texttt{compute}(\texttt{cre}_V(t)) = \texttt{pseu}_V^i$. It then encrypts $\texttt{pseu}_V^i$ with the session key $\texttt{skey}_V$ using the secret key encryption algorithm SKEnc and sends the ciphertext to V via the secure channel.

Step ④ The KGC $\texttt{return}(\texttt{pseu}_V^i)$ to V.

Step ⑤ To $\texttt{validate}(\texttt{pseu}_V^i)$, V decrypts the set of $\texttt{pseu}_V^i$ acquired using SKDec with $\texttt{skey}_V$. It runs $\texttt{CLSenrol}_V(x_V^i)$ that generate its set of secret value y_V^i and compute a set of its key pairs $(\texttt{pk}_V^i, \texttt{sk}_V^i)$. The set of secret keys $\texttt{sk}_V^i$ is stored in the black box while the rest of the other parameters and public keys are stored in the vehicle's OBU.

Our scheme provides flexibility where the retrieval period varies. There is a tradeoff between the frequency a vehicle retrieves its keys from the KGC and the efficiency of the scheme. Long interval between retrieval period may be desirable as it may ease management to the KGC who does not need to compute the keys for a vehicle frequently. However, it will lead to storage problem to a vehicle that needs to preload a lot of keys over a long period of time. Meanwhile, a shorter interval between retrieval period solves the storage problem as a vehicle only needs to store fewer keys for a shorter time duration. It also provides a simpler means of revocation. Once it runs out of keys, a misbehaved vehicle would not be able to obtain the next set of keys from the KGC. However, it implies frequent interaction between the KGC and a vehicle.

5.3.2 Broadcast Phase.

An announcing vehicle, say V_s generates a road-related message msg and broadcasts it to its neighbouring vehicles. This is described as follows.

1. V_s forms a $\texttt{MSG} = (h = \mathcal{H}_4(\texttt{msg}), t_b)$ where $h = \mathcal{H}_4(\texttt{msg})$ is a hash of the message and t_b is the time when the message was announced.

2. A vehicle V_s perform Step ⑥ where the $\texttt{CLSsign}()$ takes as input $\texttt{MSG}$, V_s's signing key $\texttt{sk}^i_{V_s}, \texttt{pseu}^i_{V_s}$, and V_s's public key $\texttt{pk}^i_{V_s}$. It returns a signature $\theta_{V_s} = (U, v)$.

$$\theta_{V_s} \leftarrow \texttt{CLSsign}(\texttt{MSG}, \texttt{sk}^i_{V_s}, \texttt{pseu}^i_{V_s}, \texttt{pk}^i_{V_s})$$

3. V_s forms a *message tuple* $M = (\texttt{msg}, t_b, \theta_{V_s}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s})$ and broadcasts M to its neighbouring vehicles.

5.3.3 Message Verification Phase

Upon receiving the message tuple M, a receiving vehicle, say V_r, performs the following procedure:

1. it determine whether it is interested in the message $\texttt{msg}$. If it is, it computes $h = \mathcal{H}_4(\texttt{msg})$;

2. The trusted hardware retrieves the current time t_r from its embedded clock and V_r determines message freshness. A message is considered to be fresh if $t_r - t_b \leq \Psi_t$ where Ψ_t is very short time period after a sending vehicle announced a message.

3. V_r perform Step ⑦ where it runs $\texttt{CLSverify}(\texttt{MSG}, \theta_{V_s}, \{\texttt{pseu}^i_{V_s}, \texttt{pk}^i_{V_s})$. If it returns **accept**, then the signature θ_{V_s} is considered valid. Otherwise V_r **rejects** the message.

The message $\texttt{msg}$ is considered reliable if all the above requirements are satisfied. V_r will act upon the message and make decisions quickly once it collects and verifies t messages of the same event reported by t distinct vehicles within a period of time.

5.3.4 Revocation Phase.

Step ⑧ If a vehicle found to be malicious, the KGC will stop issuing its credentials. Therefore, V_s won't be able to generate its full key pair $(\mathtt{pk}_{\mathtt{V}_s}, \mathtt{sk}_{\mathtt{V}_s})$ to continue participating in the network.

5.4 Analysis

In this section, we analyse the security of our schemes, and evaluate its performance. We compare our schemes with schemes that adopt a pseudonyms method [18, 92], which is of the most interest to us in this work.

5.4.1 Security Analysis

We compare our schemes with Hybrid [18] and pseudonymous public key (PPK) [92] based on three main security requirements of reliability, privacy and accountability. We consider the eight security requirements as discussed in Section 2.3 and summarised our finding in Table 5.1 below.

5.4.1.1 Reliability

The requirement of sender authenticity and message integrity are satisfied in all four schemes, as long as the digital signature techniques used are secure. Similarly, in feedback reporting, reporter authenticity and report integrity are achieved if the digital signature schemes are secure. We also require the signature, public and symmetric key encryption schemes adopted during reputation score and keys retrieval phase in Section 5.2.4 and 5.3.1 to be secure. This is to ensure that the trusted authority provides the correct credentials after verifying the legitimacy of a requesting vehicle V.

However, the property of message truthfulness is not provided in Hybrid as distin-

guishability of message origin is difficult to achieve without an online trusted party. Hence, the threshold technique cannot be adopted. It is also not satisfied in the scheme proposed in PPK as, for the same message, a signing vehicle can disguise as multiple vehicles. A similar problem occur for our threshold-based scheme $\mathtt{CLS}_T$. In our other scheme using reputation system $\mathtt{CLS}_{\mathtt{RS}}$, a message is regarded as truthful if the message originator has a "good" reputation. Hence in order to lie successfully, an adversary could do one of two things: it can manipulate the reputation score of the sending vehicle, or it can manipulate the message content of an announcement.

In the latter case, neither an external nor an internal adversary will be able to convince receiving vehicles that a modified message is valid if the certificateless signature scheme is secure. On the other hand, an internal adversary with a high reputation score can deceive a receiving vehicle into accepting a false message easily: it simply broadcasts the false message. However, if it does this persistently over a long period, then the negative feedback will result in a decrease in its reputation score. Eventually its reputation score will decrease to 0 and it will be revoked from the system.

To manipulate the reputation score of a target vehicle V, firstly an adversary could impersonate V and broadcast false messages in order for V to receive negative feedback and thereby decrease its reputation score. This cannot be done if the certificateless signature scheme is secure. Secondly an adversary could instead replace V's reputation score with a lower one in a broadcast message. Again this could not be done if the $\mathtt{CLS}$ is secure. Lastly an adversary could provide negative feedback for announcements made by V. Clearly an external adversary cannot perform this attack given that the $\mathtt{CLS}$ is secure. An internal adversary acting on its own can only report a false feedback per announcement, and this will have only a small impact on V's reputation score. Even if the internal adversary colludes with a group of other internal adversaries, the effect will remain small if the proportion of dishonest vehicles is small, as is the assumption. In addition, the provision of timestamps limits the vehicles who can provide feedback to those in proximity when the message is announced.

Hence we see that our scheme provides reliability and also provides system robustness in the presence of a small fraction of adversaries.

5.4.1.2 Privacy

In PPK and both our schemes, messages are linkable only over the short validity period of a pseudonym. In Hybrid, a vehicle uses its group signing key to certify a self-generated pseudonym. The rate at which pseudonyms are updated depends on the various factors. Hence, similar to our schemes and PPK, messages signed using the same pseudonym are linkable over its short lifetime (marked $\checkmark^*$ in Table 5.1). This is a slight compromise of privacy in favour of reducing storage and communication costs. The length of the validity period can be adjusted according to the level of privacy required. In $\texttt{CLS}_{\texttt{RS}}$, this applies to both announcements and feedback reporting. The request activity for credentials made by V is also unlinkable using a secure symmetric key encryption scheme where a random session key is generated to encrypt each request. The session key is then encrypted using a secure public key encryption scheme.

Anonymity of broadcast messages is achieved by both Hybrid and PPK. In $\texttt{CLS}_{\texttt{RS}}$, communications for the retrieval of reputation scores and pseudonyms are protected by signatures and encryptions. As long as these schemes are secure, a vehicle and its credentials will be anonymous. Hence our scheme preserves anonymity in reputation score retrieval, message announcements and feedback reporting.

Note that the above refers to privacy against any eavesdropper apart from the trusted authority. None of the schemes provide any privacy against the `TP` (`MS` and `KGC` in our case) in the sense that if a set of broadcast messages were presented to the `TP`, it would be able to link the messages to the senders. There is also no privacy against the `MS` in feedback reporting. Since the `MS` is trusted to correctly manage the reputation system, this is not a great compromise. Note though that the `MS` does not know the activities of the vehicles since a feedback report only contains a hash of the message content.

5.4.1.3 Accountability

The property of traceability is satisfied in all schemes. The group signature in Hybrid allows a `TP` to open signature of malicious vehicles, where the identity of misbehaved vehicles is revealed by law enforcement authorities for liability purposes. In PPK as

well as our scheme, the TP is able to search in its database and trace the identity of misbehaved vehicles.

Neither Hybrid nor PPK provides non-repudiation. The group signature technique used in Hybrid permit the issuer to create the private keys of group members. In the scheme in PPK, the TP generates the secret key for all vehicles. Therefore, these schemes does not achieve non-repudiation as the signer is not the sole holder of the signing key. In our schemes, the MS and KGC does not have access to entities' private key as it only generates an entity with a partial private key. This satisfies the requirement of non-repudiation.

Revocation in Hybrid is achieved by having a vehicle's revocation token added into the revocation list. Upon verifying a message, signature generated from a revoked vehicle will not be accepted. In PPK, the TP exhaustively search in its huge database where it stores all the anonymous certificates issued to vehicles to find the real identity of a misbehaved vehicle. In our schemes, the MS and KGC maintains a map from a vehicle's long term identity to its set of pseudonyms. The MS can perform an inverse mapping and identify the vehicle whose reputation score decreases to 0 for $\mathtt{CLS}_{\mathtt{RS}}$. The authority will then stop issuing pseudonyms, reputation scores and partial keys (pseudonyms and partial keys for $\mathtt{CLS}_T$) to misbehaved vehicles and hence, these vehicles would not be able to generate its secret value, its public key and compute a full secret key to announce a message.

5.4.2 Performance Analysis

We compare the performance of our scheme with Hybrid [18] and PPK [92]. The group signature (GS) in Hybrid used to certify self-generated pseudonym is adopted from [13] and we choose to employ elliptic curve cryptosystem, such as ECDSA scheme [14, 52, 54] as the basic signature algorithm to sign messages, which will also be used in PPK. We set security level $l = 80$ bits for message signatures and $l = 128$ bits for certificates in Hybrid and PPK. This is a similar adoption of values and signature algorithm as in Hybrid, to ease the purpose of comparison. We summarise our findings in Tables 5.2 and 5.3.

Security Analysis					
Security goals	Security components	Hybrid [18]	PPK [92]	$\texttt{CLS}_{\texttt{RS}}$	$\texttt{CLS}_{T}$
Reliability	Sender's Authenticity	✓	✓	✓	✓
	Message Integrity	✓	✓	✓	✓
	Message truthfulness	×	×	✓	×
Privacy	Anonymity	✓	✓	✓	✓
	Unlinkability	✓*	✓*	✓*	✓*
Accountability	Non-repudiation	×	×	✓	✓
	Revocation	✓	✓	✓	✓
	Traceability	✓	✓	✓	✓

Table 5.1: Comparison of security analysis

Computational cost. We evaluate the computational cost of signature generation and verification in the broadcast of messages. As observed in [23, 24], the two most expensive operations are multiplications in $\mathbb{G}_1$ and pairing evaluation, which we shall consider here. We compare the cost between our scheme with Hybrid [18] and PPK [92] for $t = 1$, as our scheme requires only one message provided that the message generator has sufficiently high reputation.

The signing operation in PPK requires 2 scalar multiplications and the verification requires 4 scalar multiplications. Meanwhile, the Hybrid scheme requires a vehicle to generate 2 signatures; a group signature adopted from [13] to certify a self-generated pseudonym `pk` and a signature similar to PPK on the announced message. The group signature requires 8 scalar multiplications and 1 pairing operation for the signing phase, while the verification phase requires 5 scalar multiplications and 3 pairing operations. The signature generation and verification on a message is then similar to PPK described earlier.

The signing procedure of both our schemes requires 3 scalar multiplications and the verification requires 4 pairing operations. These findings are summarised in Table 5.2. We see that the computational cost for our scheme is comparable to PPK and more efficient compared to Hybrid. In addition, as noted before, in our scheme, a receiving vehicle may make a decision on whether to rely on a broadcast message immediately,

while in PPK and Hybrid, a receiving vehicle typically requires a few messages before reliability can be confirmed.

Our $\mathtt{CLS}_{\mathtt{RS}}$ scheme has additional operations where V_r may choose to provide a feedback to rate its experience with the message generator. In this case, the computational cost is that of 1 signature. The verification of feedback requires 2 signatures verifications. This is performed by the MS and can be done offline.

Signature length. The signature in PPK generated using elliptic curve digital signature algorithm (ECDSA)[14, 52, 54] comprises of 2 elements of $\mathbb{G}_1$. A group signature in Hybrid comprises of 2 elements of $\mathbb{G}_1$ and 5 elements of $\mathbb{Z}_q$. Meanwhile, the length of signature in both our schemes composed of 2 elements of $\mathbb{G}_1$, which is similar to PPK. To provide a security level 2^{80}, we can set q to be 190-bit long and the element in $\mathbb{G}_1$ is 191-bit long by choosing an appropriate curve such as NIST curve [14]. Thus, the length of signature generated on a message is 48 bytes in our scheme and PPK. In Hybrid, the message signature is 48 bytes and the length of signature on the certified pseudonym is of 224 bytes (for a security level 2^{128}, we have $|q| = 255$ bits and $|\mathbb{G}_1|$=256 bits), which sums up to 272 bytes generated by a vehicle. This again shows that our scheme provides message signatures with length comparable to those of existing schemes. This result is summarised in Table 5.3.

Communication cost. A message M in Hybrid and PPK consists of: $(\theta_{\mathtt{sk}}(\mathtt{msg}), \mathtt{msg}, \mathtt{cert}_{\mathtt{TP}}(\mathtt{pk}), \mathtt{pk}, t)$, which denotes signature generated on an announced message, a message announced, its certificate which essentially is the signature of the TP on a vehicle's public key, a vehicle's public key and a timestamp to specify signature generation time respectively. To provide a security level of 2^{80}, we can set q to be 190-bit long and the element in $\mathbb{G}_1$ is 191-bit long. According to [7] the size of safety messages is 100 bytes and we choose 8 bytes for timestamp, using the unix 64-bit timestamp. Based on the implementation in [14, 60], the size of the public key is 25 bytes, message signature is 48 bytes and TP certificate is 64 bytes. Hence the length of the message in PPK is $L = 48 + 100 + 64 + 25 + 8 = 245$ bytes. In Hybrid, the message size is $L = 48 + 100 + 224 + 25 + 8 = 405$ bytes. We note that the implementation of GS in [13] adopted by Hybrid is not available to us, hence we use the similar values in Hybrid which were calculated using the number of 32-bit word multiplications required for GS

signing and verifying, extracted from [14, 60].

In $\texttt{CLS}_{\texttt{RS}}$, a message is composed of: $(\theta_{V_s}(\texttt{msg}), \texttt{msg}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{\texttt{rs}_{V_s}}, t_b)$, where $\theta_{V_s}(\texttt{msg}), \texttt{msg}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s}, \texttt{repscore}^i_{V_s}, t^i_{\texttt{rs}_{V_s}}$ and t_b denotes a signature generated on an announced message, a message announced, a vehicle's public key, its pseudonym, its reputation score and a timestamp on the reputation score and message broadcasted respectively. The size of the public key and pseudonym is of an element $\mathbb{G}_1$ each, and reputation score of size 1 byte. Therefore the size of the message size is $L = 48 + 100 + 24 + 24 + 1 + 8 + 8 = 213$ bytes. Meanwhile, in $\texttt{CLS}_T$, a message is composed of: $(\theta_{V_s}(\texttt{msg}), \texttt{msg}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s}, t_b)$. The the size of the message size is $L = 48 + 100 + 24 + 24 + 8 = 204$ bytes. We observed that our schemes yield the shortest message size compared to these two schemes. This result is summarised in Table 5.3.

Our $\texttt{CLS}_{\texttt{RS}}$ scheme is also composed of a feedback reporting phase where a receiving vehicle V_r may choose to rate its experience with the message generator V_s. A feedback report is composed of: $((\texttt{feedrate}, h, t_r, t_b, \theta_{V_s}, \texttt{pk}^i_{V_s}, \texttt{pseu}^i_{V_s}), \theta_{V_r}, \texttt{pk}^j_{V_r})$. The size of the `feedrate` is of 1 byte, the timestamp t_r and t_b is of 8 bytes each, and hash of the announced event h is of an element q, which is 24 bytes. The pseudonym $\texttt{pseu}^i_{V_s}$ and both public keys $\texttt{pk}^i_{V_s}$ and $\texttt{pk}^j_{V_r}$ is an element of $\mathbb{G}_1$ each respectively. The signature generated by V_r on the feedback is of two elements of $\mathbb{G}_1$, similar to θ_{V_s}. Hence the length of the feedback report is $F = 1+24+8+8+48+24+24+48+24 = 137$ bytes.

Storage cost. We compare the storage cost of our scheme with PPK during credential retrieval phase given the similar approach of preloading credentials onto a vehicle. For each credential retrieval period, PPK preloads a large set of key pairs and their corresponding certificate onto each vehicle, for its usage over a long period of time (i.e. a year). The next retrieval may occur during periodical vehicle maintenance visits, for instance. The public and private key is 25 bytes and 24 bytes respectively, using ECDSA-192 and a `TP` certificate is 64 bytes using ECDSA-256. This sums up to storage space of $25 + 24 + 64 = 113$ bytes per key. In [91], they assumed an average a driver uses his car is 2 hours per day, where the lifetime of each key is one minute. Then the number of required keys per year is approximately 43800, which amounts to storage space of 4.95 Mbytes on each vehicle.

In $\texttt{CLS}_{\texttt{RS}}$, a vehicle retrieves from the $\texttt{MS}$ a set of credentials $\texttt{Cre} = (\texttt{pseu}_V^i, \texttt{repscore}_V^i, t_V^i, x_V^i)$. The partial key x_V^i and pseudonym $\texttt{pseu}_V^i$ is an element of $\mathbb{G}_1$ each, hence x_V^i and $\texttt{pseu}_V^i$ is of 24 bytes each for $|\mathbb{G}_1| = 191$ bits. The sum of storage space is of $8 + 1 + 24 + 24 = 57$ bytes per key, which is more efficient as it is less than half compared to PPK for each key. The retrieval period in our scheme is shorter and flexible, depends on whether a vehicle would like to obtain its latest reputation score or when it runs out of credentials. In $\texttt{CLS}_T$ a vehicle retrieves from the $\texttt{KGC}$ a set of pseudonyms and partial keys. The sum of storage space is of $24 + 24 = 48$ bytes per key, which is more efficient.

Scheme	Msg signature Sign	Msg signature Verify	Group signature Sign	Group signature Verify
PPK	$2 \cdot \mathbb{G}_1$	$4 \cdot \mathbb{G}_1$	N/A	N/A
Hybrid	$2 \cdot \mathbb{G}_1$	$4 \cdot \mathbb{G}_1$	$8 \cdot \mathbb{G}_1 + 1 \cdot P$	$5 \cdot \mathbb{G}_1 + 3 \cdot P$
$\texttt{CLS}_{\texttt{RS}}$	$3 \cdot \mathbb{G}_1$	$4 \cdot P$	N/A	N/A
$\texttt{CLS}_T$	$3 \cdot \mathbb{G}_1$	$4 \cdot P$	N/A	N/A

Here $n \cdot \mathbb{G}_1$ denotes n scalar multiplications and $n \cdot P$ denotes n pairing operations.

Table 5.2: Comparison of computational cost

Scheme	Signature length (bytes)	Communication cost	Storage cost
PPK	$2\|\mathbb{G}_1\|$ (48)	245 bytes	113 bytes/key
Hybrid	(Group sig) $2\|\mathbb{G}_1\| + 5\|q\|$ (224) (Msg sig) $2 \cdot \mathbb{G}_1$ (48)	405 bytes	- -
$\texttt{CLS}_{\texttt{RS}}$	$2 \cdot \mathbb{G}_1$ (48)	213 bytes	57 bytes/key
$\texttt{CLS}_T$	$2 \cdot \mathbb{G}_1$ (48)	204 bytes	48 bytes/key

Table 5.3: Comparison of communication and storage cost ($l = 80$)

5.5 Conclusion

We have presented two novel privacy-preserving authentication protocols for VANETs based on certificateless signature. To the best of our knowledge, these are the first

certificateless announcement schemes for VANETs that has been proposed in the literature. We have shown that our schemes are efficient and robust, and achieves the desirable property of a reliable, anonymous and accountable announcement scheme without inducing the problem of certificate management and overhead.

Chapter 6

Conclusion

In this chapter, we highlight the contributions of this thesis and discuss future research.

Contents

6.1 Concluding remarks and Summary of Contributions

Wireless networks have developed over time to be sophisticated enough to meet the demands from evolving modern communication technologies. One of the emerging technologies in wireless networks is VANET. The rise of collaborative safety applications in VANETs that utilize wireless communicating vehicles may have the potential to mitigate the implication of traffic accidents and even prevent them altogether. These applications allow a vehicle to broadcast information associated with each event on the road. The information announced include real-time speed and position of a vehicle to warn neighbouring vehicles about potential dangerous situations ahead of them.

Despite the safety benefits derived from these services, privacy is a critical concern in VANETs. A lot of personal information can be inferred from vehicle-generated messages as it contains signature, location, and other associated information from the sending vehicle. The privacy of a vehicle may be compromised if extensive position information is compiled, leading to profiling of a vehicle. Techniques on anonymous

communication can be employed to protect a vehicle's privacy. At the same time, the system should allow for identity resolution when misbehaviour issues arise.

In this thesis, we constructed authenticated anonymous announcement schemes, which we called as 3A. We considered the challenging setting of conflicting security requirements, in order to strike a balance between a reliable and privacy-preserving 3A in VANETs while enabling a vehicle to be held accountable in case of dispute. First, we systematically studied different credential techniques of an announcement scheme in the literature and discussed their advantages and limitations. We defined the security model we consider in an announcement scheme and elaborated the composition of entities and their role in the system. We constructed a generic abstraction based on threshold method. As far as we are aware of, this is the *first* construction of such abstraction exist in the literature. We also provide a generic abstraction based on a reputation system.

Within these abstractions, we constructed three secure privacy-preserving announcement schemes. The first scheme uses reputation system, which is integrated with public key cryptography. Through reputation mechanism, vehicles can be assisted to choose a reputable message announced by neighboring vehicles, based on their aggregated historical trust, represented by its reputation score. While the use of signature schemes in VANET has been widely deployed and effective, the use of reputation system in conjunction with signature scheme is not as widely studied. Furthermore, the use of reputation system is efficient as it does not face the problem of distinguishing message origin; a prerequisite security property unfortunately suffered by most threshold-based announcement schemes. We performed simulations using GrooveNet simulator and demonstrate that our scheme is efficient and usable for real-world implementation. The other two schemes were constructed using certificateless signature (CLS). To our knowledge, our schemes are the *first* certificateless announcement schemes for VANETs proposed in the literature. These schemes use CLS that eliminate the need of certificates and the associated processing and management overheads of PKI in a traditional PKC. It also enjoys the implicit certificate property of ID-PKC without suffering the inherent key escrow problem. Our schemes are robust and outperforms some previous schemes in the literature in terms of message length and storage cost.

6.2 Future research

The work presented in this thesis has identified some open problems that remain to be solved and possible extension to some of the presented contributions that can be pursued.

- One of the key constraints of the reputation model constructed in this thesis is that it requires vehicles to consistently communicate with the `TP` to acquire its latest reputation score. It would be interesting to develop a different technique using reputation systems to the setting where this communication can be reduced or eliminated, while allowing a vehicle to establish its reputation or enabling trust. Research in this direction may yield another variant of reputation mechanism deployed in an announcement scheme for VANETs in the literature.

- In the same vein, the reputation model developed in this thesis can be extended in several ways. For instance, the feedback aggregation algorithm presented in this thesis is based on binary feedback ratings. It might be of interest to investigate alternative approaches which allow continuous feedback ratings and thus provide richer results.

- In our schemes, an announced event is only utilised by its neighbouring vehicles. It might be of interest to extend the current scheme to where a message can be utilised by vehicles in a greater area. How this may be done without compromising the security against reputation manipulation attacks is the subject of future research.

- The MAC construction of [28] that we analysed in Chapter 3 provides an attractive tradeoff between cheaper computational cost and delay of message authentication. It would be interesting to introduce and analyse a construction in which we incorporate time-release cryptography into the existing work. This construction may provide another means to solve the problem associated with delayed message authentication.

- Privacy threats imposed onto a security protocol depends on the data accessible to an adversary. An interesting open problem would be to 'profile' an adversary

on its ability to derive information about vehicles. Specifically, analytical models capturing the strategy of the adversary, as well as the cost to implement and execute attacks, would definitely improve the understanding of location privacy threats and have an impact on our protocols design and simulation results.

Bibliography

[1] *Vehicle-to-Vehicle Communication Can Prevent Crashes*, 2012. Available at http://www.consumerreports.org/cro/magazine/2012/04/vehicle-to-vehicle-communication-can-prevent-crashes/index.htm. Last accessed on 4 January 2013.

[2] Advanced Cruise-Assist Highway System Research Association (Japan). *Results From Proving Tests of Advanced Cruise-Assist Highway Systems* , 2001. Available at http://trid.trb.org/view.aspx?id=682829. Last accessed on 9th March 2013.

[3] AHS. *Advanced Cruise-Assist Highway Systems*. Available at http://www.mlit.go.jp/road/ITS/1998HBook/chapter3/3-3e.html. Last accessed on 9th March 2013.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. *Computer Networks*, 38(4):393–422, 2002.

[5] S. S. Al-Riyami and K. G. Paterson. Certificateless Public Key Cryptography. In *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 452–473. Springer, 2003.

[6] M. Armaghan, M. Fathy, and S. Yousefi. Improving the Performance of Beacon Safety Message Dissemination in Vehicular Networks Using Kalman Filter Estimation. In *FGIT-FGCN*, volume 56, pages 74–82. Springer, 2009.

[7] ASTM E2213-03. Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specification, 2003.

[8] ASV4. *Advanced Safety Vehicle Project.* Available at http://www.itsforum.gr.jp/Public/E4Meetings/P07/SS6420wani.pdf. Last accessed 1 October 2012.

[9] F. Beruscha, K. Augsburg, and D. Manstetten. Haptic Warning Signals at the Steering Wheel: A Literature Survey Regarding Lane Departure Warning Systems. *Haptics-e, The Electronic Journal of Haptic Research*, 4(5):1–6, 2011.

[10] N. Bißmeyer, J. Njeukam, J. Petit, and K. Bayarou. Central Misbehavior Evaluation for VANETs Based on Mobility Data Plausibility. In *Proceedings of the Ninth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, VANET '12, pages 73–82. ACM, 2012.

[11] D. Boneh, X. Boyen, and H. Shacham. Short Group Signatures. In *CRYPTO*, volume 3152, pages 41–55. Springer, 2004.

[12] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[13] D. Boneh and H. Shacham. Group Signatures with Verifier-Local Revocation. In *ACM Conference on Computer and Communications Security*, pages 168–177, 2004.

[14] M. Brown, D. Hankerson, J. López, and A. Menezes. Software Implementation of the NIST Elliptic Curves Over Prime Fields. In *CT-RSA*, Lecture Notes in Computer Science, pages 250–265. Springer, 2001.

[15] M. Burmester, E. Magkos, and V. Chrissikopoulos. Strengthening Privacy Protection in VANETs. In *IEEE International Conference on Wireless and Mobile Computing*, pages 508–513. IEEE, 2008.

[16] L. Buttyán, T. Holczer, and I. Vajda. On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs. In *ESAS*, volume 4572 of *Lecture Notes in Computer Science*, pages 129–141. Springer, 2007.

[17] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte. SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs. In *IEEE Vehicular Networking Conference (VNC)*, 2009.

[18] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy. Efficient and Robust Pseudonymous Authentication in VANET. In *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks*, pages 19–28. ACM, 2007.

[19] The CAMP Vehicle Safety Communications Consortium. *Vehicle Safety Communications Project Task 3 Final Report*, 2005. Sponsored by U. S. Department of Transportation (USDOT). Available through National Technical Information Service, Springfield, Virginia 22161.

[20] J. L. Campbell, C. M. Richard, J. L. Brown, and M. McCallum. *Crash Warning System Interfaces*. NHTSA, 2007. Final Report DOT HS 810697.

[21] CAR 2 CAR Consortium Manifesto version 1.1. Technical report, CAR 2 CAR Communication (C2CC) Consortium, 2007. Available at http://www.car-2-car.org. Last accessed: June 2011.

[22] W. Chang, W. Hwang, and Y. G. Ji. Haptic Seat Interfaces for Driver Information and Warning Systems. *International Journal of Human-Computer Interaction*, 27(12):1119–1132, 2011.

[23] L. Chen, P. Morrissey, and N. P. Smart. DAA: Fixing the Pairing-Based Protocols. *IACR Cryptology ePrint Archive*, page 198, 2009. Available at http://eprint.iacr.org/2009/198.

[24] L. Chen, S. Ng, and G. Wang. Threshold Anonymous Announcement in VANETs. *IEEE Journal on Selected Areas in Communications*, 29:605–615, 2011.

[25] R. Chen, D. Ma, and A. Regan. TARI: Meeting Delay Requirements in VANETs with Efficient Authentication and Revocation. In *In 2nd International Conference on Wireless Access in Vehicular Environments (WAVE)*. IEEE, 2009.

[26] I. Chlamtac, M. Conti, and J. J.-N. Liu. Mobile Ad Hoc Networking: Imperatives and Challenges. *Ad Hoc Networks*, 1(1):13–64, 2003.

[27] J. Choi and S. Jung. A Security Framework with Strong Non-Repudiation and Privacy in VANETs. In *Proceedings of the 6th Annual IEEE Consumer Communications & Networking Conference (IEEE CCNC)*, 2009.

[28] J. Y. Choi, M. Jakobsson, and S. Wetzel. Balancing Auditability and Privacy in Vehicular Networks. In *Q2SWinet*, pages 79–87. ACM, 2005.

[29] L. Chou, C. Ho, and J. Chen. An Early Warning Scheme for Broadcasting Critical Messages using VANET. *International Journal of Ad Hoc Ubiquitous Computer*, 6(1):1–9, 2010.

[30] E. Commission. *Data Protection: Progress on EU Reform Now Irreversible After European Parliament Vote*, 2014. Available at: http://ec.europa.eu/justice/data-protection. Last accessed on 30 October 2014.

[31] Council of the European Union. *Council directive 96/96/EC of 20 December 1996 on the approximation of the laws of the member states relating to roadworthiness tests for motor vehicles and their trailers*, 1997. Official Journal L 046, 17/02/1997 P1.

[32] M. Dahl, S. Delaune, and G. Steel. Formal Analysis of Privacy for Vehicular Mix-Zones. In *ESORICS*, volume 6345 of *Lecture Notes in Computer Science*, pages 55–70. Springer, 2010.

[33] D. E. Dass Jr., A. J. Uyttendaele, and J. M. B. Terken. Haptic In-Seat Feedback for Lane Departure Warning. In *AutomotiveUI*, pages 258–261. ACM, 2013.

[34] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo. Trustworthy Privacy-Preserving Car Generated Announcements in Vehicular Ad Hoc Networks. *IEEE Transaction on Vehicular Technology*, 58(4):1876 – 1886, 2009.

[35] J. Domingo-Ferrer and Q. Wu. Safety and Privacy in Vehicular Communications. In *Privacy in Location-Based Applications*, volume 5599 of *Lecture Notes in Computer Science*, pages 173–189. Springer, 2009.

[36] J. Domingo-Ferrer, Q. Wu, and Ú. González-Nicolás. *Balanced Trustworthiness, Safety and Privacy in Vehicle-to-Vehicle Communications*, 2010. To be published in IEEE Transactions on Vehicular Technology. DOI: 10.1109/TVT.2009.2034669.

[37] F. Dötzer. Privacy Issues in Vehicular Ad Hoc Networks. In *Privacy Enhancing Technologies*, volume 3856 of *Lecture Notes in Computer Science*, pages 197–209. Springer, 2005.

[38] F. Dötzer, L. Fischer, and P. Magiera. VARS: A Vehicle Ad Hoc Network Reputation System. In *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, volume 1, pages 454–456, 2005.

[39] J. R. Douceur. The Sybil Attack. In Peter Druschel and M. Frans Kaashoek and Antony I. T. Rowstron, editor, *IPTPS*, volume 2429 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 2002.

[40] DSRC. Dedicated Short Range Communications. Available at http://grouper.ieee.org/groups/scc32/dsrc/index.html. Last accessed: July 2012.

[41] A. Eidehall, J. Pohl, and F. G. andJonas Ekmark. Toward Autonomous Collision Avoidance by Steering. *IEEE Transactions on Intelligent Transportation Systems*, 8(1):84–94, 2007.

[42] Fraunhofer SIT. *Safe and Intelligent Mobility Test Field Germany*, 2012. Available at http://www.sit.fraunhofer.de/en/fields-of-expertise/projects/simtd.html. Last accessed 26 February 2013.

[43] H. Fujii, O. Hayashi, and N. Nakagata. Experimental Research on Inter-Vehicle Communication Using Infrared Rays. *Proceedings of the IEEE Intelligent Vehicles Symposium*, pages 266–271, 1996.

[44] O. Goldreich. *Secure Multi-Party Computation*, 2002. Manuscript, version 1.4. 2002. Available at http://www.wisdom.weizmann.ac.il/ oded/pp.html.

[45] P. Golle, D. H. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETs. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, pages 29–37. ACM, 2004.

[46] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys*, pages 31–42, 2003.

[47] D. Han and H. Yang. The Multi-Class, Multi-Criterion Traffic Equilibrium and the Efficiency of Congestion Pricing. *Transportation Research Part E*, 44(5):753–773, 2008.

[48] HONDA. *Safety for Everyone in Our Mobile Society.* Available at http://world.honda.com/CSR/pdf/CSR-06-7-Safety-Initiatives.pdf. Last accessed on 9 January 2013.

[49] HONDA. *Honda Completes Development of ASV-3 Advanced Safety Vehicles*, 2005. Available at http://www.rpec.co.uk/archive/Honda20ASV.pdf. Last accessed on 9 January 2013.

[50] HONDA. *Honda Begins Testing of Advanced Safety Vehicles and Driving Safety Support Systems on Public Roadways*, 2008. Available at http://world.honda.com/news/2008/4080324Advanced-Safety-Vehicles/. Last accessed on 9 January 2013.

[51] J. Hubaux, S. Capkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy*, 2(3):49–55, 2004.

[52] IEEE 1363a. IEEE Standard Specifications for Public Key Cryptography - Amendment 1: Additional Technique, 2004.

[53] ITS Review Japan. *Trends in Intelligent Transport Systems (ITS): Research Report, Special Topic Full-Fledged Application of Dedicated Short-Range Radio Communications for ETC*, 2003.

[54] D. Johnson, A. Menezes, and S. A. Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.

[55] P. Kamat, A. Baliga, and W. Trappe. An identity-Based Security Framework for VANETs. In *Vehicular Ad Hoc Networks*, pages 94–95. ACM, 2006.

[56] P. Kamat, A. Baliga, and W. Trappe. Secure, Pseudonymous, and Auditable Communication in Vehicular *Ad Hoc* Networks. *Security and Communication Networks*, 1(3):233–244, 2008.

[57] F. Kargl and P. Papadimitratos. *Demonstration at 7th Annual International Conference on Mobile Systems, Applications and Services ACM MobiSys*, 2009.

[58] F. Kargl and P. Papadimitratos. *Proposal for MobiSys Demonstration Secure Vehicle Communication (SeVeCom)*, 2009.

[59] F. Kargl, P. Papadimitratos, L. Buttyán, M. Muter, B. Wiedersheim, E. Schoch, T. Thong, G. Calandriello, A. Held, A. Kung, and J. Hubaux. Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges. *CoRR*, abs/0912.5393, 2009.

[60] N. Koblitz and A. Menezes. Pairing-Based Cryptography at High Security Levels. In *IMA Int. Conf.*, pages 13–36, 2005.

[61] G. Kounga, T. Walter, and S. Lachmund. Proving Reliability of Anonymous Information in VANETs. *IEEE Transactions on Vehicular Technology*, 58(6):2977–2989, 2009.

[62] K. Kozak, J. Pohl, W. Birk, J. Greenberg, B. Artz, M. Blommer, L. Cathey, and R. Curry. *Evaluation of Lane Departire Warnings for Drowsy Drivers*, 2006. Proceeding of the Human Factors and Ergonomics Society 50^{th} Annual Meeting.

[63] R. Kroh, A. Kung, and F. Kargl. VANETs Security Requirements final version. Technical report, Secure Vehicle Communication (SeVeCom), 2006.

[64] W. Lee, S. Tseng, and C. Wang. Design and Implementation of Electronic Toll Collection System Based on Vehicle Positioning System Techniques. *Computer Communications*, 31(12):2925–2933, 2008.

[65] Q. Li, A. Malip, K. M. Martin, S. Ng, and J. Zhang. A Reputation-based Announcement Scheme for VANETs. *IEEE Transactions on Vehicular Technology*, 61(9):4095–4108, 2012.

[66] X. Lin, X. Sun, and P. Ho. GSIS: Secure Vehicular Communications with Privacy Preserving. In *IEEE Transactions on Vechicular Technology*, volume 56, pages 3442–3456, 2007.

[67] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong. Revocable Ring Signature. *Journal of Computer Science and Technology*, 22(6):785–794, 2007.

[68] R. Lu, X. Lin, X. Liang, and X. S. Shen. A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):127–139, 2012.

[69] X. Ma, J. Zhang, and T. Wu. Reliability Analysis of One-Hop Safety-Critical Broadcast Services in VANETs. *IEEE Transactions on Vehicular Technology*, 60(8):3933–3946, 2011.

[70] A. Malip, S. Ng, and Q. Li. A Certificateless Anonymous Authenticated Announcement Scheme in Vehicular Ad Hoc Networks. *Security and Communication Networks*, 7(3):588–601, 2014.

[71] R. Mangharam, D. Weller, R. Rajkumar, P. Mudalige, and F. Bai. GrooveNet: A Hybrid Simulator for Vehicle-to-Vehicle Networks. In *Proceeding 3rd Annual Interntional Conference on Mobile Ubiquitous System - Network Server*, pages 1–8, 2006.

[72] F. G. Mármol and G. M. Pérez. TRIP, a Trust and Reputation Infrastructure-based Proposal for Vehicular Ad Hoc Networks. *Journal of Network and Computer Applications*, 35(3):934–941, 2012.

[73] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen. Towards Expanded Trust Management for Agents in Vehicular Ad Hoc Networks. In *International Journal of Computational Intelligence Theory and Practice (IJCITP)*, pages 3–15, 2010.

[74] C. Murray, A. Lopez, C. Mathers, and C. Stein. *The Global Burden of Disease 2000 project: Aims, Methods and Data Sources (GPE discussion Paper No. 36).* Geneva, World Health Organization, 2001.

[75] J. Navarro, F. Mars, and J. Hoc. Lateral Control Assistance for Car Drivers: A Comparison of Motor Priming and Warning Systems. *Human Factors*, 49(5):950–960, 2007.

[76] J. Navarro, F. Mars, and J. Hoc. Lateral Control Support for Car Drivers: A Human-Machine Cooperation Approach. In *ECCE*, volume 250 of *ACM International Conference Proceeding Series*, pages 249–252. ACM, 2007.

[77] NoW. *Network on Wheels*, 2004. Available at http://www.network-on-wheels.de/. Last accessed on May 2011.

[78] U. D. of Transportation. *Connected Vehicle Technology Demonstration at 2012 Annual Meeting.* USDOT/CAMP VSC3, 2012. Last accessed on 30 October 2014. Available at http://www.itsa.org/awards-media/press-releases/1410-usdotcamp-vsc3-connected-vehicle-technology-demonstration-at-2012-annual-meeting-.

[79] B. Ostermaier, F. Dotzer, and M. Strassberger. Enhancing the Security of Local DangerWarnings in VANETs - A Simulative Analysis of Voting Schemes. In *ARES*, pages 422–431. IEEE Computer Society, 2007.

[80] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux. Secure Vehicular Communication

Systems: Design and Architecture. *IEEE Communications Magazine*, pages 100–109, 2008.

[81] P. Papadimitratos, L. Buttyan, J. Hubaux, F. Kargl, A. Kung, and M. Raya. Architecture for Secure and Private Vehicular Communications. In *The 7th International Conference on ITS Telecommunications (ITST)*, 2007.

[82] P. Papadimitratos, A. de La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza. Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation. *IEEE Communications Magazine*, 47(11):84–95, 2009.

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

[84] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha. A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks. In *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems*, pages 1–8, 2006.

[85] M. Peden, R. Scurfield, D. Sleet, D. Mohan, A. A. Hyden, E. Jarawan, and C. M. (eds.). *World Report on Road Traffic Injury Prevention.* Geneva, World health Organization, 2009. Available at http://whqlibdoc.who.int/publications/2004/9241562609.pdf. Last accessed on 30 September 2012.

[86] J. Pohl and J. Ekmark. *Development of a Haptic Intervention System for Unintended Lane Departure*, 2003. Proceeding of SAE World Congress, 2003-01-0282.

[87] D. Quick. *Worlds Largest Field Test of Connected Vehicle Technology Gets Underway in the U.S*, 2012. Last accessed on 21 February 2013. Available at http://www.gizmag.com/connected-vehicle-field-test-us/23817/.

[88] R. Ramanathan. Challenges: A Radically New Architecture for Next Generation Mobile Ad Hoc Networks. In *MOBICOM*, pages 132–139. ACM, 2005.

[89] M. Raya. *Data-Centric Trust in Ephemeral Networks.* PhD thesis, École Polytechnique Fédérale de Lausanne, 2009.

[90] M. Raya, A. Aziz, and J. Hubaux. Efficient Secure Aggregation in VANETs. In *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks*, pages 67–75. ACM, 2006.

[91] M. Raya and J. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceeding of SASN*, pages 11–21. ACM, 2005.

[92] M. Raya and J. Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[93] M. Raya, P. Papadimitratos, V. D. Gligor, and J. Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM*, pages 1238–1246. IEEE, 2008.

[94] R. Reinders, M. van Eenennaam, G. Karagiannis, and G. J. Heijenk. Contention Window Analysis for Beaconing in VANETs. In *IWCMC*, pages 1481–1487. IEEE, 2011.

[95] RITA. *Safety Pilot Program Overview*. Research and Innovative Technology Administration, U.S. Department of Transportation. Available at http://www.its.dot.gov/safetypilot/index.htm. Last accesed on 4 January 2013.

[96] R. L. Rivest, A. Shamir, and Y. Tauman. How to Leak a Secret. In *ASIACRYPT*, pages 552–565, 2001.

[97] S. Rosenblatt. *Car Hacking Code Released at Defcon*, 2013. Available at http://www.cnet.com/news/car-hacking-code-released-at-defcon/. Last accessed on 30 October 2014.

[98] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran. AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589, 2007.

[99] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schfer. *Vehicle Behavior Analysis to Enhance Security in VANETs*, 2008. Fourth Workshop on Vehicle to Vehicle Communications (V2VCOM 2008).

[100] SeVeCom. Secure Vehicular Communications: Security Architecture and Mechanisms for V2V/V2I, Deliverable 2.1. Available at http://www.sevecom.org. Last accessed on September 2011.

[101] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO*, pages 47–53, 1984.

[102] K. Shin, H. Choi, and J. Jeong. A Practical Security Framework for a VANET-based Entertainment Service. In *Proc. ACM International Workshop on Performance Monitoring, Measurement, and Evaluation of Heterogeneous Wireless and Wired Networks*, pages 175–182, 2009.

[103] M. L. Sichitiu and M. Kihl. Inter-Vehicle Communication Systems: A Survey. *IEEE Communications Surveys and Tutorials*, 10:88–105, 2008.

[104] A. Studer, F. Bai, B. Bellur, and A. Perrig. Flexible, Extensible, and Efficient VANET Authentication. *Journal of Communications and Networks*, 11(6):574–588, 2009.

[105] I. Teranishi, J. Furukawa, and K. Sako. k-Times Anonymous Authentication (Extended Abstract). In *ASIACRYPT*, pages 308–322, 2004.

[106] U. S. Department of Transportation. *Collaborative Connected Vehicle - Research Update*. The CAMP Vehicle Safety Communications Consortium, 2013. Available at http://www.its.dot.gov/presentations/pdf/V2V-Collaborative-Research-MikeLukuc-2013.pdf. Last accessed on 30 October 2014.

[107] U. S. Department of Transportation. *Governement -Industry Meeting. Crash Avoidance II: Connected Vehicles*. The CAMP Vehicle Safety Communications Consortium, 2013. Available at http://www.sae.org/events/gim/presentations/2012/finalpresentationschaffnit.pdf. Last accessed on 30 October 2014.

[108] UK Department for Transport. *Transport Statistics Great Britain 2012*, 2012. Available at https://www.gov.uk/government/publications/transport-statistics-great-britain-2012. Last accessed on 4 February 2014.

[109] D. O. U.S. Census Bureau, Washington. *TIGER / Line Database*, 2011. Available at: http:www.census.gov/geo/www/tiger.

[110] M. van Eenennaam, A. Remke, and G. Heijenk. An Analytical Model for Beaconing in VANETs. In *VNC*, pages 9–16. IEEE, 2012.

[111] M. van Eenennaam, W. K. Wolterink, G. Karagiannis, and G. Heijenk. Exploring the Solution Space of Beaconing in VANETs. In *Proceeding of IEEE Vehicular Networking Conference (VNC)*, pages 1–8, 2009.

[112] T. Watt. *SimTD - Biggest Ever Real-World Intelligent Vehicle Road Test*, 2012. Available at https://connect.innovateuk.org/web/intelligent-mobility/articles/-/blogs/9011911/maximized;jsessionid. Last accessed on 26 February 2013.

[113] WHO. *Global Status Report on Road Safety*. Geneva, World Health Organization, 2009. Available at http://whqlibdoc.who.int/publications/2009/9789241563840_eng.pdf. Last accessed on 30 September 2012.

[114] C. Winston. Efficient Transportation Infrastructure Policy. *Journal of Economic Perspectives*, 5:113–127, 1991.

[115] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu. Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication. In *International Communications Conference (ICC 2010)*, 2010.

[116] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in Mobile Ad Hoc Networks: Challenges and Solutions. *IEEE Wireless Communication*, 11(1):38–47, 2004.

[117] Z. Zhang, D. S. Wong, J. Xu, and D. Feng. Certificateless Public-Key Signature: Security Model and Efficient Construction. In *ACNS*, volume 3989 of *Lecture Notes in Computer Science*, pages 293–308, 2006.

[118] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty. P^2DAP - Sybil Attacks Detection in Vehicular Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 29(3):582–594, 2011.