SECURING ANONYMOUS AUTHENTICATED ANNOUNCEMENT PROTOCOL FOR GROUP SIGNATURE IN INTERNET OF VEHICLE

NUR AFIQAH BINTI SUZELAN AMIR

FACULTY OF SCIENCE
UNIVERSITI MALAYA
KUALA LUMPUR

2021

SECURING ANONYMOUS AUTHENTICATED ANNOUNCEMENT PROTOCOL FOR GROUP SIGNATURE IN INTERNET OF VEHICLE

NUR AFIQAH BINTI SUZELAN AMIR

DISSERTATION SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE

INSTITUTE OF MATHEMATICAL SCIENCES
FACULTY OF SCIENCE
UNIVERSITI MALAYA
KUALA LUMPUR

2021

UNIVERSITI MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **NUR AFIQAH BINTI SUZELAN AMIR**

Registration/Matric No.: **17036380/1 SGP160007**

Name of Degree: **MASTER OF SCIENCE**

Title of Thesis ("this Work"):

SECURING ANONYMOUS AUTHENTICATED ANNOUNCEMENT PROTOCOL FOR GROUP SIGNATURE IN INTERNET OF VEHICLE

Field of Study:

APPLIED MATHEMATICS

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: 1/4/2021

Subscribed and solemnly declared before,

Witness's Signature Date: 1/4/2021

Name:
Designation:

SECURING ANONYMOUS AUTHENTICATED ANNOUNCEMENT PROTOCOL FOR GROUP SIGNATURE IN INTERNET OF VEHICLE

ABSTRACT

The past decade has witnessed a growing interest in vehicular networking and its vast array of potential applications. Improved wireless internet connectivity from vehicles has prompted road safety technologies to emerge. Announcement protocol in Internet of Vehicles (IoV) is an intelligent application to improve road safety, relieve traffic congestion and enhance the comfort of transportation. IoV has drawn extensive attention to provide more enjoyable and safer driving environment. It requires communication between vehicles, roadside units and pedestrian to disseminate safety related messages. Vehicular cloud (VC) computing can guarantee reliable and timely broadcast of safety messages. The integration of IoV and VC may significantly reduce road casualities. However, as vehicles are connected to the internet, it makes them accessible globally to a potential adversary or malicious parties. Safety-related application requires a message to be reliable, however it may intrude the privacy of a vehicle. Contrarily, if some misbehaviour emerges, the trusted party (TP) must be able to trace and revoke their legitimacy from the network. This is a contradiction between privacy and accountability since the privacy of a user should be preserved. We begin by analysing some existing announcement protocol based on various cryptographic primitives in the literature for VC and IoV respectively and consider to what extent they achieve the conflicting security requirements of reliability, privacy and accountability. From our analysis, we discover that there is no group signature technique has been proposed in the literature. This highlights the need to design a secure and efficient announcement protocol based on group signature technique in IoV technology. We formulate a generic abstraction of an announcement protocol for group signature.

This generic abstraction aims to provide a basis for future construction of announcement protocol using group signature in IoV. To the best of our knowledge, our work is the first comprehensive construction of an announcement protocol in IoV that deploys group signature. We then analyse the security of our proposed protocol and evaluate its performance. We demonstrate that our protocol efficiently solves these conflicting security requirements of message reliability, privacy and accountability using 5G communication channel. The performance of our protocol is validated by simulations. The performance analysis and simulation results signify our work achieves performance efficiency in IoV communication.

Keywords: Announcement, group signature, vehicular communication, security.

PROTOKOL PENGUMUMAN PENGESAHAN TANPA NAMA YANG EFISIEN UNTUK TANDATANGAN BERKUMPULAN DALAM INTERNET KENDERAAN

ABSTRAK

Dekad yang lalu menyaksikan minat yang semakin meningkat dalam rangkaian kenderaan dan rangkaian aplikasi yang berpotensi. Sambungan internet tanpa wayar yang bertambah baik dari kenderaan telah mendorong teknologi keselamatan jalan raya. Protokol pengumuman di internet kenderaan (IoV) adalah aplikasi pintar untuk mempertingkatkan keselamatan jalan raya, kelancaran lalu lintas dan meningkatkan keselesaan pengangkutan. IoV telah menarik perhatian yang luas untuk menyediakan persekitaran pemanduan yang lebih menyeronokkan dan lebih selamat. Ia melibatkan komunikasi antara kenderaan, unit infrastruktur jalan dan pejalan kaki untuk menyebarkan mesej berkaitan keselamatan. Pengkomputeran awan kenderaan (VC) dapat menjamin penyiaran mesej berkaitan keselamatan yang boleh dipercayai dan tepat pada masanya. Penyepaduan antara IoV dan VC dapat mengurangkan kemalangan jalan raya dengan ketara. Namun, kerana kenderaan disambungkan ke internet, kenderaan tersebut dapat diakses secara global oleh pihak musuh atau pihak yang berniat jahat. Aplikasi berkaitan keselamatan memerlukan mesej yang diumumkan boleh dipercayai, namun ia boleh mengganggu privasi kenderaan. Sebaliknya, jika muncul salah laku, pihak yang dipercayai (TP) mesti dapat mengesan dan membatalkan penglibatan mereka dari rangkaian. Ini adalah percanggahan antara privasi dan akauntabiliti kerana privasi pengguna harus dijaga. Kajian dimulakan dengan menganalisis beberapa protokol pengumuman berdasarkan pelbagai primitif kriptografi yang terdapat dalam kesusasteraan untuk VC dan IoV dan mempertimbangkan sejauh mana mereka mencapai konflik keperluan keselamatan mengenai kebolehpercayaan, privasi dan

akauntabiliti. Dari analisis kami, kami mendapati bahawa tidak ada teknik tandatangan kumpulan yang telah diusulkan dalam kesusateraan. Kelompongan dalam kesusasteraan ini menekankan keperluan untuk merancang protokol pengumuman yang selamat dan efisien berdasarkan teknik tandatangan kumpulan dalam teknologi IoV. Kami merumuskan abstraks generik protokol pengumuman untuk tandatangan kumpulan. Abstraks generik ini bertujuan untuk menyediakan asas untuk pembinaan protokol pengumuman di masa depan menggunakan tandatangan kumpulan di IoV. Untuk pengetahuan, kajian kami adalah pembinaan protokol pengumuman komprehensif pertama yang menggunakan tandatangan kumpulan untuk teknologi IoV. Kami kemudian menganalisis keselamatan protokol yang kami cadangkan dan menilai prestasinya. Kami menunjukkan bahawa protokol kami dengan berkesan menyelesaikan konflik keperluan keselamatan mengenai kebolehpercayaan, privasi dan akauntabiliti mesej dengan menggunakan saluran komunikasi 5G. Prestasi protokol kami dibuktikan oleh simulasi. Hasil analisis prestasi dan simulasi menandakan hasil kajian kami mencapai kecekapan prestasi dalam komunikasi IoV.

Kata kunci: Pengumuman, tandatangan kumpulan, komunikasi kenderaan, sekuriti.

ACKNOWLEDGEMENTS

Alhamdulillah to the most gracious and mighty Allah S.W.T who has made this work possible. The past years have been thus far the most challenging, interesting, and rewarding part of my life. I am very thankful and grateful that I have crossed paths with many wonderful people who have helped me in many ways in my pursuit of a Master Degree. First and foremost, I would like to thank my supervisors, Dr. Amizah Malip and Associate Professor Dr. Wan Ainun Mior Othman, for their excellent supervision, teaching, guidance, patience and support in this research, and for getting me through the unlimited and vast world of thoughts towards completing my Master degree. My heartfelt appreciation goes to my beloved family for their continuous love and prayers which have given me the strength to complete this thesis. They are my motivation and inspiration. Their wholehearted encouragement and support led me to complete this research. Special thanks go to my friends and all ISM members in the department, who have helped and supported me over these years throughout this study

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

AC : Authentication Cloud

CC : Cloud computing

DLP : Discrete Logarithm Problem

DSRC : Dedicated Short Range Communication

ECU : Electronic Control Unit

EDR : Event Data Recorder

GPS : Global Positioning System

IoT : Internet of Thing

IoV : Internet of Vehicle

ITS : Intelligent Transportation System

OBU : On-Board Unit

PKC : Public Key Cryptography

TC : Tracing Cloud

TP : Trusted Party

TPD : Tamper Proof Device

RC : Registration Cloud

RSU : Roadside Unit

V2I : Vehicle-to-Infrastructure communication

V2P : Vehicle-to-Pedestrian communication

V2V : Vehicle-to-Vehicle communication

VANET: Vehicular Ad Hoc Network

VC : Vehicular Cloud

WAVE : Wireless Access Vehicular Environment

WHO : World Health Organization

CHAPTER 1: INTRODUCTION

In this chapter, we first define our research motivation. Then, we present an overview of vehicular ad hoc network (VANET), vehicular cloud (VC) and internet of vehicles (IoV). Lastly, we state the scope and contributions of our thesis.

1.1 Motivation

Over the past few years, the US Department of Transportation (US-DOT) reported that congested highways cost more than 75 billion in lost productivity for employees and more than 8.4 billion gallons of fuel in a single year because of several congestion incidents. The US-DOT also noted that over half of all congestion events are caused by highway incidents rather than by rush-hour traffic in big cities (WHO, 2015). The National Highway Traffic Safety Administration (NHTSA) also stated that densely populated highways are one of the major causes of accidents on the road. Extrapolating from January till September 2009 statistics, NHTSA predicted for 2009, an estimated 25,576 fatalities directly attributable to traffic-related incidents (Campbell et al., 2007). Road fatalities are the main cause of deaths and the tenth major cause of all deaths worldwide (Abueh & Liu, 2016; Eze et al., 2015). The United Nations announced the launch of Decade of Action (2011 – 2020) for Road Safety across the globe on 11_{th} May 2011. According to the NHTSA, there are about 43,000 people killed in car accidents each year in the United States and according to Road Safety in European Commission, there are about 35,000 people killed in car accidents each year in the European Union in every six seconds reported in (UNRSC, 2011). If current patterns persist, road traffic accidents are expected to be the third largest factor to worldwide disease and injury burdens by 2020. This emerging concern has attracted considerable interest for researchers in the construction of revolutionary technologies that will enhance the road safety.

The growing concern in road safety and traffic efficiency has drawn a significant interest towards the development of secure vehicular communications. This drives the evolution of transportation technology known as vehicular ad hoc network (VANET). VANET guarantees a secure and efficient driving environment by enabling vehicles to communicate with each other (V2V) and infrastructure (V2I) to enhance driving safety and traffic efficiency (L. Chen et al., 2011; Kounga et al., 2009; Malip et al., 2014; Raya, Papadimitratos, & Hubaux, 2006). However, VANET has lower capacity in terms of processing and computation for the future high-end vehicle technologies (Kaiwartya et al., 2016). Therefore, a new paradigm shift from conventional VANET to Internet of Vehicles (IoV) was envisioned. The IoV technology evolves from Vehicular Cloud (VC)(Ahmad et al., 2012; Alzain et al., 2013; Y. Argawal et al., 2018; L. Chen et al., 2011; Foster et al., 2009; Ghafoor et al., 2013; Marston et al., 2011; Ruj et al., 2014; Zissis & Lekkas, 2012). VC assists in the reliable and efficient delivery of safety messages. It permits to capitalize by accessing underutilized resources available on neighbouring vehicles. The incorporation of IoV and VC technologies has a great impact on daily life. It will help to manage traffic and reduce the occurrence of the road casualties. The vehicular connectivity of Internet of Things (IoTs) gives rise to IoV. IoV is inseparable components of a smart city environment due to its role to improve life quality, safety and security. This new trendsetter technology has significant impact and the potential to improve road safety and traveling experience in the future. Studies have shown that more than 60 percent of network traffic incidents could be avoided if drivers are notified of a car accident at least 500 milliseconds (ms) in advance (Eze et al., 2014) therefore, IoV is a very appealing emerging technology due to its characteristics and capabilities in supporting a safety-related applications.

1.2 Objectives

In this thesis, we design a secure and efficient announcement protocol where our work is a modification and extension of MLGS scheme (Q. Wu et al., 2010). To the best of our knowledge, our work is the first comprehensive construction of an announcement protocol using group signature that resolves the conflicting security requirements of message reliability, privacy and accountability in IoV. Our objectives are as follows:

- To construct a generic abstraction of an announcement protocol where the underlying cryptographic primitive is based on group signature.
- To design a secure announcement protocol for IoV under the precondition of enhancing safety and privacy preserving while attaining the feature of accountability.
- To prove the practicality and applicability of our protocol in real world deployment and achieve good performance efficiency without compromising security using 5G communication channel.

1.3 Problem Overview

Despite the advantages of IoV, security and privacy matters need to be addressed for the conception idea of IoV is to be widely accepted and adopted. Hence, a sophisticated security and privacy preservation approach are demanded to attract vehicles and pedestrians to participate the network. Due to its globally accesible, the network is vulnerable to an adversary or malicious parties. An adversary may cause harmful effects that could potentially threaten the life of other users in the network. Announcement protocols in IoV permit vehicles to broadcast and inform neighboring vehicles and pedestrians regarding safety related announcements such as traffic delays, injuries, potholes and hazardous roadways. This enables vehicles and pedestrians to be aware of their surrounding environment, make decisions and take appropriate actions accordingly upon assessing the

situation. In order to fully utilize IoV, the transmission of safety messages must reflect the actual situations while preserving the privacy of vehicles at the same time. However, verification of message reliability may allow irresponsible parties to track vehicles or pedestrians for *profiling*. Profiling is the activity of collecting confidential information that may lead to the true identity of the sending vehicle. On the other hand, in a situation where a misbehaved vehicle acts maliciously, there must be a mechanism to allow the TP to trace and identify the vehicle's identification for law enforcement purposes. Furthermore, the misbehaved vehicle could not repudiate of sending the message. The presence of adversaries in the network is a common assumption in vehicular communications (L. Chen et al., 2011; Joy & Gerla, 2017; Li et al., 2012; Malip et al., 2014; Raya, Papadimitratos, & Hubaux, 2006; Sun et al., 2015; Q. Wu et al., 2010). There are two categories of adversaries: external and internal. External adversary is a malicious entity that is not equipped with credentials to participate in the network. Meanwhile, an internal adversary is a legitimate malicious participant who possesses valid credentials issued by the TP in the network. Hence, IoV security and privacy issues are very important to take place in order to gain broader acceptance towards this technology. The following are examples of some consequences:

- If message reliability is not provided, a malicious vehicle might inject the false message or modify the content of a message to fool other vehicle. By doing so, the public safety will be compromised and the goal of safety application cannot be fulfilled as the intended vehicle could not utilized the broadcasted message.
- If privacy is not supported, it might lead to the deployment vulnerable network in which the irresponsible entity can easily trace the identity of the senders. Hence, it will discourage the participant to participate in the network.
- If accountability is not demonstrated, a malicious vehicle can anonymously an-

nounced the fraudulent message without the fear of being caught.

1.4 Vehicular Ad Hoc Networks (VANETs)

A vehicular ad hoc network (VANETs) consists of groups of moving or stationary vehicles connected by a wireless network. VANETs have a wide variety of potential applications. These applications are classified into two categories: application related to safety and application not related to safety (Raya, Papadimitratos, & Hubaux, 2006). In application related to safety, vehicles broadcast warning signals or beacons to notify vehicles of traffic conditions such as congestion and accidents (L. Chen et al., 2011; D. He et al., 2015). Meanwhile, for application that not related to safety, called infotainment services, include certain types of applications include payment systems, internet connectivity, places, and toll systems.

1.4.1 Entities

A VANET comprises of three main entities: vehicles, roadside units (RSUs), and trusted parties (TPs). Each entity is described below.

1.4.1.1 Vehicle

Vehicles in VANET are smart vehicles because they are equipped with computing, processing, positioning, and location capabilities shown in Figure 1.1. Besides, they can run wireless networking protocols (Raya, Papadimitratos, & Hubaux, 2006).

Vehicle's On-Board Unit (OBU) is a central computing platform connected with the wireless communication facilities and other devices like: sensors and data recorders. Some of the most used devices are:

1. Event data recorder (EDR): to record the vehicle data for crash reconstruction or determination of the misbehaved vehicles.

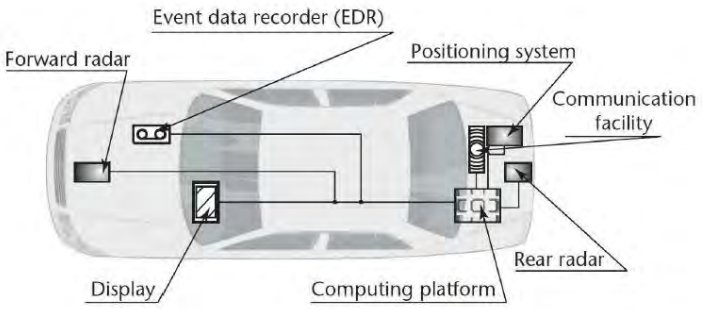

Figure 1.1: Smart Vehicle.

2. GPS receiver: to get the current position of the vehicle.
3. Front-end and rear radars: for detecting obstacles at front and rear of vehicle. They can be used for parking.

In our work, we assume that each vehicle in the network is equipped with a computing device called an onboard unit (OBU). An OBU has wireless communication capability that consist of Event Data Recorder (EDR), which records received messages. In addition, we assume that Tamper Proof Device (TPD) is embedded as part of OBU that implements cryptographic tools and ensures authenticated access control.

1.4.1.2 Roadside Unit (RSU)

In the traditional VANET, a RSU is a physical system situated at stationary locations along highways and roads or at particular locations including gas stations, car parks and restaurants. An RSU is equipped with at least a wireless communications network system to engage in the VANET. The main functions of the RSUs are listed as below (Park et al., 2011).

- Expanding an ad hoc network's contact spectrum through redistributing information to certain OBUs and coordinating with other RSUs in the transmission or dissemination of safety information.

- Operating safety applications.
- Providing internet connectivity to OBU.
- Performing as gateways to servers and authorities.

1.4.1.3 Trusted Parties

The TPs are responsible for managing vehicle's admission into the system and revoking dishonest vehicles. It is accountable for the issuing out and managing of credentials. The identity of a misbehaved vehicle will only be revealed by a TP when the vehicle is found to be malicious. In our work, we rely on a cloud network that plays the role of a trusted party (TP). The cloud also computes and verifies the reliability of safety messages. This may reduce the computational burden on V_r as we utilize the functionality of the cloud. In the literature, the TPs are commonly referred to as certification authorities (CAs) (Kounga et al., 2009; Raya, Papadimitratos, & Hubaux, 2006; Sahbi et al., 2018), tracing manager (TM) (Q. Wu et al., 2010) and reputation server (RS) (Li et al., 2012; Malip et al., 2014).

1.4.1.4 Communication Channel

A fifth generation (5G) wireless technology is adopted to support V2V, V2R and V2P communications in IoV. 5G is designed to achieve high data-rates (up to 20 Gbps) and provides a latency of 1 ms for real-time applications (Ferrag et al., 2018). The coverange of 5G is up to 30km for vehicle and pedestrian to communicate (Hussain et al., 2019).

1.5 Cloud Computing

Cloud Computing (CC) has changed the computing and networking by decoupling the physical infrastructure's digital assets and thus allowing virtualisation (Armbrust et al., 2010). The main motivation of the cloud computing is to "exactly what you need and when you need". CC offers practically unlimited capacity at very low accessible rates

and there are many cloud services providers on the market like Amazon, Microsoft, and Google (Hussain & Oh, 2014; Hussain et al., 2015, 2012; Oh & Hussain, 2014).

1.5.1 Cloud Services

The cloud services is consist of three basic delivery models which are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) (Hussain et al., 2012) represent in Figure 1.2. The top model is known as Software as a Service (SaaS). This layer provides internet-based software to users. The advantage of the service is that the customer does not have to incur the upfront costs for licensing the hardware or software. The by far best example of this service is the Google Drive. Google provides the aforementioned service to its user for free and as long as the user have internet connection, he/she can always utilize the service provided.

Platform as a Service (PaaS) is the second type of service that provides the framework for users to create, run and manage apps (Iqbal et al., 2016). This enables the service provider run the customer remotely. This form of service usually works well at the enterprise level and the best example is Google App Engine.

At the last level of the service of CC provides is Infrastructure as a Service (IaaS) (Dillon et al., 2010). IaaS offers storage or network resources for the infrastructure, space, servers, and data center, it may also incorporate software.

1.6 Vehicular Cloud

VC evolves with two emerging paradigms: VANET and cloud computing (CC). Research in CC has attracted a lot of attention from governments, research institutes and industry leaders (Ahmad et al., 2012; Alzain et al., 2013; Y. Argawal et al., 2018; L. Chen et al., 2011; Foster et al., 2009; Ghafoor et al., 2013; Marston et al., 2011; Ruj et al., 2014; Zissis & Lekkas, 2012). CC technologies have the potential to improve road safety and

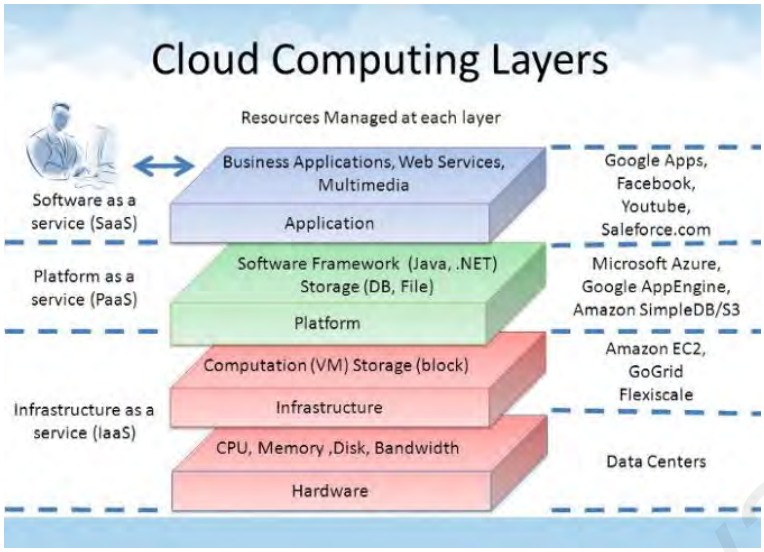

Figure 1.2: CC Services.

traveling experience for extended VANETs solution where it distribute the level of services to users outside of the cloud via virtualization. Services such as computing resources, networks, storage, servers, and applications can be delivered on demand to the users. A number of literatures have presented the notion of VC by incorporating conventional VANET to cloud computing (CC) (Hussain et al., 2013; Hussain & Oh, 2014; Hussain et al., 2015, 2012; Oh & Hussain, 2014; Olariu et al., 2011; Yan et al., 2009, 2013). Olariu *et al.* (Olariu et al., 2011) introduced the concept of VC as a group of vehicles whose pooled computing, sensing, communication and physical resources can be dynamically distributed to legitimate vehicles. In order to prevent under-utilized resources, the owner of the vehicles may rent out their resources capacity on demand to fully utilize their resources efficiently. Yan *et al.* (Yan et al., 2013) theorized VC as combining resources and assemble information dynamically while being in motion. Vehicles can acquire the cloud services ubiquitously, depending on their need. As a result, the vehicular resources can be distributed or rented out among different users. Hence, no vehicle can be considered as underuse.

1.7 Internet of Vehicles

The Internet of Vehicles (IoV) is a network system that facilitates the use of information generated by connected vehicles and vehicular ad hoc networks (VANETs). The key concept of IoV is to provide interconnectivity with other devices and things of the communication network (Stergiou et al., 2018). This interconnectivity of things will not only enable connectivity between devices and objects, it will also provide information to the interconnected things and make their information available to be used by other entities in the system (Akpakwu et al., 2018). Consider the following scenario:

" Suppose an upcoming vehicle is passing a parked vehicle in basement car park area. A pedestrian who fully blocked by the parked vehicle intends to cross. However, neither the upcoming vehicle nor the pedestrian has an obstructed view due to the occluded parked vehicle. The parked vehicle also affect the sensors installed in the upcoming vehicle where there exist a restriction of their direct line of sight to the pedestrian. Hence, that would be a potentially dangerous situation for both upcoming vehicle and a pedestrian ". This instance of a scenario, gives rise to IoV (Figure 1.3). IoV permits V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interconnectivity, thereby creating an intelligent network for each entities to communicate with each other (Cui et al., 2018; Storck & de L. P. Duarte-Figueiredo, 2019). As a predominant technology, IoV is regarded as likely to provide optimistic solution to revolutionize transportation systems and automobile services. It is a fusion of three networks namely: an inter-vehicle network, an intra-vehicle network, and vehicular mobile internet.

Inter-vehicle network provide communication among vehicles via wireless communication. Meanwhile, intra-vehicle network is an exchange of data within the electronic control unit (ECU) where an ECU is an embedded system in vehicle that controls one or more subsystems. Vehicular mobile internet is referred to as a vehicle being connected to internet

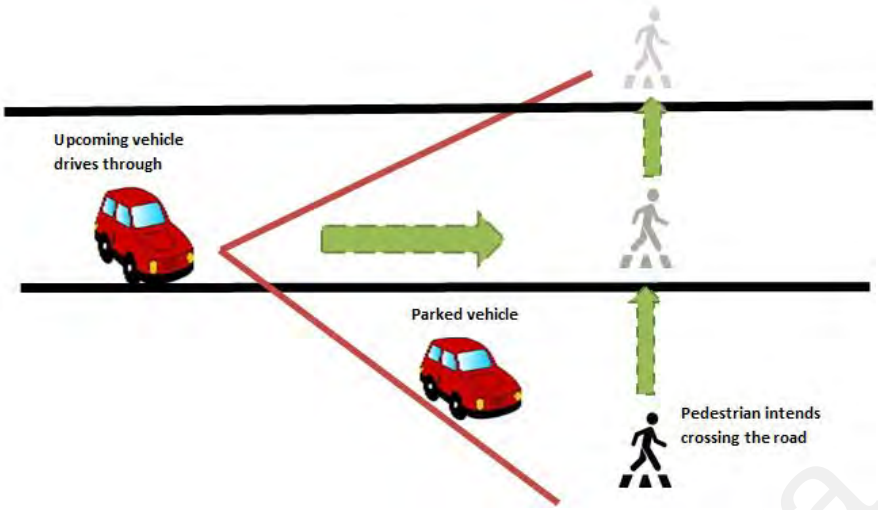

Figure 1.3: A scenario in IoV

in IoV. The convergence of three networks leads to a broad decentralized system for wireless communication and the dissemination of information among vehicles highways, people and the internet. With IoV paradigm, vehicles are equipped with an established internet protocol (IP) communication and data interaction standards (such as IEEE 802.11p WAVE standard, and cellular technoloy, e.g 4G or 5G). Such network integration supports safety applications in particular intelligent traffic management, intelligent dynamic information service, and intelligent vehicle control.In IoV, every network entity functions as such a "smart" object and may employ pervasive internet connectivity that allow people, objects, vehicles, systems and infrastructures to be integrated in order to create an artificial network that provides different services (Talib et al., 2018).

Security and privacy issues have attracted wide attention in IoV (C. Chen et al., 2019; Cui et al., 2018; J. Liu et al., 2018; Y. Liu et al., 2017; Sahbi et al., 2018). As vehicles connected to the internet, it makes them vulnerable to an adversary or malicious parties. An adversary may cause harmful effects that could potentially threaten the life of other users in the network. For instance, they may install malicious input onto vehicles and downloading infected files that may affect the whole network relatively quick (Talib et

al., 2018). If a network intrusion occurs in IoV, vehicles may be under the control of an adversary. A malicious attacker controlling the data system of a vehicle using malwares or any other means could fully exploit any various subsystems of the vehicle, such as the safety system. Scalability, interoperability, reliability, efficiency, availability, and security can be challenging to achieve in IoV environment due to its globally internet connectivity. A comparison of IoV, VANETs and VC is provided below in Table 1.1.

1.7.1 Security mechanism in IoV

In order to benefit from the rich tools of IoV, vehicles must consider a number of security requirement to fully utilize its safety applications (L. Chen et al., 2011; Li et al., 2012; Malip et al., 2014; Raya, Papadimitratos, & Hubaux, 2006; Q. Wu et al., 2010). A safety message is considered reliable if:

- Messages announced by legitimate vehicles using valid credentials provided by a trusted party (TP) in the network.
- The integrity of the message is preserved.
- The reliability of a message is measured (Li et al., 2012; Malip et al., 2014).

We consider the privacy necessity, since this is one of the important reasons for IoV deployment. Exchange of information on the network should be anonymous and untraceable where no user information can be exposed. Information associated to user privacy should be preserved in the existence of a malicous parties. In order to make the network resilient to vulnerable attacks, it must fulfill the accountability requirement. If any dispute arise, the vehicle could not deny having sent message and traceable. If proven misbehaved, it will be revoked from further participation in the network.

1.8 Scope and Contribution of the Thesis

The scope of the thesis focuses on authentication protocol in IoV. Due to life critical and time sensitivity, millions of safety messages must be processed in a very short time in IoV. Vehicle's privacy is another crucial concern in IoV in which vehicle's identity is anonymous and messages announced by a vehicle is unlinkable. At the same time, if there is an evidence of misbehaviour, the user will be kept accountable for public safety. This contradictory security requirement is a non-trivial concern in case of dispute. Thus, it is a significant challenge to design a secure announcement protocol for IoV under the precondition of enhancing safety and privacy preserving while attaining the feature of accountability. To meet this challenge, we propose a new efficient announcement protocol for IoV. In short, our work posesses the appealing features below:

- We construct a generic abstraction of an announcement protocol for group signature. This generic abstraction aims to provide a basis for future construction of announcement protocol using group signature in IoV. As far as we are aware of, this is the first construction of such abstraction proposed in the literature for IoV.

- We design the first comprehensive construction of an announcement protocol in IoV using group signature that possesses the remarkable features of message reliability, privacy and accountability simultaneously. The main advantage of group signatures is that vehicles only need to store a key pair, thereby overcoming the drawback of a large number of anonymous certificates being pre-stored.

- We provide an analysis that shows our protocol achieves efficient security level, system robustness and performance efficiency. We then run our protocol on a network simulator NS-2.35. This simulation demonstrates the practicality of our

work in real world implementation.

1.9 Organisation of the Thesis

This thesis consists of five chapters. Chapter 1 presents an introduction to this thesis, while the other chapters are organised as follows:

Chapter 2 (Literature Review). This chapter analyses the security requirement goals for the design of an annoucement protocol in IoV. We then examine authentication protocols in some recent announcement schemes based on different cryptographic primitives in VC and IoV paradigm. We discuss the advantages and disadvantages of the protocols and summarize each protocol at the end of the section.

Chapter 3 (Cryptographic Tools). In this chapter, we introduce the cryptographic primitive used in our work, that is, group signature. Then, we provide some mathematical background underlying the construction of our work in the thesis.

Chapter 4 (Securing Anonymous Authenticated Announcement Protocol for Group Signature in Internet of Vehicle). In this chapter, we design a generic abstraction of authentication announcement protocols for group signature. This abstraction then serves as a guideline for our new announcement protocol for group signature schemes in IoV. The performance analysis and simulation signify our work is secure and robust against adversaries and achieve good performance efficiency in the IoV communication. The work presented in this chapter has been submitted to an ISI journal as stated below:

- N. A. S. Amir, A. Malip and W. A. M. Othman, "Securing Anonymous Authenticated Announcement Protocol for Group Signature in Internet of Vehicles," KSII Transactions on Internet and Information Systems, vol. 14, no. 11, pp. 4573-4594, 2020. DOI: 10.3837/tiis.2020.11.018.

Chapter 5 (Conclusion and FutureWork). This chapter summarizes our contributions and we discuss some future directions of the research.

Table 1.1: Comparison of IoV, VANET and VC

Aspects	IoV	VANET	VC
Objectives	Traffic safety, efficiency and infotainment (Cui et al., 2018; Kang et al., 2018; Yang et al., 2015)	Traffic safety, efficiency and infotainment (L. Chen et al., 2011; Li et al., 2012)	Traffic safety, efficiency and infotainment (Boukerche & Grande, 2018; Hussain et al., 2013)
Network architecture	Collaborative networking between a variety of networks connected to the Internet (Sahbi et al., 2018)	Limited network architecture due to neighboring vehicles and infrastructure communication only (Kaiwartya et al., 2016)	The VC is temporarily created by interconnecting resources available in the vehicles and infrastructure (Lee et al., 2014)
Communication types	Four types of communication (V2V, V2I, V2P,V2S) (Eze et al., 2015)	Two types of communication (V2V, V2I) (Malip et al., 2014)	Two types of communication (V2V, V2I) (Hussain et al., 2013)
Mobile Device Compatability	Personal devices are compatible with the network and able to communicate with vehicles (Kaiwartya et al., 2016)	Not compatible between personal devices and network due to limited network architechure (Spelta et al., 2010)	Both mobile phones and vehicles can unload tasks into another vehicle or infrastructure(Ahmed et al., 2019).
Processing capacity	Use of cloud for storing, processing and analyzing the obtained information (Contreras-Castillo et al., 2018)	Lower capacity in terms of processing and computation capacity (W. He et al., 2014)	The best processing capacity available due the on demand cloud based service (Kaiwartya et al., 2016)
Decision Analytics	Decision making based on artificial inteliigence and critical analysis (Jameel et al., 2019)	Decision making based on simple and logical computation (Kumar et al., 2015)	Decision making based on high computation of cloud services (Oh & Hussain, 2014).
Application Service	Efficient and reliable due to stability internet connectivity (Kaiwartya et al., 2016)	The network channel is based on dedicated short range communication (DSRC) where it delivers in close proximity and tight latency (Hartenstein & Laberteaux, 2010)	Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) (Hussain et al., 2013; Oh & Hussain, 2014)

CHAPTER 2: LITERATURE REVIEW

In this section, we review announcement protocols particularly for VC and IoV. We discuss in detail the component of security requirement. We examine multiple scheme under each cryptoraphic primitive and analyse how these security requirements are achieved. We then summarize and examine the extent of security of these announcement protocols.

2.1 Requirement of Anonymous Authenticated Announcement Protocol in IoV

2.1.1 Reliability of message

To acquire universal acceptance towards this deployment of technology, building trust is vital in IoV network. It is fair to say that vehicles have no trust relationship with each other (Malip, 2014). Digital signature technique is commonly used to solve the first two requirements of message reliability. Signing a message using valid credentials from a TP assures sender's authenticity and data integrity. However, verification of message trustworthiness may allow irresponsible parties to track vehicles for profiling.

To achieve the last requirement, the threshold method (L. Chen et al., 2011; Daza et al., 2009; Kounga et al., 2009; Raya, Aziz, & Hubaux, 2006; Q. Wu et al., 2010) and reputation system (Bermad et al., 2019; Malip, 2014) are among the common techniques adopted in announcement protocols for vehicular communication. Reputation system is based on an evaluation of parameterized feedback messages represented by a numerical score. A message is considered reliable if the vehicle that generates the message has sufficient high reputation and vice versa. We focus on threshold method where an announced message is considered to be reliable if a number of different legitimate transmitters of a certain threshold reported the same event. However, the threshold method requires distinguishability of message origin where a verifier could verify whether the same signer

produces two distinct signatures on that same message and that the message can be linked. This contradicts with privacy. Hence, this presents a challenging security concern in which message reliability checks may reveal the real identity of the sender. Thus, protecting vehicle's privacy is indispensable in IoV network where vehicle's identity and messages announced should be preserved and unlinkable respectively.

2.1.2 Privacy

Privacy is the critical concern in IoV. If the privacy is not preserved, the actual identification of a vehicle can be exposed to other participants and jeorpadize the safety of other vehicle in the network. In addition, there might be situations required by a law enforcement authority to traced down the identities of the vehicles in the incident proximity for the purpose of investigation. This demonstrates that, privacy should be delicately balanced before IoV can obtain extensive approval. The other significant privacy concerns are; anonymity and unlinkability. Anonymity indicates a sender's identity is hidden to others within the network. Meanwhile, unlinkability implies that the activities cannot be linked to its source where an entity could not determine whether two messages originate from the same vehicle or not. However, message verification may violate vehicle's privacy by revealling some information about the sender's identity. Thus, the protection of user privacy is thus a matter of great importance in IoV.

2.1.3 Accountability

In a pervasive IoV environment, there have possibility misbehaviour arises among users that would make the network is vulnerable to attacks. This will harm public road safety and would render the deployment of this technology. In such situations, the necessity to achieve accountability requirement is desirable. However, it contradicts the privacy requirement where it allows the TP to trace and revoke a malicious vehicle by opening

the signature (L. Chen et al., 2011; Q. Wu et al., 2010). Non-repudiation can be satisfied if the originator of the message disavows to send a signed message using an anonymous credential that belonged solely to the vehicle (Song et al., 2019). One of the common ways to revoke misbehaved vehicles is by updating and distributing certificate revocation lists (CRLs) across the network. At the same time, the authorities can also disclose the vehicle's identity (Malip, 2014).

2.2 Review of Announcement Protocol

In this section, we review schemes based on anonymous authenticated announcement protocol in IoV. In the first part, we classify recent protocols according to their cryptographic primitives, including "traditional" public key cryptography, identity-based cryptography and symmetric key cryptography. We then examine and analyse the extent to which they satisfy the main component of security requirement which are reliability, privacy and accountability. We then summarize the shortcomings of existing announcement protocols in literature.

2.3 Announcement Protocol in "Traditional" Public Key Cryptography

"Traditional" public key cryptography (PKC) is well-explored method in VANETs (Raya & Hubaux, 2007; Raya, Papadimitratos, & Hubaux, 2006) for security purposes, especially for roadside infrastructure. Public key cryptography requires two keys which are private key and public key. These two keys are mathematically related. A private key is used to digitally sign a message, while a public key is used to validate digital signatures. The public key can be shared and seen by everyone and private key is kept hidden from other entities in the network. A public key is associated to a user by a certificate, which is the signature of the trusted party (TP) on the public key. This certificate is used by verifiers to check the validity and can uniquely identifies the real identity associated to a signer.

The TP is responsible to store all the issued certificates to allow traceability in case of misbehaviours. We review some announcement protocols based on the "traditional" public key cryptography in VC and IoV (Cui et al., 2018; Hussain et al., 2013; Hussain & Oh, 2014; Hussain et al., 2015, 2012; Kang et al., 2018; J. Liu et al., 2018; Oh & Hussain, 2014; Sahbi et al., 2018; Yan et al., 2009, 2013).

2.3.1 Security challenges in vehicular cloud computing

Yan *et al.*(Yan et al., 2009, 2013) extend the work of (Scott & Denning, 2003) and presented on efficient location based encryption called Geoencrypt using symmetric algorithm. Their concept is using a vehicle's geographical location to produce the private key distributed by the TP to sign messages, hence guarantees the authenticity of the sender and integrity of the message. However, it cannot be used in threshold mechanism where distinguishability of message origin is not satisfied. Anonymity is adressed by employing pseudonym changing based authentication technique. This results in the identity of the signer being kept private where pseudonym are changed and updated regularly. Each pseudonym may be used once at a time or has a short lifetime subjected to its privacy requirement. The limitation of this scheme is that a frequent interaction between vehicles and TP is required for symmetric key authentication every time vehicles want to sign a message. The accountability requirement is not satisfied where the integrity and origin of data cannot be guaranteed.

2.3.2 Cooperation-aware vanet clouds: Providing secure cloud services to vehicular ad hoc networks

A different variation of location based encryption scheme were proposed in (Hussain et al., 2013; Hussain & Oh, 2014; Hussain et al., 2015, 2012; Oh & Hussain, 2014) which are an enhancement of (Yan et al., 2013). Hussain *et al.* envisioned geolock encryption where the key generation solely relies on the location information. This scheme

achieves message authentication as a message is signed and generated only by a valid legitimate vehicle who possess valid credential from TP. Matter of privacy was adressed by introducing identityless beacon messages, which is known as Mobility Vectors (MVs). The requirement of anonymity and unlinkability is achieved using MVs that does not contain any identifying information that associate a message to the sender. However, the message origin is indistinguishable. For the same message, a signing vehicle can disguise as multiple vehicles, resulting in Sybil attack. Therefore, threshold mechanism cannot be adopted. In order to protect against adversary, their scheme adopt the traditional method of revoking certificates by distributes certificate revocation lists (CRLs) across the network.

2.3.3 A network model for internet of vehicles based on SDN and cloud computing

Sahbi *et al.* (Sahbi et al., 2018) presented an announcement scheme for IoV based on public key cryptography. A TP generates a pair of public and private key together with certificates during the preliminary phase. The RSU is involved in message broadcast phase by assigning a pair of keys to a vehicle who enters its communication range. The vehicle then uses the pair of keys to communicate with each other in its domain. This scheme fulfill the property of message authentication. However, the third requirement of message reliability is not satisfied where the origin of message is indistinguishable. A threshold mechanism cannot be adopt in this scheme. Matter of privacy and accountability has not been discussed in (Sahbi et al., 2018) which may render the scheme inefficient.

2.3.4 An efficient anonymous authentication scheme for internet of vehicles

In (J. Liu et al., 2018), an anonymous authentication protocol based on certificateless short signature scheme (CLSS) was proposed. The protocol consists of four parties which are the vehicles, the RSUs, the transportation control center (TCC), and the trace back authority (TBA). The TCC generates the key pair and choses an encryption algorithm based

on elliptic curve cryptography (ECC) and a message authentication code (MAC). At the same time, TCC maintains the revocation lists. A vehicle signs a message using a legitimate credential issued by TCC, therefore satisfy the requirement of message authentication. A RSU acts as a regional management strategy. The same public and private key pairs are distributed to RSUs in the same wireless area. When a vehicle enters a new area, RSUs will issue the broadcasted public key. If a vehicle broadcasts a false message, the TCC will send the vehicle's service request message to TBA. If proven misbehaved, TCC can reveal the real vehicle's identity. In terms of privacy, anonymity is achieved using pseudonyms that does not contain information associated to sending vehicle. A message is signed using a one-time pseudonym, thus satisfy unlikability requirement. However, the protocol could not provide the evaluation of message reliability where the origin of message is indistinguishable. Therefore, threshold mechanism cannot be adopted in this scheme.

2.3.5 Privacy preserving authentication using a double pseudonym for internet of vehicles

Cui *et al.* (Cui et al., 2018) proposed privacy preserving authentication using a double pseudonym for IoV. This scheme adopt batch authentication to evaluate message reliability. Each vehicle generates its own pairwise public and secret key together with corresponding certificates preloaded by TP to sign a safety message. Signing a message using valid credential from TP satisfy the first two requirement of message reliability. This scheme achieve anonymity by using pseudonym. Message is linkable for a short time, where vehicles change and update pseudonym regularly. Issue arise in this scheme is where the vehicles need to regenerate its private key whenever it wants to sign a message. This require periodic credential verification from TP, thus render (Cui et al., 2018) to be impractical. Moreover, the drawback of batch authentication is that message origin cannot distinguish. Therefore, the threshold technique cannot be used in this scheme.

2.3.6 Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles

Fog-computing supported IoV known as F-IoV was proposed in (Kang et al., 2018). Fog computing is the extension of CC that consist of multiple edge nodes directly connected to physical devices. This scheme proposes the privacy-preserving pseudonym (P_3) scheme to protect wireless communication security and trace misbehaved vehicles. Each vehicle initially receives its public and private key pairs, and short-term certificates from TP. Message is signed using valid credentials via a secured communication channel from TP satisfy the requirement of message authentication. The TP stores all the issued certificates to allow traceability in case of misbehaviours. In order to achieve the need of privacy, each psedonymn will be changed and updated subjected to its privacy requirement. However, the origin of message is indistinguishable. This indicate threshold mechanism cannot be adopted in this scheme.

2.4 Announcement Protocol in Identiy based Cryptography

In 1984, Shamir introduced the notion of identity-based cryptography (IBC) in which the public key of a user may be his real identities, such as names, email addresses or phone numbers, to replace the use of certificates to announce safety messages. This identity-based setting gets rid of the public key management and, therefore, simplifies the "traditional" PKC requirements. In this primitive, a trusted party (TP) is required to compute a private key that corresponds to a particular public key. This TP has to be completely trusted as it is in possession of the vehicles private keys. We review announcement protocols based on identity-based schemes in (R. Argawal et al., 2019; C. Chen et al., 2019; Jiang et al., 2018; Y. Liu et al., 2017; Vasudev & Das, 2019; Zhang et al., 2020).

2.4.1 Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud

In (Zhang et al., 2020), Zhang *et al.* presented a secure and privacy-preservation communication scheme using the combination of identity based and public key cryptography in VC . An authentication based on an asymmetric group key agreement (AGKA) protocol and a location based encryption (LBE) scheme were provided in which the TP is considered to be completely trusted. A TP generates a pool of one time use pseudonyms and the corresponding private keys for each vehicle to sign a safety message. The requirement of message authentication is achieved in this scheme. Such pseudonyms are used to safeguard vehicle's privacy. Therefore, fulfill the requirement of privacy. However, the reliability of message cannot be measured where the source of message is indistinguishable. Hence, threshold method cannot be implemented in this scheme. In addition, there has been no discussion of the issue of accountability in (Zhang et al., 2020) which could make the scheme inefficient.

2.4.2 Integrated authentication and key agreement framework for vehicular cloud computing

To achieve conditional privacy-preserving (CPP) Jiang *et al.* (Jiang et al., 2018) proposed integrated authentication and key agreement (AKA) framework for VC. The underlying cryptographic primitive is based on identity cryptography. During the registration process, vehicles present their identity, which serves as the public key and receive the corresponding private key and smart card associated to its true identity. Then, vehicle sign a message using the smart card where satisfies the requirement message authentication. This scheme introduced another scenario of privacy protection where TP must extract the signer of valid message with valid signature. However, the possibility of tracking malicious behavior becomes a quite challenging. Furthermore, the threshold mechanism cannot be adopted in this scheme where the origin of a message is indistinguishable. The explicit issue of

accountability is not being addressed in this scheme.

2.4.3 Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm

Liu *et al.*(Y. Liu et al., 2017) designed an efficient and privacy-preserving dual authentication and key agreement (PPDAS) scheme for a secure V2V communications. A ID based authentication was presented where the TP is assumed fully trusted. Message signed using valid credentials from TP assures message authentication. Node reputation evaluation is adopted to measure the trustworthiness of the safety message where vehicle scores each other according to the reliability of message announced. The role of RSU is needed to issue a session key to protect the privacy of the vehicle. However, this signify computation reliance on the infrastructure. In our work, RSU only needs to relay information and to provide a gateway between a TP and vehicles. The requirement of privacy is satisfied by the use of pseudonym that is updated dynamically according to the degree of privacy required by a vehicle. Nevertheless, this scheme assume TP is fully trusted. The requirement of non-repudiation is not satisfied as the vehicle is not the sole holder of the signing key.

2.4.4 An efficient authentication and secure vehicle-to-vehicle communications in an IoV

In (Vasudev & Das, 2019), Harsha *et al.* proposed an announcement authentication scheme for IoV based on identity based cryptography. This scheme focuses on V2V communication where it exploit the advantage of IoV where vehicles can broadcast message directly to TP via IP network during emergency situation. A tamper proof device (TPD) is used to generate pseudo-identities for a vehicle associate to the real identity of vehicle. The vehicle then uses the pseudo-identities to generate a signature on a message. This satisfy the property of message authentication. Threshold adaptive authentication cannot be

adopted in this scheme where the origin of the message cannot be distinguish. Anonymity and unlikability are satisfied where each vehicle generate its unique secret key preloaded in the vehicle's TPD. However, identity-based suffers key escrow problem where the TP has to be completely trusted as it is in possession of the vehicles private keys.

2.4.5 Identity-based security scheme in internet of vehicles

Argawal *et al.* (R. Argawal et al., 2019) proposed identity based security scheme in IoV. Each vehicle is equipped with a TPD. A TPD is used to generate secret key and its matching public key preloaded into the device and stored in the TP. The matching public key allows the TP to retrieve the real identity of a vehicle in case of misbehaviours. The vehicle then uses the anonymous ID to sign a safety message. This scheme fulfiill the requirement of message authentication. It could not however distinguish whether the same vehicle signed two messages or not. This indicate threshold mechanism cannot be used in this scheme. For privacy, the short term anonymous credentials are replenished whenever it enters a new RSU domain. Each vehicle generates a new secret key to sign a message then forward to TP via RSU and replaced the previous stored secret key. Thus, the properties of anonymity and unlikability are satisfied. This scheme require frequent communication with TP to authenticate the credential in which the TP might not be continuously available.

2.4.6 A secure authentication protocol for internet of vehicles

Chen *et al.* (C. Chen et al., 2019) proposed an improved authentication protocol for IoV. This scheme is based on the identity based authentication. Each vehicle receives a smart card associated to its real identity from a TP during registration. The smart card is used as vehicle's credential to sign safety messages in IoV. Signing a message using valid credentials from a TP satisfies message authentication. A TP creates a database for every vehicle registered into the network and retrieve the real identity of a vehicle in case

of misbehaviours. In terms of privacy, anonymity is achieved using smart card that does not contain any identifying information that associates it to sending vehicle. Messages sign using the same smart card is linkable over it's short lifetime. However, it could not distinguish whether two message were signed by the same vehicle or not, therefore threshold mechanism cannot be adopted in this scheme.

2.5 Announcement Protocol in Symmetric Key Cryptography

Symmetric key cryptography is a cryptographic primitive based on a common key used for the encryption or decryption of ciphertext. This approach requires an establishment of pairwise symmetric keys during authentication phase since the same key is used for both encryption and decryption procedures. Symmetric algorithms provide a relatively high level of security while simultaneously allowing for fast encryption and decryption of messages compared to "traditional" PKC. However, when exchanged over an unsecured network, these keys are susceptible to malicious third party interception. If an unauthorized user accesses a particular symmetric key, the protection of any data encrypted with that key will be compromised. This primitive require vehicle to frequently authenticate each other in the key establishment phase where the trusted parties must be online all the time to establish symmetric keys. We review announcement protocols in some schemes (Guo et al., 2017; Huang et al., 2018; Sur et al., 2016; H. Wu & Horng, 2017)

2.5.1 An efficient and secure navigation protocol based on vehicular cloud

Sur *et al.* in (Sur et al., 2016) proposed a new VC based secure and privacy-preserving navigation protocol based on symmetric crptography. The scheme utilizes a hash-sign-switch paradigm with a trapdoor hash function to provide safe navigation service. To meet the requirement of message authentication, a single use anonymous certificate and hash key are used to sign a message. Privacy can be achieved using one time pseudonym

where the necessity of anonymity and unlikability are achieved respectively. Nevertheless, their schemes suffer from a much longer processing delay because they require an online connection to TP to verify the validity of service requesting vehicles, which in reality is very difficult particularly when the vehicle is moving at a relatively high speed. However, the credentials can not be reused, which imposes higher computational costs. In addition, the reliability of message cannot be evaluated where the origin of message is indistinguishable. Athough misbehaved vehicle is traceable in this scheme, however there is no further discussion on revoking the misbehaved vehicle.

2.5.2 SmartVeh: Secure and efficient message access control and authentication for vehicular cloud computing

Huang *et al.* in (Huang et al., 2018) proposed a secure and efficient message access control and authentication scheme using attribute based encryption (ABE), where the underlying cryptographic primitive is based on symmetric cryptography. The TP is seen as a fully trusted party responsible for handling credentials and for creating system parameters for vehicles. The RSUs are connected via secured channel and provide vehicles with wireless connections where RSUs are accountable for ensuring vehicle access and verifying the source of messages by verifying vehicle signatures. This scheme achieves authentication of message as a message is signed and produced only by a legitimate vehicle that has valid TP credentials. The anonymity and unlikability of the scheme is maintaned by using an anonymous pseudonymn. Thus, satisfying the privacy requirement. This scheme can not implement the threshold mechanism where the source of a message is distinct. Moreover, the matter of accountability requirement has not been addressed in this scheme.

2.5.3 A secure mechanism for big data collection in large scale internet of vehicle

A secure mechanism based on symmetric key cryptography to keep data privacy for big data collection in large scale in IoV was presented in (Guo et al., 2017). In this scheme, each vehicle initiates a mutual authentication process with the TP and receives a unique shared symmetric key during the registration phase. Using the symmetric key, the vehicle generates a symmetric hash message authentication code (HMAC) to sign safety messages. The RSU who has the HMAC encryption keys is responsible to verify the authenticity of the message by computing a matching HMAC. Hence, the first two requirements are achieved. However, it does not achieve distinguishability of message origin. This imply threshold method cannot be adopted in this scheme. Furthermore, this scheme does not mention any privacy techniques in its construction. Symmetric primitives is efficient in terms of computation cost. Nevertheless, it could not provide non-repudiation property. Furthermore, approaches based on symmetric cryptography requires an establishment of pairwise symmetric key during authentication phase before a message is broadcasted, which may result in message delay, thus increasing message drop.

2.5.4 Establishing an intelligent transportation system with a network security mechanism in an internet of vehicle environment

Wu *et al.* (H. Wu & Horng, 2017) established an intelligent transportation system with a network security mechanism in an internet of vehicle environment. This scheme combines the symmetric keys authentication with the use of chameleon hashing where it does not require public key certificate. This scheme employs chameleon hashing in message broadcasting and identity verification while utilizing the elliptic curve discrete logarithm problem (ECDLP) to achieve its security. The TP will generate the secret key of vehicle. Each vehicle obtains the common secret key whenever it enters a RSU domain. The vehicle uses these common secret key to generate messages for V2V communication.

Message is signed using valid credential satisfy message authentication. The requirement of anonymity and unlikabilty is achieved using anonymous ID that are not associated to real identity of vehicle and subject to the validity period. When a vehicle launches malicious behaviour, TP can find such vehicles from the anonymous IDs, thus achieving traceability.

2.6 Shortcoming of The Existing Protocols

Secure messages exchange among different entities is one of the most challenging tasks in future VC and IoV paradigm. Any malicious activity has the potential to compromise the reliability of messages, privacy and accountability exchanged between different entities. Nevertheless, because the underlying interaction medium is wireless, it is vulnerable to varying safety risks. For instance, malicious users may upload bogus information and broadcast that false information to the vehicles in the network. To mitigate bogus information attack, there is a requirement to ensure accuracy of transmitted messages. Another essential aspect of efficient communication is to preserve and protect the privacy of users while accessing the vast potential of IoV communication systems. At the same time, should misbehaviour arise, a vehicle should be held accountable. We have presented an extensive analysis of different annoucement protocols deployed in some recent announcement schemes based on various cryptographic primitives in VC and IoV in Section 2.2.

2.6.1 Vehicular Cloud

A majority of the scheme in VC satisfy the first two requirement of message reliability, nevertheless all the VC scheme proposes does not fulfill the third requirement of message reliability. Threshold method cannot be utilized in (Huang et al., 2018; Hussain et al., 2013; Hussain & Oh, 2014; Hussain et al., 2015; Jiang et al., 2018; Oh & Hussain, 2014; Sur et al., 2016; Yan et al., 2009, 2013; Zhang et al., 2020). As for the privacy aspect,

all schemes in VC achieve the necessity of anonymity and unlikability respectively. For accountability, the TP is assumed to be a fully trusted party in (Huang et al., 2018; Hussain et al., 2013; Hussain & Oh, 2014; Hussain et al., 2015; Oh & Hussain, 2014; Yan et al., 2009, 2013; Zhang et al., 2020) where TP have the access to the vehicle's secret key information. The requirement of non repudiation is not provided in VC because the vehicle is not the exclusive owner of the signing key. A misbehaved vehicle is traceable however, matter of implicit revocability were not adressed in these VC schemes (Huang et al., 2018; Hussain et al., 2013; Hussain & Oh, 2014; Hussain et al., 2015; Jiang et al., 2018; Oh & Hussain, 2014; Sur et al., 2016; Yan et al., 2009, 2013; Zhang et al., 2020).

2.6.2 Internet of Vehicle

The authentication protocols discussed in (R. Argawal et al., 2019; C. Chen et al., 2019; Cui et al., 2018; Guo et al., 2017; J. Liu et al., 2018; Y. Liu et al., 2017; Sahbi et al., 2018; Vasudev & Das, 2019; H. Wu & Horng, 2017) do not provide a promising solution for secure authentication in IoV. The sender's legitimacy and message integrity is assured in all the IoV schemes proposed. However, the evaluation of message trustworthiness cannot be provided in (R. Argawal et al., 2019; C. Chen et al., 2019; Cui et al., 2018; Guo et al., 2017; J. Liu et al., 2018; Sahbi et al., 2018; Vasudev & Das, 2019; H. Wu & Horng, 2017) . Matter of privacy is addressed in all the IoV schemes presented except in (Sahbi et al., 2018). Although misbehaved vehicle is traceable in the network, however there is no explicit or further revocation technique has been discussed in (R. Argawal et al., 2019; C. Chen et al., 2019; Cui et al., 2018; Guo et al., 2017; J. Liu et al., 2018; Y. Liu et al., 2017; Sahbi et al., 2018; Vasudev & Das, 2019; H. Wu & Horng, 2017) of IoV proposed scheme. Furthermore, all schemes provide non-repudiation except in (Y. Liu et al., 2017; Vasudev & Das, 2019). In our work, we fulfill the conflicting security requirements of a message reliability, privacy and accountability of IoV announcement scheme, and examine

how to resolve such contradictions.

2.7 Summary

We have presented an extensive analysis of different announcement authentication protocols deployed in some recent announcement schemes based on various cryptographic primitives in VC and IoV. We then summarize the adoption of these annoucement authentication protocols in Table 2.1.

Table 2.1: Summary of authentication announcement protocol

Primitives	Schemes	Techniques	Technology
Traditional PKC	(Yan et al., 2013)	Location encryption	VC
	(Hussain et al., 2013; Hussain & Oh, 2014)	Location encryption	VC
	(Sahbi et al., 2018)	Model based on SDN and CC	IoV
	(J. Liu et al., 2018)	Certificateless short signature	IoV
	(Cui et al., 2018)	Privacy-preserving pseudonym using double pseudonymn	IoV
	(Kang et al., 2018)	Privacy-preserving pseudonym	IoV
Identity based	(Jiang et al., 2018)	Authentication and key agreement (AKA)	VC
	(Zhang et al., 2020)	Asymmetric group key agreement (AGKA) and location based encryption (LBE)	VC
	(Y. Liu et al., 2017)	Privacy-preserving dual authentication and key agreement	IoV
	(Vasudev & Das, 2019)	Pseudo-identities	IoV
	(R. Argawal et al., 2019)	Anonymous ID	IoV
	(C. Chen et al., 2019)	Smart card	IoV
Symmetric Key	(Sur et al., 2016)	Hash-sign-switch paradigm	VC
	(Huang et al., 2018)	Attribute based encryption (ABE))	VC
	(Guo et al., 2017)	Big data collection	IoV
	(H. Wu & Horng, 2017)	Chameleon hashing	IoV

In view of the shortcoming of the existing schemes, we propose a novel announcement protocol in IoV environment using group signature that solves the contradictory requirements of message reliability, privacy and accountability that exist in previous scheme. We modify and extend the work of MLGS scheme (Q. Wu et al., 2010) to adopt in IoV scenario and provide additional features such as ease of access and use, also reduced deployment costs. Furthermore, our review found, there is no solution that deploys group signature technique in an announcement protocol for IoV. In our work, we will solve the issues by presenting a new efficient protocol for IoV where the underlying cryptographic primitive is based on group signature. Finally, a comparative analysis and simulation are conducted to

compare our protocol to existing schemes, and the result proves that our protocol achieves better performance efficiency in IoV communication.

CHAPTER 3: CRYPTOGRAPHIC PRIMITIVE

In this chapter, we study the basic cryptography used in our research, notably group signatures. We will then discuss the mathematical contexts needed to understand the cryptographic techniques used in this thesis.

3.1 Group Signatures

The theory of group signatures, introduced by Chaum and Van Heyst (Chaum & van Heyst, 1991), is a digital signature based cryptographic primitive. The following concept is implemented by group signatures at a high level: All potential signers are treated as members of some group. Each signer can sign on behalf of the entire group without disclosing which person in the group has signed the message. These group signature can be publicly checked using the entire group's public key, which provides the individual signer with anonymity. The architecure of a group signature scheme consists of multiple group members and a group manager. The group manager is responsible for initializing the group, admitting it and revoking group members in some schemes.

3.1.1 Phases

A group signature scheme is composed of the following phases (Bellare et al., 2005; Q. Wu et al., 2010):

- **Setup**: This is the first phase in which the project manager produces only the group's public key and group manager's private key.
- **Join**: In this step, a potential member of the group must enroll to be a new group member of a group with the group manager. The registered group member receives their private signing key while the group manager receives some confidential

information which will be used later to open group signatures created by the new member.

- **Sign**: This process enables each group member to provide group signatures in possession of their (personal) secret signing key. For authentication, the generated message would be sent to a verifier.
- **Verify**: In this step, the validity of a group signature given on some message can be verified. If the signature is legitimate, a verifier must accept the signature, otherwise the message will be refused to accept.
- **Open**: In case of dispute the group manager can identify the signer of a signature of a message, together with the group public key and group manager's private key.
- **Judge**: We note that the judge will use the parameters of the public group to evaluate whether the evidence of a given certificate to the reported signer is accurate for the group manager.

3.1.2 Properties

The following properties are met by a group signature scheme (Ateniese et al., 2000; Bellare et al., 2005):

- **Correctness**. A legitimate group member who signed a message using *Sign* will always be accepted by *Verify*.
- **Anonymity**. This requirement indicates that no member, except for the group manager, can identify the signer of a given group signature.
- **Unlinkability**. An adversary would not be able to decide whether there were two or more group signatures signed by such a group member.
- **Traceability**. This property may also be seen as a security precondition for ensuring that the group manager is able to open any valid group signature in case of an

dispute.

- **Unforgeability**. This condition usually takes into account chosen message attacks where the adversary can acquire valid group signatures for any messages of their choice generated by any valid group member of their choice.
- **Exculpability**. It guarantees that no group member and not even group manager can produce any valid message-signature pair on behalf of another group member.

3.2 Mathematical Background

3.2.1 Number Theory

Number theory is the analysis of the properties of numbers and the relation between numbers. Number theory techniques in cryptography are fundamental to developing the public key cryptosystem such as the discrete logarithm problem (DLP) and the RSA algorithm.

Definition 3.2.1. Let $a, b, m \in \mathbb{Z}$ with $m \neq 0$, then a is said to be congruent to b modules if m divides $a - b$. This can be denoted as $a \equiv b$ (A. J. Menezes et al., 1996).

Example 3.2.1. i) $38 \equiv 23 \bmod 15$ since $38 - 23 = 1 \cdot 15$.

ii)$-8 \equiv 2 \bmod 5$ since $-8 - 2 = 2 \cdot 5$.

iii)$39 \equiv 3 \bmod 9$ since $39 - 3 = 4 \cdot 9$.

Definition 3.2.2. Let $M \in \mathbb{Z}\{0\}$. Then congruence mod m is an equivalence relation in other words (A. J. Menezes et al., 1996):

1. Reflexity, For all $a \in \mathbb{Z}$, $a \equiv a(m)$.
2. Symmetry, For all $a, b \in \mathbb{Z}$, $a \equiv b(m)$ then $b \equiv a(m)$.
3. Transitivity, For all $a, b, c \in \mathbb{Z}$, if $a \equiv b(m)$ and $b \equiv c(m)$ then $a \equiv c(m)$.

Proof

1. a − a = 0 is divisible by all m.
2. If m divides a − b then it also divides $(-1) \cdot (a - b) = b - a$.
3. If $a \equiv b$(mod m) and $b \equiv c$(mod m) then $a + b \equiv b + c$ (mod m) and $ab \equiv bc$(mod m).

3.2.2 Abstract Algebra

Abstract algrebra is a study of algebraic structures, including groups, rings and fields. We emphasize on group, since it is one of the main building blocks of cryptography (A. J. Menezes et al., 1996).

Definition 3.2.3. A binary operation $*$ on a set S is a function mapping S X S into S. For each (a, b) $\in S \times S$, we will denote the element $*(a, b)$ of S by $a * b$ (A. J. Menezes et al., 1996).

Definition 3.2.4. A **group** $(\mathbb{G}, *)$ is a set $\mathbb{G}$, closed under a binary operation $*$, such that the following axioms are satisfied (A. J. Menezes et al., 1996):

1. $*$ is associative in $\mathbb{G}$.
2. $\mathbb{G}$ has an identity element for $*$.
3. Every element in $\mathbb{G}$ has an inverse in $\mathbb{G}$.

Definition 3.2.5 A group $\mathbb{G}$ is finite if $|\mathbb{G}|$ is finite. The number of elements in a finite group is called its order (A. J. Menezes et al., 1996).

Definition 3.2.6. A group of $\mathbb{G}$ is cyclic if there is an element $a \in \mathbb{G}$ such that for each $b \in \mathbb{G}$ there is an integer i with $b = a^i$. Such an element a is called a generator of $\mathbb{G}$

(A. J. Menezes et al., 1996).

Definition 3.2.7. Let $\mathbb{G}$ be a group and $a \in \mathbb{G}$. The order of a is defined to be the least positive integer t such that $a^i = 1$, provided that such an integer exists. If such a i does not exist, then the order of a is defined to be ∞ (A. J. Menezes et al., 1996).

3.2.3 Bilinear Pairings

To construct efficient schemes, bilinear maps have been extensively investigated. Bilinear maps are also used to execute our protocols. Thus, we briefly review them.

Definition 3.2.8. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of the same prime order q. $\mathbb{G}_1$ is an additive group while $\mathbb{G}_2$ is a multiplicative group. A bilinear pairing on $\mathbb{G}_1$ is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ that satisfies the following properties (A. J. Menezes et al., 1996):

- Bilinearity: For all $P, Q \in \mathbb{G}_1, e(P + Q) = e(P) + e(Q)$.
- Non-degeneracy: $e(P, Q) \neq 1$
- Computability: An efficient algorithm exist to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

Such a bilinear map e can be constructed with the modified with Weil and Tate pairings (Boneh et al., 2004; A. Menezes, 2009). Typically, $\mathbb{G}_1$ is a subgroup of the group of points on an elliptic curve over a finite field and $\mathbb{G}_2$ is a subgroup of the multiplicative group of a related finite field.

3.2.4 Computational Assumptions

Our work relies on several computational assumptions, that is, the Decisional Diffie-Hellman(DDH) assumption and the Diffie-Hellman Knowledge (DHK) assumption (Q. Wu

et al., 2010). Let $\mathbb{G}$ be a finite cyclic group of prime order p and g be a generator of $\mathbb{G}$, the three assumptions are defined as follows.

- Decisional Diffie-Hellman (DDH) Assumption

  The DDH holds in $\mathbb{G}_1$ where $g, g^a, g^b, g^c \in \mathbb{G}_4$ such that a,b,$c \in \mathbb{Z}^*_{\mathrm{p}}$ decide whether $c = ab$.

  This statement means, neutrally, that there is no appropriate probabilistic algorithm that yields "true" if $c = ab$ and "false" otherwise when correctly applied.

- Diffie-Hellman Knowledge (DHK) Assumption

  Given $g, g^x \in \mathbb{G}_2$ for randomly chosen $x \in \mathbb{Z}^*_{\mathrm{p}}$, create a Diffie-Hellman tuple (g, g^x, g^r, g^{xr}) without the knowledge of r.

  That is to say, the DHK assumption claims that a Diffie- Hellman tuple can not be generated without discovering the one-tuple member's discrete logarithm relative to another, that is, r.

3.3 Conclusion

We introduced in this chapter the cryptographic primitive incorporated in our research, which is, group signature. We have implemented certain mathematical contexts into practice to clarify the cryptographic techniques included in this thesis. In summary, we presented a general review of the number theory, abstract algebra, bilinear pairing and computational assumption. Those are the basic foundation which are required for the group signature construction without sacrificing security.

CHAPTER 4: PROPOSED PROTOCOL

In this chapter, we generalize these existing announcement protocol by constructing a generic announcement protocol in IoV network. Our work comprehend the V2V, V2I and V2P communication. We design an efficient and secure announcement protocol in IoV that allows the evaluation of message reliability, preserve privacy and robust against adversary. We deploy group signature (GS) technique that efficiently solve the conflicting security requirement of message reliability and privacy. Furthermore, the adoption of IoV in GS is new.

4.1 Introduction

Our research adds to the design of a new secure announcement protocol in IoV that efficiently resolves the contradictory security requirements of message reliability, privacy and accountability in IoV. Recall that, the announcement protocols discussed in (R. Argawal et al., 2019; C. Chen et al., 2019; Cui et al., 2018; Guo et al., 2017; J. Liu et al., 2018; Y. Liu et al., 2017; Sahbi et al., 2018; Vasudev & Das, 2019; H. Wu & Horng, 2017) does not provide a promising solution for secure authenticated anonymous announcement protocol in IoV.

In our work, we formulate a generic abstraction of an announcement protocol. We then construct a new announcement protocol in internet of vehicles (IoV), where the underlying cryptographic primitive is based on group signature. To the best of our knowledge, this is the first generic announcement construction exists in the literature that systematically studies and generalise announcement protocol in IoV. We utilize the generic abstraction to design our announcement protocol. As far as we know of, our work is the first comprehensive construction of an announcement protocol using group signature that addresses the nontrivial problem of the conflicting security requirements.

We show that our proposed announcement protocol has minimal reliance on roadside units (RSUs). The involvement of the RSUs is only needed to relay information and to provide a gateway between the trusted party and users in the network. The efficiency of our work is comparable to other announcement schemes in the literature. The computational simulation on NS-2.35 proves the practicality of our protocol in real world deployment.

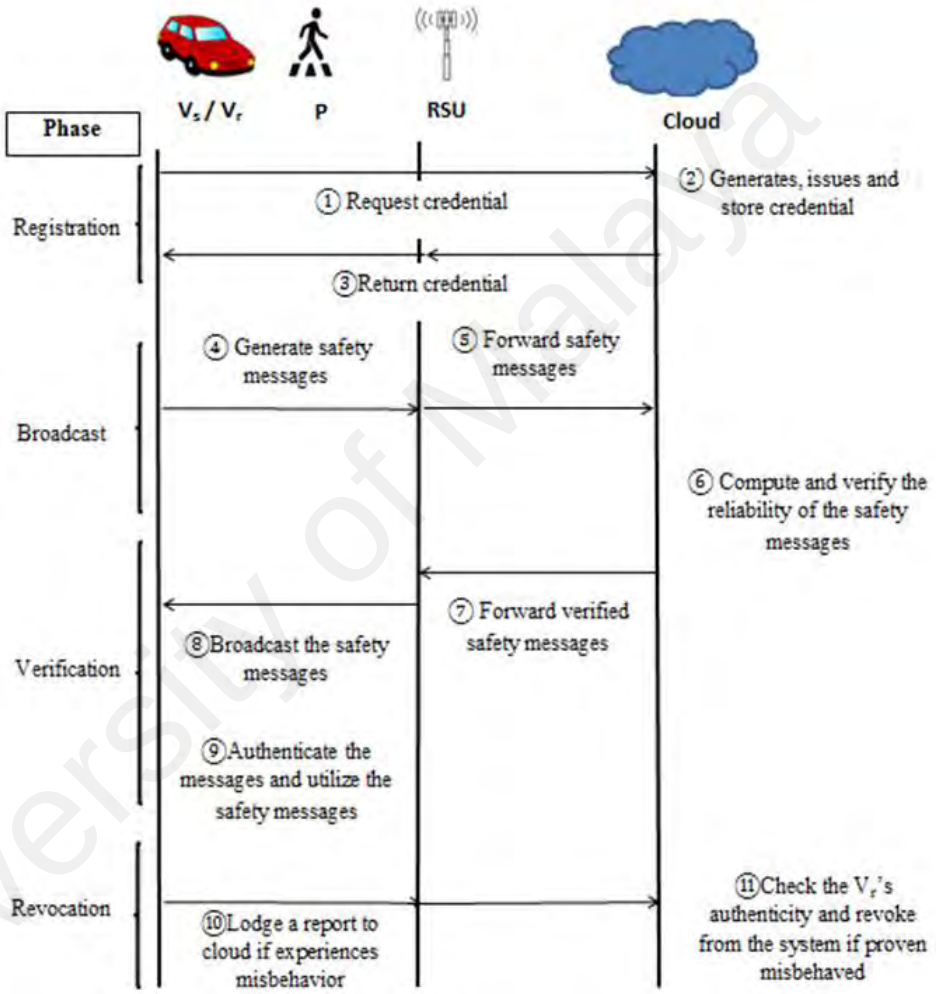

Figure 4.1: Network model.

4.2 Abstraction of an Announcement Protocol in IoV

In this section, we present our generic abstraction of announcement protocol for group signature scheme in IoV and generalize them into eleven steps as demonstrated in Figure 4.1. Before describing the abstraction, we review the main role of each entity in the

network consists of a cloud, roadside units (RSUs), vehicle which composed of sending vehicle (Vs) and receiving vehicle (Vr), and pedestrian (P). We introduce the role of each entity as follows:

- **Cloud**. We rely on a cloud network that plays the role of a trusted party (TP). One of the cloud's roles is managing vehicle's admission into the system and revoking dishonest vehicles. It is accountable for the issuance and management of credentials. The identity of a misbehaved vehicle will only be revealed by a cloud when a vehicle is found to be malicious. The cloud also computes and verifies the reliability of safety messages. This may reduce the computational burden on Vr as we utilize the functionality of the cloud.

- **Roadside Unit (RSU)**. The RSU is a physical infrastructure located along the roadsides and highways. A gradual deployment of RSUs is assumed. RSUs are expected to be densely distributed in urban areas due to the density of population in relative. Vehicles may communicate to RSUs through short range communication. The infrastructure acts as a gateway and relays the information between the cloud and vehicles. It is worth noting that our protocol does not require a confidential communication channel between the RSU and the vehicle. All RSUs are authenticated and verified by the cloud upon their participation in the network.

- **Vehicle**. Vehicles in IoV network consist of sending vehicle (Vs) to generate and forward the safety-related messages in the network and receiving vehicle (Vr) that utilize and act accordingly upon receiving the safety messages. We assume that each vehicle in the network is equipped with a computing device called an onboard unit (OBU). An OBU has a wireless communication capability that consists of Event

Data Recorder (EDR), which records received messages. The TPD is embedded as part of OBU that implements cryptographic tools and ensures authenticated access control.

- **Pedestrian**. Pedestrian's average walking speed is 1.4 m/s (5 km/h). Pedestrians have devices such as smartphones, tablets and personal digital assistant (PDA) in IoV. Current smartphones are equipped with various sensors, which include accelerometer, GPS, and communication technologies, such as cellular (LTE or 3G), Bluetooth and Wi-Fi. Smartphones has limited computation, storage and processing capability. All the computation process is performed by the cloud.

4.3 Description of the Generic Abstraction of Announcement Protocol

The abstraction of an announcement protocol in IoV shown in Figure 4.1 consist of the eleven steps as follows:

Registration Phase

Step ①: To participate in the network, V_s and P send request to acquire credential from the cloud.

Step ②: To certify V_s and P legitimacy in the network, cloud generates, issues and store credential.

Step ③: Upon success verification, cloud returns credential to V_s and P.

Broadcast Phase

Step ④: V_s generates and relays safety messages associated to the events to the cloud via RSU.

Step ⑤: RSU performs as a gateway between cloud and V_s where it forwards the safety

messages to the cloud for verification.

Verification Phase

Step ⑥: Cloud evaluates the reliability of the message.

Step ⑦: Upon success verification, cloud forward the safety messages to a nearby RSU where the reported event occurred.

Step ⑧: RSU broadcast the verified safety messages to V_r and *P* in the vicinity of the event reported.

Step ⑨: V_r and *P* validate the message and utilize the safety messages.

Revocation Phase

Step ⑩: If V_r and *P* experienced any misconduct from its encounter with V_s, they have the option to lodge a report to the cloud via the RSU..

Step ⑪: Upon receiving reports, the cloud identifies the source and integrity of the report by V_s before making a decision whether or not to revoke V_s from the network.

4.4 Secure Annoucement Protocol for Group Signature in IoV

We propose a new announcement protocol in internet of vehicles (IoV) using group signature technique that efficiently resolves the contradictory security requirements of message reliability, privacy and accountability in IoV.

4.4.1 The MLGS Construction

We present an overview of the MLGS scheme. Wu *et al.* (Q. Wu et al., 2010) proposed a message linkable group signature (MLGS) for anonymous authentication. This scheme relies on bilinear-pairing groups and anonymous threshold authentication. They formulate a flexible algorithm which allows a receiver to accept a message only if the message

is authenticated by at least a predefined distinct number of anonymous vehicles. This resilience approach can thwart Sybil attack as the real identity of a sender is revealed if a vehicle signs a message more than once.

In this scheme, multi-TPs were presented which are, a vehicle manufacturer (VM), a group registration manager (RM), and a tracing manager (TM). To participate in the network, VM and a vehicle signs a contract to verify the ownership of the vehicle. The vehicle is then able to register to RM as a legitimate group member. Vehicle self-generated public key, $Y = U_1{}^y$ for a random value $y \in \mathbb{Z}^*{}_p$ where y is the vehicle's secret key. The tracing information $T = g_2{}^y$ will be sent to TM during registration for traceability. The VM, RM and TM are semi-trusted parties and assumed to behave honestly since they have no access to the vehicle's private keys. Upon success registration in the network, RM issues a signature on the vehicle's public key. The signature will be used by the vehicle as a group certificate to broadcast the safety message.

This scheme applies threshold authentication to evaluate the trustworthiness of a message. The safety message is considered reliable if the signature of the message is valid, the integrity of the message is assured and it fulfills property of threshold authentication. The privacy is protected as long as a vehicle generates one message link identifier $\sigma_4 = H_1(m)^y$ for each message. Its identity will be revealed if misbehaved by generating more than one signature on the same message. The goal of MLGS scheme is to provide an efficient trustworthy system with a balanced public safety and vehicle's privacy. Table 4.1 shows the lists of some notations used in our protocol which was adopted from MLGS scheme (Q. Wu et al., 2010). For ease of comparison, we use the same notation.

Table 4.1: Table of the symbol and notation

Symbol	Notation
TC	Tracing cloud
RC	Registration cloud
AC	Authentication cloud
P	Pedestrian
$\mathbb{G}_{\mathrm{i}}(i = 1, 2, 3)$	Finite cyclic group of prime order p
g_{i}	A random generator of $\mathbb{G}_{\mathrm{i}}$
$U_{\mathrm{v}}, U_{\mathrm{p}}, h_2 \in \mathbb{G}_2$	Public system parameters
ϕ	An isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$
$U_1 = \phi(U_{\mathrm{v}})$	Public system parameter
$h_1 = \phi(h_2)$	Public system parameter
$H_1()$	A cryptographic hash function from $0,1^*$ to $\mathbb{G}_1$
(A, Z)	The public private key pair of registration cloud
(pk_{V_s}, sk_{V_s})	The public private key pair of vehicle
(pk_p, sk_p)	The public private key pair of pedestrian
MT	Message Type
GID_{v}	Group ID of the vehicle
ID_{RSU}	Real Identity of RSU
$K_{\mathrm{v}} = (K_1, K_2)$	The group certificate of vehicle
K_{p}	The group certificate of pedestrian
T_v=$g_2{}^{sk_{Vs}}$	The tracing information of vehicle
T_p=$g_3{}^{sk_p}$	The tracing information of pedestrian
m	A message
σ	A signature on message m
$M = (m, \sigma)$	A message appended with a signature
σ_{i}	The ith component of σ

4.5 Our Proposed Protocol

4.5.1 System architecure

The system consists of four parties, which are the cloud, roadside units, vehicles and pedestrian. A vehicle communicates with the cloud via a confidential channel to enrol into the network. During the registration process, cloud certifies the legitimacy of each vehicle and RSU by secure distribution of valid credentials in the network. The involvement of RSU is needed to relay information and perform as a gateway between the cloud and a vehicle. Cloud performs the computation process and verify the reliability of the safety messages. The RSU disseminate the successful verified messages to $\mathrm{V_r}$ and pedestrian in the proximity of event reported. A $\mathrm{V_r}$ and a pedestrian then utilizes the reliability of

messages received and verify that the message is reliable from cloud.

We consider the presence of internal adversaries in our protocol. An internal adversary may exploit their legitimacy to perform attacks to other vehicles. External adversary is not being considered in our protocol as they poses less harm to other vehicles in the network since they do not possess valid credentials or direct access to participate into the network. We assume cloud is semi-trusted as they have no access to a vehicle's and pedestrian's secret key. This protocol utilizes the presence of cloud providers in each region: the cloud is associated with a number of grids where a traffic area is partitioned into grids. The grid cell size is 20 km x 20 km. Figure 4.2 shows the grid of a traffic area.

We consider smartphones as the most widely accepted choice as a pedestrian's device. This is due to their versatility and ubiquitous feature that smartphone possess. Smartphones have limited in resources in terms of computation and storage. As the cloud has extensive computing resources that can be allocated on demand and computation power is not an issue. It performs the computation process and verify the reliability of the safety messages. A typical safety message may contain message type, location and direction of the respective vehicle or pedestrian. This safety information can be utilized by the pedestrian to be aware of the situation ahead of them and as a result, may reduce the number of road causalities. Vehicles may transmit 5 safety messages per second (i.e., at fixed 5 Hz frequency). To estimate storage requirements, consider smartphone capability of one month with 10 safety messages updates per minute. A total of 30.24.60.10 = 432 000 one-time certificates will be required. Hence, we can conclude each smartphone requires 432 KB of storage to run up this safety application. This is reasonable storage for modern smartphone in current world today (Defrawy & Tsudik, 2011).

Figure 4.2: Grids that represent a traffic area.

4.5.2 Computational assumptions and System setup

Our protocol setup algorithm is based on bilinear pairing and takes input a security parameter Ψ, and outputs a public parameter $\Upsilon = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, e)$. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be a finite cyclic group, respectively, of the same prime order, p. Assume $\mathbb{G}_1 = \langle g_1 \rangle$ and $\mathbb{G}_2 = \langle g_2 \rangle$ and e: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$ is an efficient non-degenerate bilinear map such that $e(g_1, g_2) \neq 1$ and for all $h_1 \in \mathbb{G}_2$ and $h_2 \in \mathbb{G}_2$.

Our scheme is based on Decisional Diffie-Hellman (DDH) assumption and the Diffie-Hellman Knowledge (DHK) assumption (A. Menezes, 2009). The DDH holds in $\mathbb{G}_1$ where $g, g^a, g^b, g^c \in \mathbb{G}_4$ such that a,b,$c \in \mathbb{Z}^*_{\mathrm{p}}$ for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the probability decide if $c = ab$ is neglibly away from $\frac{1}{2}$. While in DHK, given $g, g^x \in \mathbb{G}_2$ for randomly chosen $x \in \mathbb{Z}^*_{\mathrm{p}}$, it creates a Diffie-Hellman tuple (g, g^x, g^r, g^{xr}) without the knowledge of r.

We assume the DDH and DHK assumptions hold in $\mathbb{G}_1$. We assume that ϕ is computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ for instance $\phi(g_2) = g_1$. Let h_2 and U_2 be randomly chosen from $\mathbb{G}_2$ and $u, v \in \mathbb{Z}, e(h^u{}_1, h^v{}_2) = e(h_1, h_2)^{uv}$. The system parameters

are $\pi = \langle p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, g_3, e, h_1, h_2, h_3 U_1, U_{\mathrm{v}}, U_{\mathrm{v}}, H_1, H \rangle$.

4.5.3 Vehicle and Pedestrian Registration

To register to a IoV network, a vehicle communicates with the cloud via a confidential medium in the subsequent steps:

Step ①: To participate in the network, $\mathrm{V_s}$ self-generate a key pair pk_V, sk_V. $\mathrm{V_s}$ sends request to the cloud to certify its self-generated public key, pk_V while keeping its private key (sk_V) private at time, t, where ($pk_V = U_{\mathrm{v}}{}^{sk_V} \in \mathbb{Z}_R{}^*{}_{\mathrm{p}}$). For pedestrian registration, P self-generate a key pair pk_p, sk_p where ($pk_p = U_{\mathrm{p}}{}^{sk_p} \in \mathbb{Z}_R{}^*{}_{\mathrm{p}}$) and forwards the request to cloud to certify its self-generated public key, pk_p while its secret key sk_p is then kept confidential. Vehicle computes tracing information $T_v = g_2{}^{sk_V}$ while, pedestrian computes its tracing information $T_p = g_3{}^{sk_p}$ where g_{i} represent random generator of $\mathbb{G}_{\mathrm{i}}$. Vehicle and pedestrian send (pk_V, pk_p, T_v, T_p) to TC.

Step ②: TC performs authentication check by checking $e(pk_V, pk_p, g_2, g_3) = e(U_v, U_p, T_v, T_p)$. Upon success verification, TC generates a signature on pk_V and pk_p. TC sends to V_{s} and P respectively. TC stores (pk_V, pk_p, T_v, T_p) into its local database.

Step ③: $\mathrm{V_s}$ runs a Zero-Knowledge Proof Protocol (ZKPP) denoted by $ZK\{sk_V | pk_V = U_1{}^{sk_V}\}$ with RC. RC first verifies the signature on pk_V and pk_p to certify the legitimacy of the vehicle and pedestrian in the network. The RC has a public-private key pair denoted by $(A, Z) = (\mathrm{e}(Z, g_2, g_3), Z)$. Then, RC validates TC's signature on pk_V and pk_p. RC checks the ZKPP runs by $\mathrm{V_s}$, $ZK\{sk_V | pk_V = U_1{}^{sk_V}\}$ is valid and performs computation of $K_1 = g_1{}^k$, $K_2 = Z(h_1 pk_V)^{-k}$ and $K_{\mathrm{p}} = Z(h_{\mathrm{p}} pk_p)^{-k}$ where $k \in \mathbb{Z}^*{}_{\mathrm{p}}$. Upon success computation, RC

distribute $K_v = (K_1, K_2)$ to legitimate vehicle and K_p to authorized pedestrian. A vehicle verifies that $e(K_2, g_2)e(K_1, h_2)e(K_1{}^{sk_V}, U_2)$=$A$ to validate the signature. If the check holds, vehicle and pedestrian have succesfully register to cloud and can use K_v and K_p across the network as a group certificate. Vehicle can use its (sk_V) to generate signature on any safety message.

4.5.4 Message Broadcast

In this phase, a V_s generates a road-related safety message and broadcasts it to neighbouring vehicles via RSUs. This is outlined as follows:

Step ④: V_s generates the message (m) as follow:

$$m = MT, t_{\text{stamp}}, loc_{\text{cur}}, GID_{\text{v}}, ID_{\text{RSU}}$$

Message type is denoted as MT, t_{stamp} is the signature generation time to ensure message freshness, loc_{cur} is current position of the vehicle moving. Let GID_{v} be a group identity of the vehicle where it enable to distinguish which group the vehicle belongs to. The real identity of RSU is denoted as ID_{RSU}.

Under the group signature scheme, a member of the group shall sign a message on behalf of the group. Signatures can be checked with regard to a specific public key group, but they may not disclose the identity of the signatory. The group signature is composed of three parts as below:

- Distribute in a randow way the group certificate to show that the signatory is a lawful member of the group while protecting privacy on the network. V_s computes

$\sigma_1 = K_1 g_1{}^{s}, \sigma_2 = K_2(h_1 pk_V)^{-s}$ for a randomly chosen $s \in \mathbb{Z}^*_p$.

- Set up the public key of a group member in a rabdom where, $\sigma_3 = \sigma_1{}^{sk_V}$ and produce a message link-identifier $\sigma_4 = H_1(m)^{sk_V}$.
- Generate the group signature on m using private key, sk_V in $\sigma_3 = \sigma_1{}^{sk_V}$ and $\sigma_4 = H_1(m)^{sk_V}$. V executes zero knowledge proof to convince the verifier of a given statement's validity, without leaking any information further than the statement's validity to generate a group signature.

To generate a group signature, V_s performs the following computation:

- Randomly choses $r \leftarrow \mathbb{Z}^*_p$.
- Calculate assumptions $R_1 = H_1(m)^r$ and $R_2 = \sigma_1{}^r$.
- Obtain a challenge from the computed assumptions of R_1 and R_2 where $\sigma_5 = H(m||\sigma_1||\sigma_2||\sigma_3||\sigma_4||R_1||R_2)$.
- Response to the challenge with $\sigma_6 = r - \sigma_{5sk_V} \pmod p$ and output the group signature as $\sigma = (\sigma_1, \sigma_2, ..., \sigma_6)$ of m.

V_s broadcast a message tuple, $M = (m, \sigma)$. The message link-identifier, σ_4 that can only produced once by V_s for the same message. V_s then announces a messages to authentication cloud, *AC* via RSU.

Step ⑤: RSU forward M to *AC* to evaluate the reliability of the safety messages. *RSU* rejects messages that included the same σ_4 as replay of σ_4 demonstrates that the same messages were signed by the same vehicle more than once. The *AC* then validates predefined number of messages reporting the same event.

4.5.5 Message verification

Upon receiving the message, cloud performs the following steps :

Step⑥: For message verification:

- *AC* checks $e(\sigma_2, g_2)e(\sigma_1, h_2)e(\sigma_3, U_2) = A$ in order to validate the group certificate.
- Performs check on:

  $\sigma'_5 = H(m||\sigma_1||\sigma_2||\sigma_3||\sigma_4||H_1(m)^{\sigma 6}\sigma_4{}^{\sigma 5}||\sigma_1{}^{\sigma 6}\sigma_3{}^{\sigma 5})$.

If the freshness of the message is preserved, *AC* considers a message to be reliable if and only if $\sigma'_5 = \sigma_5$. In addition, our protocol adopt flexible threshod authentication where *AC* measure the reliability of a message based on influx of a message received.

Step ⑦:Upon success verification, *AC* forwards the safety message, *M* to nearby RSU.

Step ⑧: RSU broadcast the safety message *M* to V_r and *P* via RSU in the vicinity of the event reported.

Step ⑨: V_r and *P* validate the content of the message by checking the t_{stamp}. If t_{stamp} are valid and both checks for message verification are hold, the safety message is considered reliable. V_r ensures the message is reliale and being verified by *AC* where V_r randomly choses *s*, and computes *x*=*h*(*s*) where *x* demonstrate the knowledge of *s* without discloses it. V_r compute the challenge $f = (s, V_r)_{pk_{AC}}$ and sends to *AC*. Here pk_{AC} denotes the public key of *AC* and *h* is a one-way hash function. *AC* responds to the challenge by decrypts *f* to recover *s*' and computes *x*'=*h*(*s*)' and quits if *x*'≠*x* (implying *s*'≠*s*). Otherwise, *AC* sends *s*=*s*' to V_r. Hence, V_r succeeds with authentication of *AC* upon verifying the received *s*

agrees with that sent earlier.

4.5.6 Vehicle Traceability and Revocation

Step ⑩: V and P lodge a revocation report to the $TC$when experienced misbehaviour in the network.

Step ⑪: The TC validates the matching σ and authenticity of M to revoke misbehaved V. We note that, TC holds some pk_{V} trap door knowledge. For revocation and law enforcement purposes, the TC must check its local database to link pk_{V} with V's identity. We adopt the revocation protocol from our previous work in (Shari et al., 2020) and refer the readers to (Shari et al., 2020) for in depth understanding of the revocation phase.

4.6 Performance Evaluation

4.6.1 Security Analysis

In this section, we discuss security issues of our proposed protocol and evaluate its performance. Cloud is accountable to verified safety messages without revealling the true identity of a signer. This approach enables a vehicle to remain anonymous if it generates one signature on each message but can be traced once it produces more than one signature on the same message. We compare our scheme with CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017) as both schemes are IoV context and proposed the authenticated anonymous announcement protocol in IoV. The following two security requirements are critical concerns to be met towards IoV deployment:

1) **Reliability**. The first two requirements of message reliability are sender's authenticity and data integrity, which are satisfied in all schemes proposed. A secure digital signature technique is commonly used to achieve message authentication. A message generated and announced without alteration is assured reliable and the integrity of the message is

preserved. In our protocol, the requirement of V_s's user authenticity and data integrity are achieved as message is signed using valid credentials from cloud.

The scheme in (Y. Liu et al., 2017) fulfil the third requirement of message trustworthiness by using reputation system to evaluate message reliability. However, it is not satisfied in (J. Liu et al., 2018), as no solution to evaluate message reliability was proposed. The property of threshold technique is not suitable to be adopted as the origin of the message in (J. Liu et al., 2018) is indistinguishable. In our work, we fulfil the requirement of threshold authentication property. We adopt the flexible threshold system which allows the cloud to determine the threshold depending on the message's content and location. For example, the threshold in a city is higher compared to the rural area, which is relative to traffic density.

Claim 1. *The proposed protocol is robust against Sybil attack and achieves the third requirement of message reliability.*

We consider a Sybil attack executed by an internal adversary. An external adversary is not considered, as they do not own a valid credential or direct access to the network thus pose less harms to other users in the network. Sybil attack occurs when an internal adversary generates multiple signatures and disguise as different vehicles in order to compromise the functionality of the IoV network.

Proof: Let an internal adversary be Υ. We consider a scenario where Υ generates two signatures on the same message and announce these messages. Upon receiving these messages, AC checks the message-link identifier, σ_4 to ensure that a legitimate vehicle in the network generates each message once. However, Υ can be identified when the two signatures share the same component of $\sigma_4 = H_1(m)^{sk_V}$.

Hence, Υ can be computationally related by evaluating the component of σ_4 on two messages reporting the same event. Therefore, our scheme provides the distinguishability of origin that supports threshold authentication and thus, achieves the requirement of message reliability.

Recall that, part of the signature under a one-time public key shows that $\sigma_3 = {\sigma_1}^{sk_V}$ and $\sigma_4 = H_1(m)^{sk_V}$ where the value of sk_V is undisclosed in (σ_3, σ_4). The TC uses the tracing informationT_v=${g_2}^{sk_V}$ to identify the group member by checking $e(pk_{\mathrm{V}}, pk_p, g_2, g_3) = e(U_{\mathrm{v}}, U_{\mathrm{p}}, T_{\mathrm{v}}, T_{\mathrm{p}})$.

This enable Υ to be traceable when the replay of σ_4 is recognized upon endorsing the same message more than once. Hence, the message will be discarded and thus, our protocol is robust against Sybil attack.

2) **Privacy**. There are two aspects of privacy that we consider; anonymity and unlinkability. The identity of vehicles is protected where the information of the user is anonymous against unauthorized vehicles in the network. In CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017) scheme, both employ pseudonym in order to satisfy privacy requirement. Anonymity of message announced is achieved by both schemes where the pseudonyms are used to prevent linking to the vehicle's real identity. Messages are linkable only over the short validity period of a pseudonym. The validity period of the pseudonym depends on its privacy requirement. Thus, satisfy unlikability requirement in (J. Liu et al., 2018) and (Y. Liu et al., 2017).

Claim 2. *Our protocol protects the privacy of the originators against an internal adversary.*

Proof: Let an internal adversary be β. Consider the following anonymity game. We generate key pair as depicted in our work and obtaining n key pairs $(pk_{V_1}, sk_{V_1}), \ldots, (pk_{V_n}, sk_{V_n})$. The system parameters π is forwarded to adversary β upon request where

$\pi = \langle p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, g_3, e, h_1, h_2, h_3 U_1, U_{\mathrm{v}}, U_{\mathrm{v}}, H_1, H \rangle$

We assume that the adversary β query the vehicle's secret key at index i, $1 \leq i \leq n$. We respond with key pair (pk_{V_i}, sk_{V_i}). We produce a valid signature σ_i on M using sk_{V_i}) and forward σ_i to β. The adversary β then generates a message M^*. We randomly choose a bit $b \in_R 0, 1$ where b is unknown to us. We then compute a signature σ^* on M^* using $(sk_{V_i} b)$. We send σ^* to β. When β obtains the signature, β analyses the signature and outputs the guess of b' of b where $b' \in_R 0, 1$. We declare failure and β wins the game, provided tha tβ can guess the value of $b' = b$. This anonymity game defines the advantage of adversary β winning the game as equation below, where $Pr[b' = b]$ represents the probability of $b' = b$ where $Pr[b' = b] = \frac{1}{2}$.

The probability is taken over the coin tosses of adversary β. Consequently, the adversary β is unable to exploit the randomized key generation and signing algorithm to win the anonymity game in polynomial time with a non-negligible probability. Hence, our protocol satisfy the privacy requirement.

3) **Accountability**.An entity performing some unlawful actions is traceable by the TP. Moreover, it must satisfy non-repudiation, that is, the assurance that they cannot deny to be the originator of the malicious message. When the malicious activity is proven true, the TP has evidence to revoke the vehicle off the network.

Claim 3. *Our protocol achieves all the accountability requirements.*

Proof: We fulfil the accountability requirement of traceability, non-repudiation and revocation in our scheme. The property of traceability is satisfied where the group signature allows the *TC* to reveal signature of a malicious vehicle. The identity of an adversary is traceable when the same component of σ_4 is recognized upon verifying the same message more than once and the proof runs similar to the proof in Claim 1. Non-repudiation is achieved since *AC* does not have access to the vehicle's secret key as the vehicle is the sole holder of the signing key, as illustrated in our scheme. Meanwhile, revocation is supported by the *TC* who maintains some trapdoor information to revoke dishonest vehicles. For an elaboration of the revocation technique, we refer the readers to our previous work in (Shari et al., 2020).

We show that our construction completes the security requirement of message reliabilty and privacy in IoV network. Table 4.2 present a summary of the security requirement analysis. We compare the functionalities of message reliability and privacy requirement with other existing announcement protocols in IoV network in the literature as we illustrated in Table 4.2. In our work, we successfully satisfy the conflicting security requirement of message reliability, privacy and accountability simultaneously which outperform CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017) schemes. Hence, our authenticated anonymous announcement protocol is proposed to address the gap and adaptable for IoV network.

Table 4.2: Security Requirement in VC Network

Scheme	Reliability			Privacy		Accountability		
	Sender's authenticity	Data integrity	Truthfulness	Anonymity	Unlikability	Traceability	Non repudiation	Revocation
CLSS (J. Liu et al., 2018)	✓	✓	✗	✓	✓	✓	✓	✗
PPDAS (Y. Liu et al., 2017)	✓	✓	✓	✓	✓	✓	✗	✗
Our work	✓	✓	✓	✓	✓	✓	✓	✓

4.6.2 Performance Analysis

This section we evaluate the performance efficiency between our proposed protocol with CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017). To provide a security level of 2^{80}, approximately the same level as a standard 80-bit security level we set p a 160-bit long prime and then the element in $\mathbb{G}_1$ is 160 bits long by choosing an appropriate curve such as National Institute of Standards and Technology (NIST) curve (Brown et al., 2001; Mell & Grance, 2011). With respect to the communication overhead, in our proposed protocol a broadcasted message composed of one payload, one time stamp, one group ID and one real identity of RSU. If we further use 100 bytes, 2 bytes, 2 bytes and 1 bytes to represent a payload, a time stamp, a group ID and real identity of RSU respectively then the length of vehicle-generated messages with 80-bit security level can be computed as 100 + 2 + 128 + 2 + 1 = 233 bytes. In CLSS (J. Liu et al., 2018), the length of message is 640 bytes while in PPDAS (Y. Liu et al., 2017) the message size is 849 bytes. Our scheme deploy group signature in message broadcast where a member of a group of vehicles can sign a message anonymously on the behalf of the group, therefore we set the length of the signature in our protocol is 128 bytes. Hence we can conclude our protocol achieve better communication cost than the other selected schemes. We depict the communication cost as in Figure 4.3. We conduct our comparison in two categories:

Computational cost. We evaluate the computational cost of signature generation and verification in the broadcast of message. Table 4.3 shows the number of operation for each algoritmn for our proposed protocol. We consider the three most expensive operations, particularly scalar multiplication in $\mathbb{G}_1$, exponentiation in $\mathbb{G}_T$ and pairing evaluation. We compare the computational cost between our scheme with (J. Liu et al., 2018) and (Y. Liu et al., 2017) for t=1.

In this table, $k.\mathbb{G}_1$ indicates k scalar multiplications in $\mathbb{G}_1$, $v.P$ indicates v pairing

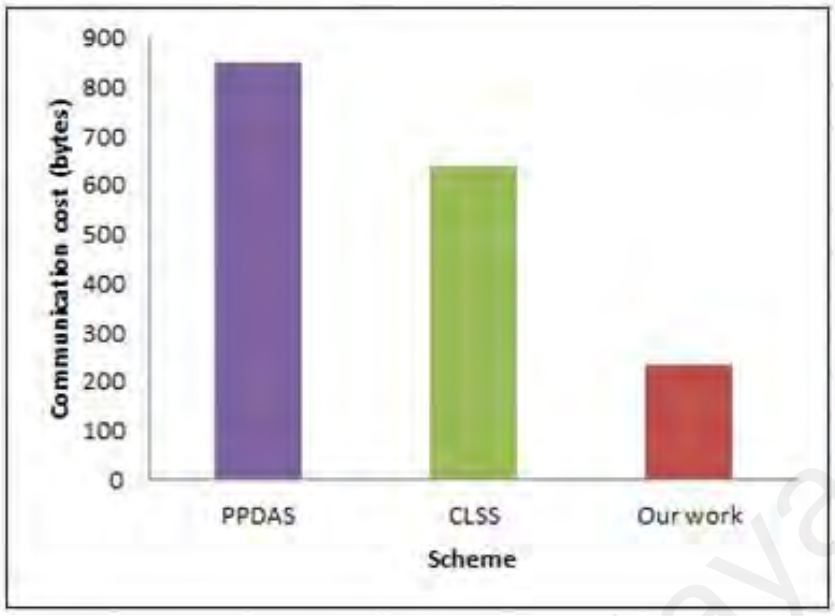

Figure 4.3: The communication cost of our protocol

operations. The signing operation in CLSS (J. Liu et al., 2018) requires 2.$\mathbb{G}_1$ and the verification require 1 Pairing + 3.$\mathbb{G}_1$. Meanwhile, the PPDAS (Y. Liu et al., 2017) scheme require 1 Pairing + 1.$\mathbb{G}_1$ for the signing operation, whereas the verification phase requires 1 Pairing + 5.$\mathbb{G}_1$. The signing procedure for our proposed protocol requires 6.$\mathbb{G}_1$ and the verification requires one pairing + 4.$\mathbb{G}_1$ operations. These findings are summarised in Table III. We see that the computational cost for our scheme is comparable with CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017) scheme.

Computation time. Based on the set value of p = 160 bits and $\mathbb{G}_1$ = 161 bits, one pairing evaluation and one scalar multiplication in $\mathbb{G}_1$ can be done within 4.5 ms and 0.6 ms respectively (L. Chen et al., 2011). Using this information, we calculate the computation time of operations tabulated in the computational cost column of Table IV. For instance, to calculate 'Sign' operation in our work, we take 0.6ms then multiply it by 6.$\mathbb{G}_1$ to obtain 3.6 ms. Similarly for the 'verify' operation, for 1 Pairing + 4.$\mathbb{G}_1$ we multiply each of them with 0.6 ms and 4.5 ms respectively to obtain 6.9 ms. We present the rest of the calculation

result in Computation Time column of Table 4.3.

From the above analysis, our work reuires lower communication cost as compared to the schemes (J. Liu et al., 2018) and (Y. Liu et al., 2017). We can conclude that our work achieves comparable performance to CLSS (J. Liu et al., 2018) and more efficient compared with PPDAS (Y. Liu et al., 2017) while providing the additional features of flexible threshold authentication and a secure privacy preserving by deploying group signature. Table 4.2 and Table 4.3 summarizes the performance of our proposed protocol.

Table 4.3: Comparison of Performance Analysis

	Communication Cost	Computational Cost		Computation Time	
		Sign	Verify	Sign (ms)	Verify(ms)
CLSS (J. Liu et al., 2018)	640 Bytes	2.$\mathbb{G}_1$	1 Pairing + 3.$\mathbb{G}_1$	1.2	6.3
PPDAS (Y. Liu et al., 2017)	849 Bytes	1 Pairing + 1.$\mathbb{G}_1$	1 Pairing + 5.$\mathbb{G}_1$	5.1	7.5
Our work	233 Bytes	6.$\mathbb{G}_1$	1 Pairing + 4.$\mathbb{G}_1$	3.6	6.9

4.6.3 Simulation Analysis

The network simulator NS 2.35 was used. Our simulation analysis are conducted based on the V2V and V2P communication. We implement IEEE 802.11a as the wireless network. We note that this wireless network offering service same as 5G network protocol. We evaluated two major performance metrics for V2V communication, denoted as average message delay (MD_{v}) and average message loss ratio (ML_{v}). Meanwhile, we analysed average message delay (MD_{p}) for V2P communication. We assume the vehicular nodes and pedestrian are distributed at random. In order to assess our performance metric, we formulated in such a way:

$$MD_{\mathrm{v}} = \frac{N_v \times M_{sent} \times T_{sign}}{M_{received}}$$

$$ML_{\mathrm{v}} = \frac{(N_v - M_{received}) \times T_{verify}}{N_c \times N_v}$$

$$MD_{\mathrm{p}} = \frac{N_p \times N_v \times (T_{sign} + T_{verify})}{N_p}$$

where N_v, N_c, N_p is number of vehicle, cloud and pedestrian respectively. Meanwhile, M_{sent} is amount of message sent, $M_{received}$ known as amount of message received. Total signature time denoted as T_{sign} and total verification time symbolize as T_{verify}.

The simulation design setting for this scheme is as follows as in Table 4.4:

Table 4.4: Simulation Parameters

Parameters	Value
Mobility model	Ad hoc On-Demand Distance Vector (AODV)
Simulation region	2 km x 2 km
No of vehicles	20-100
No of pedestrian	5-25
Speed of vehicles	20-108 km/h
Speed of pedestrian	5 km/h
Data rate	6 Mbps
Messaging frequency	10Msg/s, 20 Msg/s
Simulation time	30 min

The simulation results are shown in Figure 4.4 and Figure 4.5 for V2V communication. In this experiment, we set our threshold at *(*t)=5 where *(*t) indicates trustworthiness of messages. The trustwothiness of message can be illustrate as vehicle observe the same event in the vicinity and agree with the broadcasted safety message.

Figure 4.4 shows the simulation result of average message delay with respect to number of vehicles. A higher average of message delay implies that a lower number of vehicles can utilize the verified message, hence affect the driving efficiency. We assume each

vehicle broadcast one message. We observe that our work yields the lowest message delay followed to CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017) schemes. We consider this is natural because a higher number of vehicles in the vicinity may receive a higher number of verified of the same message up to the predefined threshold. This proves that our proposed protocol has advantage over other schemes.

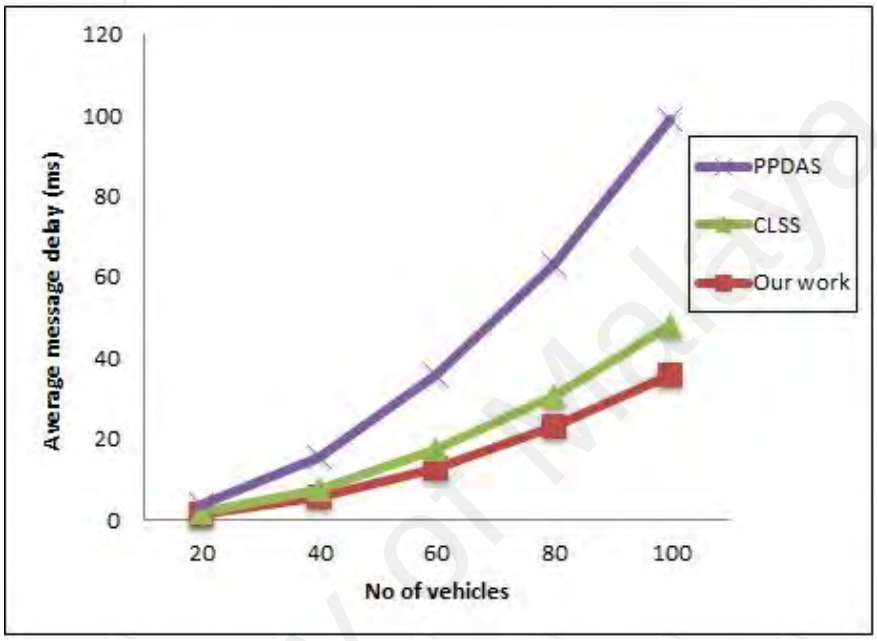

Figure 4.4: The relationship between average message delay and number of vehicles

Figure 4.5 shows the simulation result of average message loss ratio with respect to number of vehicles. The average message loss demonstrates the protocol's validity and feasibility. For a given threshold, we observe that, the average message loss increases as the number of vehicle increase. We discover that this feature is triggered by a large number of messages being lost because the bulk of the message is sent repeatedly due to heavy traffic. In terms of message loss, our scheme apparently comparable and better than CLSS (J. Liu et al., 2018) and PPDAS (Y. Liu et al., 2017) schemes.

Meanwhile, for V2P communication, we observe the simulation result of average message delay against number of pedestrian as in Figure 4.6. As we can see, the rate of average message delays grows almost linearly to number of pedestrian in simulation area.

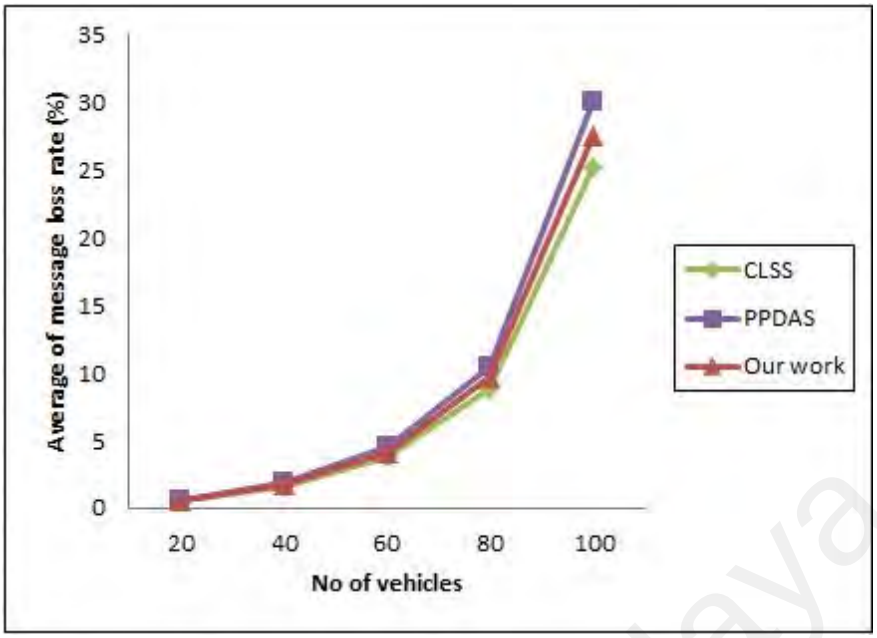

Figure 4.5: The relationship between average message loss ratio and number of vehicles

This functionality ensures that our protocol is acceptable to different traffic situations and does not significantly degrade its performance in the case of a large number of vehicles.

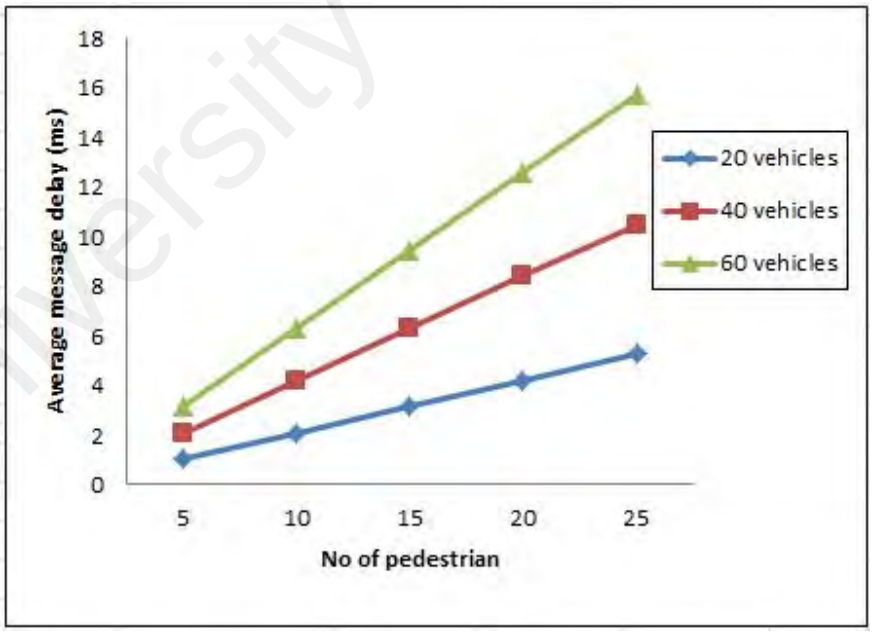

Figure 4.6: The relationship between average message delay and number of pedestrian

4.7 Conclusion

In this chapter, we have presented a secure and efficient authenticated anonymous announcement protocol for IoV network where the underlying cyptographic primitive is based on group signature. Our extensive generic abstraction architecture can help provide guidance for the design of future announcement protocol based on group signatures in IoV network. We have constructed a new group signature protocol based on our generic abstraction. As far as we are aware, this is the first generic abstraction for announcement protocol using group signature for IoV in the literature. We have demonstrated that our protocol effectively satisfies these conflicting requirements of reliability, anonymity, and accountability of messages. The results of performance analysis and simulation prove our work is resilient against adversaries and achieves good performance efficiency in IoV communication.

CHAPTER 5: CONCLUSION

This chapter concludes the contributions of this thesis and discuss the directions for future work.

5.1 Summary of Contributions

IoV has been one of the new wireless communication technologies to improve the efficiency and quality of transportation. This technology provides vehicles to exchange various information collected and transmitted via the massive internet environment on road and traffic patterns such as traffic congestion, accidents, road conditions and collision avoidance. Therefore, all neighboring entities are notified of potential hazards and thus are able to take reasonable precautions to avoid those dangers.

The security and privacy concerns received significant attention in IoV. It makes them susceptible to an adversary or malicious parties, as vehicles connected to the internet. An adversary can cause damage, congestion and accidents by injecting malicious input into the vehicle. If a network intrusion occurs in IoV, vehicles may be under the control of an adversary. The adversaries may control the vehicle system, send fake messages, and track vehicles activities thereby causing harm on road users. This thesis emphasizes on internal adversaries's threats because most external threats can be avoided by maintaining privacy and improving device authenticity.

In this paper, we have presented a secure and efficient announcement protocol for IoV network where the underlying cyptographic primitive is based on group signature. We showed that our protocol efficiently solve these contradictory requirements of message reliability, privacy and accountability in IoV announcement protocol using 5G communication channel. We examined related work associated to vehicular communication network

in VC, the advantages and limitation of VC schemes and schemes that present security and privacy issues in IoV. We formulated generic abstraction for announcement protocol using group signature for IoV. Our comprehensive construction of generic abstraction may assist to provide guidelines to design future announcement protocol based on group signatures in IoV network. We designed a new group signature announcement protocol based on our generic abstraction. We have demonstrated that our protocol efficiently address the conflicting security requirements of reliability, privacy and accountability simultaneously. Implementation of our work on NS 2.35 simulator proves the practicality and applicabilitiy of our protocol in real world deployment.

5.2 Directions for Future Works

There are several research directions that can be followed beginning from the work presented in this thesis. Some of the possible extensions are defined as follows.

- While this research focuses on announcemnet protocol for group signature in IoV that utilized threshold method to evaluate message reliability, it might be interesting to design announcement protocol in IoV based on other method to measured the reliability of the message.

- In our scheme, the pedestrian can only receive verified message from the cloud via RSU. Extending the current scheme could be of interest where a pedestrian can also announce the safety message. How the configuration of the system will not violate other security requirements is the focus of future research.

- Exploring other cryptographic techniques that can greatly improve the performance efficiency for a reliable annoucement protocol in IoV without sacrificing on security

requirements.

- It might be worthwhile to formulate abstract model of announcement protocols based on other cryptographic primitives. This may reduce the possibility of overlooking some important features to design a practical announcement protocol.

REFERENCES

Abueh, Y. J., & Liu, H. (2016). Message authentication in driverless cars. *Proceedings of IEEE Symposium on Technologies for Homeland Security*, *1*, 1–6.

Ahmad, A. A., Colin, B., & M, G. N. J. (2012). Geoproof: Proofs of geographic location for cloud computing environment. *Proceeding of the 32nd International Conference on Distributed Computing Systems Workshops*, *1*, 506-514.

Ahmed, B., Malik, A. W., Hafeez, T., & Ahmed, N. (2019). Services and simulation frameworks for vehicular cloud computing: a contemporary survey. *EURASIP Journal of Wireless Communication and Networking*, Article#4.

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2018). A survey on 5g networks for the internet of things: Communication technologies and challenges. *IEEE Access*, *6*, 3619–3647.

Alzain, M. A., Soh, B., & Pardede, E. (2013). A survey on data security issues in cloud computing: From single to multi-clouds. *Journal of Software*, *8*(5), 1068–1078.

Argawal, R., Pranay, S. S., Rachana, K., & Sultana, H. P. (2019). Identity-based security scheme in internet of vehicles. *Smart Intelligent Computing and Applications, Smart Innovation, System and Technologies*, *104*, 515–523.

Argawal, Y., Jain, K., & Karabasoglu, O. (2018). Smart vehicle monitoring and assistance using cloud computing in vehicular ad hoc networks. *International Journal of Transportation Science and Technology*, *7*, 60-73.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., ... Zaharia, M. (2010). A view of cloud computing. *Communication ACM*, *53*(4), 50–58.

Ateniese, G., Camenisch, J., Joye, M., & Tsudik, G. (2000). A practical and provably secure coalition-resistant group signature scheme. *Springer*, *1880*, 255–270.

Bellare, M., Shi, H., & Zhang, C. (2005). Foundations of group signatures: The case of dynamic groups. *Springer*, *3376*, 136–153.

Bermad, N., Zemmoudj, S., & Omar, M. (2019). Context-aware negotiation, reputa-

tion and priority traffic light management protocols for vanet-based smart cities. *Telecommunication Systems*, *72*(1), 131–153.

Boneh, D., Boyen, X., & Shacham, H. (2004). Short group signatures. *Springer*, *3152*, 41–55.

Boukerche, A., & Grande, R. E. D. (2018). Vehicular cloud computing: Architectures, applications, and mobility. *Computer Networks*, *135*, 171–189.

Brown, M., Hankerson, D., López, J., & Menezes, A. (2001). Software implementation of the NIST elliptic curves over prime fields. *Springer*, *2020*, 250–265.

Campbell, J. L., Richard, C. M., Brown, J. L., & McCallum, M. (2007). Crash warning system interfaces. *NHTSA. Final Report DOT HS 810697*.

Chaum, D., & van Heyst, E. (1991). Group signatures. *Springer*, *547*, 257–265.

Chen, C., Xiang, B., Liu, Y., & Wang, K. (2019). A secure authentication protocol for internet of vehicles. *IEEE Access*, *7*, 12047–12057.

Chen, L., Ng, S., & Wang, G. (2011). Threshold anonymous announcement in vanets. *IEEE Journal on Selected Areas in Communications*, *29*(3), 605–615.

Contreras-Castillo, J., Zeadally, S., & Ibáñez, J. A. G. (2018). Internet of vehicles: Architecture, protocols, and security. *IEEE Internet of Things Journal*, *5*(5), 3701–3709.

Cui, J., Xu, W., Zhong, H., Zhang, J., Xu, Y., & Liu, L. (2018). Privacy-preserving authentication using a double pseudonym for internet of vehicles. *Sensors*, *18*(5), Article#1453.

Daza, V., Domingo-Ferrer, J., Sebé, F., & Viejo, A. (2009). Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. *IEEE Transactions Vehicular Technology*, *58*(4), 1876–1886.

Defrawy, K. M. E., & Tsudik, G. (2011). ALARM: anonymous location-aided routing in suspicious manets. *IEEE Transactions Mobile Computing*, *10*(9), 1345–1358.

Dillon, T. S., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. *IEEE Computer Society*, 27–33.

Eze, E. C., Zhang, S., & Liu, E. (2014). Vehicular ad hoc networks (vanets): Current state, challenges, potentials and way forward. *Paper presented at 20th International Conference on Automation and Computing, September 12-13, Bedfordshire, United Kingdom*.

Eze, E. C., Zhang, S., & Liu, E. (2015). Improving reliability of message broadcast over internet of vehicles (iovs). *Paper presented at 15th IEEE International Conference on Computer and Information Technology, CIT, October 26-28 Liverpool, United Kingdom.*.

Ferrag, M. A., Maglaras, L. A., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4g and 5g cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, *101*, 55–82.

Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud computing and grid computing 360-degree compared. *Computing Research Repository*, *901*, 1–31.

Ghafoor, K. Z., Bakar, K. A., Mohammed, M. A., & Lloret, J. (2013). Vehicular cloud computing: Trends and challenges. *Mobile Networks and Cloud Computing Convergence for Progressive Services and Applications*, *14*, 262-274.

Guo, L., Dong, M., Ota, K., Li, Q., Ye, T., Wu, J., & Li, J. (2017). A secure mechanism for big data collection in large scale internet of vehicle. *IEEE Internet of Things Journal*, *4*(2), 601–610.

Hartenstein, H., & Laberteaux, K. P. (2010). VANET: vehicular applications and inter-networking technologies. *Wiley Online Library*.

He, D., Zeadally, S., Xu, B., & Huang, X. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Transactions Information Forensics and Security*, *10*(12), 2681–2691.

He, W., Yan, G., & Xu, L. D. (2014). Developing vehicular data cloud services in the iot environment. *IEEE Transactions Industrial Informatics*, *10*(2), 1587–1595.

Huang, Q., Yang, Y., & Shi, Y. (2018). Smartveh: Secure and efficient message access control and authentication for vehicular cloud computing. *Sensors*, *18*(2), Article#666.

Hussain, R., Abbas, F., Son, J., & Oh, H. (2013). Tiaas: Secure cloud-assisted traffic information dissemination in vehicular ad hoc networks. *Paper presented at 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, May 13-16, Delft, Netherlands*.

Hussain, R., Hussain, F., & Zeadally, S. (2019). Integration of vanet and 5g security: A review of design and implementation issues. *Intelligent transportation systems*.

Hussain, R., & Oh, H. (2014). Cooperation-aware VANET clouds: Providing secure cloud services to vehicular ad hoc networks. *Journal of Information Processing System*, *10*(1), 103–118.

Hussain, R., Rezaeifar, Z., & Oh, H. (2015). A paradigm shift from vehicular ad hoc networks to vanet-based clouds. *Wireless Personal Communications*, *83*(2), 1131–1158.

Hussain, R., Son, J., Eun, H., Kim, S., & Oh, H. (2012). Rethinking vehicular communications: Merging VANET with cloud computing. *Paper presented at 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, December 3-6, Taipei, Taiwan*.

Iqbal, S., Kiah, M. L. M., Anuar, N. B., Daghighi, B., Wahab, A. W. A., & Khan, S. (2016). Service delivery models of cloud computing: security issues and open challenges. *Security and Communication Networks*, *9*(17), 4726–4750.

Jameel, F., Chang, Z., Huang, J., & Ristaniemi, T. (2019). Internet of autonomous vehicles: Architecture, features, and socio-technological challenges. *IEEE Wireless Communication*, *26*(4), 21–29.

Jiang, Q., Ni, J., Ma, J., Yang, L., & Shen, X. (2018). Integrated authentication and key agreement framework for vehicular cloud computing. *IEEE Network*, *32*(3), 28–35.

Joy, J., & Gerla, M. (2017). Internet of vehicles and autonomous connected car - privacy and security issues. *Paper presented at 26th International Conference on Computer Communication and Networks, July 31 - Aug. 3, Vancouver, BC, Canada*.

Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C., & Liu, X. (2016). Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access*, *4*, 5356–5373.

Kang, J., Yu, R., Huang, X., & Zhang, Y. (2018). Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Transactions Intelligent Transportation Systems*, *19*(8), 2627–2637.

Kounga, G., Walter, T., & Lachmund, S. (2009). Proving reliability of anonymous information in vanets. *IEEE Transactions Vehicular Technology*, *58*(6), 2977–2989.

Kumar, N., Misra, S., & Obaidat, M. S. (2015). Collaborative learning automata-based routing for rescue operations in dense urban regions using vehicular sensor networks. *IEEE Systems Journal*, *9*(3), 1081–1090.

Lee, E., Lee, E., Gerla, M., & Oh, S. (2014). Vehicular cloud networking: Architecture and design principles. *IEEE Communications Magazine*, *52*(2), 148–155.

Li, Q., Malip, A., Martin, K. M., Ng, S.-L., & Zhang, J. (2012). A reputation-based announcement scheme for vanets. *IEEE Transactions Vehicular Technology*, *61*(9), 4095-4108.

Liu, J., Li, Q., Sun, R., Du, X., & Guizani, M. (2018). An efficient anonymous authentication scheme for internet of vehicles. *Paper presented at IEEE International Conference on Communications, ICC 2018,May 20-24 Kansas City, MO, USA*.

Liu, Y., Wang, Y., & Chang, G. (2017). Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an iov paradigm. *IEEE Transactions Intelligent Transportation Systems*, *18*(10), 2740–2749.

Malip, A. (2014). Anonymous authenticated announcement schemes in vehicular ad hoc networks. *(Doctoral Dissertation)*, 156.

Malip, A., Ng, S.-L., & Li, Q. (2014). A certificateless anonymous authenticated announcement scheme in vehicular ad hoc networks. *Security and Communication Networks*, *7*(3), 588-601.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing

- the business perspective. *Decision Support Systems*, *51*(1), 176–189.

Mell, P., & Grance, T. (2011). The nist definition of cloud computing. *Special Publication*, *800*, Article#145.

Menezes, A. (2009). An introduction to pairing-based cryptography. *Recent trends in cryptography, American Mathematical Society*.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. *CRC Press*, 49–86.

Oh, H., & Hussain, R. (2014). Cooperation-aware VANET clouds: Providing secure cloud services to vehicular ad hoc networks. *Journal of Information Processing System*, *10*(1), 103–118.

Olariu, S., Khalil, I., & Abuelela, M. (2011). Taking VANET to the clouds. *International Journal of Pervasive Computing and Communications*, *7*(1), 7–21.

Park, M., Gwon, G., Seo, S., & Jeong, H. (2011). Rsu-based distributed key management (RDKM) for secure vehicular multicast communications. *IEEE Journal on Selected Areas in Communications*, *29*(3), 644–658.

Raya, M., Aziz, A., & Hubaux, J. (2006). Efficient secure aggregation in vanets. *Paper presented at Proceedings of the Third International Workshop on Vehicular Ad Hoc Networks, VANET 2006, September 29, Los Angeles, CA, USA*.

Raya, M., & Hubaux, J. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39–68.

Raya, M., Papadimitratos, P., & Hubaux, J. (2006). Securing vehicular communications. *IEEE Wireless Communications*, *13*(5), 8–15.

Ruj, S., Stojmenovic, M., & Nayak, A. (2014). Decentralized access control with anonymous authentication of data stored in clouds. *IEEE Transactions Parallel Distribution System*, *25*(2), 384–394.

Sahbi, R., Ghanemi, S., & Djouani, R. (2018). A network model for internet of vehicles based on SDN and cloud computing. *Paper presented at the 6th International*

Conference on Wireless Networks and Mobile Communications, WINCOM.

Scott, L., & Denning, D. E. (2003). A location based encryption technique and some of its applications. *Institute of Navigation National Technical Meeting*, 734-740.

Shari, N. F. M., Malip, A., & Othman, W. A. M. (2020). Revocation protocol for group signatures in vehicular ad hoc networks: A secure construction. *KSII Transactions on Internet and Information Systems*, *14*, 299–322.

Song, C., Gu, X., Wang, L., Liu, Z., & Ping, Y. (2019). Research on identity-based batch anonymous authentication scheme for vanet. *KSII Transactions on Internet and Information Systems*, *13*, 6175–6189.

Spelta, C., Manzoni, V., Corti, A., Goggi, A., & Savaresi, S. M. (2010). Smartphone-based vehicle-to-driver/environment interaction system for motorcycles. *Embedded Systems Letters*, *2*(2), 39–42.

Stergiou, C., Psannis, K. E., Kim, B., & Gupta, B. B. (2018). Secure integration of iot and cloud computing. *Future Generation Computing System*, *78*, 964–975.

Storck, C. R., & de L. P. Duarte-Figueiredo, F. (2019). A 5g V2X ecosystem providing internet of vehicles. *Sensors*, *19*(3), Article#550.

Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L., . . . Xiong, Y. (2015). Security and privacy in the internet of vehicles. *Paper presented at International Conference on Identification, Information, and Knowledge in the Internet of Things, IIKI 2015, October 22-23, Beijing, China*.

Sur, C., Park, Y., & Rhee, K. H. (2016). An efficient and secure navigation protocol based on vehicular cloud. *Intrnational Journal of Computing Mathematics*, *93*(2), 325–344.

Talib, M. A., Abbas, S., Nasir, Q., & Mowakeh, M. F. (2018). Systematic literature review on internet-of-vehicles communication security. *International Journal of Distributed Sensor Network*, *14*, Article#12.

UNRSC. (2011). *Global plan for the decade of action for road safety 2011-2020.* Retrieved 2019-01-30, from `http://www.who.int/roadsafety/decade_of_action/plan/plan_english.pdf`

Vasudev, H., & Das, D. (2019). An efficient authentication and secure vehicle-to-vehicle communications in an iov. *Paper presented at 89th IEEE Vehicular Technology Conference, VTC Spring 2019, April 28 - May 1, Kuala Lumpur, Malaysia*.

WHO. (2015). *Global status report on road safety 2015.* Retrieved 2019-01-30, from http://www.who.int/violence_injury_prevention/road_safety_status/2015GSRRS2015_Summary_EN_final.pdf

Wu, H., & Horng, G. (2017). Establishing an intelligent transportation system with a network security mechanism in an internet of vehicle environment. *IEEE Access*, *5*, 19239–19247.

Wu, Q., Domingo-Ferrer, J., & González-Nicolás, Ú. (2010). Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. *IEEE Transactions Vehicular Technology*, *59*(2), 559–573.

Yan, G., Olariu, S., & Weigle, M. C. (2009). Providing location security in vehicular ad hoc networks. *IEEE Wireless Communication*, *16*(6), 48–55.

Yan, G., Wen, D., Olariu, S., & Weigle, M. C. (2013). Security challenges in vehicular cloud computing. *IEEE Transactions Intelligent Transportation Systems*, *14*(1), 284–294.

Yang, F., Wang, S., Li, J., & Liu, Z. (2015). An overview of internet of vehicles. *Communications China*, *11*(10), 1–15.

Zhang, L., Meng, X., Raymond, K.-K., Zhang, Y., & Dai, F. (2020). Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud. *IEEE Transactions on Dependable Secure Computing*, *17*(3), 634–647.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computing System*, *28*(3), 583–592.

LIST OF PUBLICATIONS AND PAPERS PRESENTED

List of Publication

1. **Amir, N. A. S**., Malip, A., Othman., W. A. M. (2020). Securing anonymous authenticated announcement protocol for group signature in internet of vehicles. KSII Transactions on Internet and Information Systems, *14(11)*, 4573-4594.