UTM UNIVERSITI TEKNOLOGI MALAYSIA

	PESANAN TEMPATAN	SALINAN ASAL
	PPTJ040000062017000438	Muka Surat : 2 dari 8
	NO PENDAFTARAN UTM	BP08201100926
Nama dan alamat pembekal	NO PENDAFTARAN CBP (GST)	000174211072
FORMIS NETWORK SERVICES SDN BHD	TARIKH PESANAN	15/06/2017
6TH FLOOR, MENARA SMI,6 LORONG P.RAMLEE50250,WILAYAH PERSEKUTUAN KUALA LUMPUR	TARIKH HANTARAN	28/06/2017

RM: SERATUS SEMBILAN BELAS RIBU DUA RATUS TIGA PULUH EMPAT DAN SEN: SEPULUH SAHAJA

Pemohon HASLINDA BINTI SABARI	Disemak Pegawai Bertanggungjawab	Diluluskan Pegawai Bertanggungjawab
Alamat Hantar Barang / Perkhidmatan PEPRUSTAKAAN UTM UTM JOHOR BAHRU JOHOR 0	MOHD ALIAS TOHIRAN Pegawai Eksekutif Kanan Perpustakaan UTM Universiti Teknologi Malaysia 81310 Johor Bahru, Johor	HASLINA BINTI OTHMAN Timbalan Ketua Pustakawan (Galerium) Perpustakaan UTM Universiti Teknologi Malaysia 81310 Johor Bahru, Johor.

PERAKUAN OLEH JABATAN

Dengan ini adalah disahkan bahawa barangan/perkhidmatan yang terkandung di dalam pesanan ini telah diterima sepenuhnya dan mengikut spesifikasi yang ditetapkan

Tarikh : 18/07/2017

HASLINDA BINTI SABARI
Pustakawan
(Unit Perolehan & Penyelenggaraan Komputer)
Bahagian Automasi
(Perpustakaan UTM)
Universiti Teknologi Malaysia
81310 Johor Bahru, Johor

Tandatangan & Cop Penerima Bekalan/Perkhidmatan

PERAKUAN PEMBEKAL

Dengan ini adalah disahkan bahawa saya/syarikat kami telah membekal barang-barang atau melaksanakan perkhidmatan mengikut butiran yang terkandung dalam pesanan ini serta mutu dan syarat-syarat yang telah dipersetujui dengan Universiti Teknologi Malaysia.

FORMIS NETWORK SERVICES SDN BHD (188270-U)

Tandatangan & Cop Pembekal

PERINGATAN PENTING

1. Pembekal hendaklah menghantar pada atau sebelum tarikh hantaran kepada alamat seperti yang dinyatakan.
2. Perakuan Pembekal dan Pengesahan Penerimaan oleh Ketua Pusat Tanggungjawab hendaklah dilengkapkan.
3. Pembekal/Kontraktor diberi peringatan supaya mengemukakan bil/tuntutan yang lengkap dalam tempoh 14 hari daripada tarikh bekalan atau perkhidmatan dibekalkan atau kerja disempurnakan untuk membolehkan bayaran dibuat dengan segera. Kerajaan tidak akan bertanggungjawab di atas kelewatan pembayaran kepada pembekal/kontraktor jika bil/tuntutan tidak dihantar dengan segera dalam tempoh 14 hari.
4. CPB (GST) tidak akan dikenakan ke atas bekalan yang telah mendapat Relief Order

UNTUK KEGUNAAN UTM

Permohonan	Pendaftaran	No Rujukan Sebut Harga	No Sebut Harga	Chargeline
PMJ040000012017000106	PDJ040000052017000379	PSJ040000022017000004	SHJ022017000004	U.J040000.0100.00000

ANONYMOUS AUTHENTICATION MECHANISM BASED ON GROUP SIGNATURE AND PSEUDONYM PUBLIC KEY INFRASTRUCTURE FOR SAFETY APPLICATION OF VEHICULAR AD HOC NETWORK

ALI ASADI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

AUGUST 2016

I would like to dedicate this thesis to my beloved family without them it was impossible for me to complete my research

ACKNOWLEDGEMENT

I am indebted to my supervisor, Prof. Dr. Abdul Samad bin Haji Ismail for giving me the opportunity to work with him and introducing me to this very exciting field of vehicular ad hoc networks. Without his continued support and interest, this thesis would not have been the same as presented here. Working with him was truly a rewarding experience. I am also thankful to my thesis committee members, Prof. Dr. Abdul Hanan bin Abdullah, Prof. Dr. Md Yazid bin Mohd Saman, and Prof. Dr. Naomie binti Salim for their detailed review and constructive comments.

I am deeply grateful to my good friends Hofar Shokravi, Dr. Mohammad Ghanbari and Dr. Maneea Eizadi Sharifabad for their encouragement and support and also for including me in the many collaborative opportunities. My colleagues should also be recognized for their valuable suggestions and support. Especially I would like to express my sincere gratitude to Dr. Raheleh Hossainian, Dr. Safaa Saud, Masoumeh Shadkam, and Masoumeh Shahverdi for their assistance and support during my research.

Last but not least, I must express my sincerest and heartiest thanks to my family; Mahmood, Parvin, Maryam, Mina, Sanaz, Sania, Amirhosain, Mohammadreza Reza, and Reza for their encouraging attitude, selfless love, and unfailing patience during my entire life.

ABSTRACT

Safety applications of Vehicular Ad hoc Network (VANET) demand delay intolerant and are vulnerable to attacks due to the mobility of nodes and wireless nature of their communications. These applications require an integrated security mechanism, which provides message integrity, anonymity, non-repudiation, revocation, availability, and location authentication services. This mechanism should provide acceptable message delay with or without dependency to Road Side Units (RSUs). Realizing the importance of VANET security, two mechanisms are proposed and evaluated in this research. The mechanisms are aimed at fulfilling the VANET security requirements for safety applications with acceptable message delay. Two new lightweight security mechanisms, RSU-Aided Anonymous Authentication (RAAA) and Group Signature-based Anonymous Authentication (GSAA) have been proposed. These mechanisms are based on Group Signature (GS) and Pseudonym Public Key Infrastructure (PPKI). GS scheme was applied to ensure anonymity, non-repudiation and revocation, whereas PPKI was applied to achieve authentication and message integrity. Additionally, a novel function for location verification was proposed to guarantee availability and location authentication. Simulations were performed using NS2 to verify and evaluate the efficiency of the mechanisms for urban and highway scenarios with various traffic conditions. Simulation results showed that RAAA and GSAA outperformed Group Signature and Identity-based Signature (GSIS), and Short-Term Linkable Group Signatures with Categorized Batch Verification (STLGSCBV). In comparison to GSIS and STLGSCBV, the results indicated improvements of at least 5.26% and 7.95% in terms of vehicle density impact on message delay, and at least 11.65% and 11.22% in the case of vehicle density impact on message loss ratio. Furthermore, the simulated RAAA and GSAA methods resulted in approximately 11.09% and 10.71% improvement in message delay during signature verification in comparison to GSIS and STLGSCBV. Additionally, RAAA and GSAA proved to achieve at least 13.44% enhancement by considering signature verification on message loss ratio in comparison to GSIS and 7.59% in comparison to STLGSCBV. The simulation results also demonstrated that less than 20ms message delay was achieved by RAAA and GSAA mechanisms in the case of less than 90 vehicles within the communication range. This is an acceptable message delay and hence, the proposed mechanisms have a great potential to be used in safety critical applications.

ABSTRAK

Aplikasi Keselamatan Rangkaian Ad hoc Kenderaan (VANET) menuntut tiada toleransi kepada masa lengah dan mudah terdedah kepada serangan kerana mobiliti nod dan sifat komunikasi tanpa wayar mereka. Aplikasi ini memerlukan satu mekanisme keselamatan bersepadu yang menyediakan integriti mesej, ketanpanamaan, tanpa sangkalan, pembatalan, kebolehsediaan dan perkhidmatan pengesahan lokasi. Mekanisme ini perlu menyediakan masa lengah mesej sewajarnya dengan atau tanpa pergantungan kepada Unit Tepian Jalan (RSU). Menyedari tentang kepentingan keselamatan VANET, dua mekanisme telah dicadangkan dan dinilai dalam kajian ini. Mekanisme ini bertujuan untuk memenuhi keperluan keselamatan VANET untuk aplikasi keselamatan dengan masa lengah mesej yang boleh diterima. Dua mekanisme keselamatan ringan yang baharu iaitu Pengesahan Awanama Berbantukan RSU (RAAA) dan Pengesahan Awanama Berasaskan Tandatangan Kumpulan (GSAA) telah dicadangkan. Mekanisme ini berasaskan Tandatangan Kumpulan (GS) dan Tandatangan Digital Lengkung Eliptik (PPKI). Skema GS telah diaplikasi untuk memastikan ketanpanamaan, tanpa sangkalan dan pembatalan, manakala PPKI telah digunakan untuk mencapai pengesahan dan integriti mesej. Selain itu, fungsi baharu pengesahan lokasi telah dicadangkan untuk menjamin kebolehsediaan dan pengesahan lokasi. Simulasi telah dilaksanakan menggunakan NS2 untuk mengesah dan menilai kecekapan mekanisme yang dicadangkan dalam senario bandar dan lebuh raya dengan pelbagai keadaan lalu lintas. Keputusan simulasi menunjukkan bahawa RAAA dan GSAA mengatasi Tandatangan Kumpulan dan Tandatangan Berasaskan Integriti (GSIS), dan Tandatangan Kumpulan Pautan Jangka Pendek dengan Pengesahan Berkelompok Berkategori (STLGSCBV). Berbanding dengan GSIS dan STLGSCBV, keputusan menunjukkan peningkatan sekurang-kurangnya 5.26% dan 7.95% dari segi kesan kepadatan kenderaan kepada masa lengah mesej dan sekurang-kurangnya 11.65% dan 11.22% dalam kes kesan kepadatan kenderaan kepada kadar kehilangan mesej. Tambahan pula, simulasi kaedah RAAA dan GSAA menunjukkan lebih kurang 11.09% dan 10.71% penambahbaikan untuk masa lengah mesej semasa pengesahan tandatangan berbanding dengan GSIS dan STLGSCBV. Selain itu, RAAA dan GSAA terbukti mencapai sekurang-kurangnya 13.44% peningkatan dengan mengambil kira pengesahan tanda tangan pada nisbah kehilangan mesej berbanding dengan GSIS dan 7.59% berbanding dengan STLGSCBV. Keputusan simulasi juga menunjukkan kurang daripada 20ms mesej kelewatan telah dicapai oleh mekanisme RAAA dan GSAA untuk kes kurang daripada 90 kenderaan dalam julat komunikasi. Ini merupakan satu masa lengah mesej yang boleh diterima dan menunjukkan mekanisme mempunyai potensi yang besar untuk digunakan dalam aplikasi keselamatan kritikal.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	-	Ad Hoc On-Demand Distance Vector
BLS	-	Boneh–Lynn–Shacham
C2C-CC	-	Car-to-Car Communication Consortium
CA	-	Certificate Authority
CALM	-	Communications Access for Land Mobiles
CRL	-	Certificate Revocation List
DoS	-	Denial of Service
DSRC	-	Dedicated Short Range Communications
EC	-	Elliptic Curve
ECDSA	-	Elliptic Curve Digital Signature Algorithm
ECN	-	Electronic Chassis Number
EDR	-	Event Data Recorder
ELP	-	Electronic License Plate
ETC	-	Electronic Toll Collection
ETSI	-	European Telecommunications Standards Institute
GM	-	Group Manager
GPS	-	Global Positioning System
GS	-	Group Signature
GSAA	-	Group Signature-based Anonymous Authentication
GSB	-	Group Signature Based
GSIS	-	Group Signature and Identity-based Signature
GTA	-	Governmental Transportation Authority
HSM	-	Hardware Security Module
IB	-	Identity Based
ITS	-	Intelligent Transportation System
LEA	-	Law Enforcement Authorities
MAC	-	Medium Access Control

OBU	-	On Board Unit
PP	-	Pseudonym Provider
PPKI	-	Pseudonym Public Key Infrastructure
RAAA	-	RSU-Aided Anonymous Authentication
RL	-	Revocation List
RSU	-	Road Side Unit
STLGSCBV	-	Short-Term Linkable Group Signatures with Categorized Batch Verification
V2R	-	Vehicle to RSU
V2V	-	Vehicle to Vehicle
VANET	-	Vehicular Ad hoc Network
VM	-	Vehicle Manufacturers
WAVE	-	Wireless Access in Vehicular Environments
WHO	-	World Health Organization
WSMP	-	Wave Short Message Protocol

LIST OF SYMBOLS

v_i	-	vehicle i
m	-	safety message
sk_{vi}	-	vehicle i active private key
$\delta_{sk_{vi}}(m)$	-	digital signature of the message m signed by vehicle i active private key
pk_{vi}	-	vehicle i active public key
$Cert_{CA}(pk_{vi})$	-	certificate of vehicle i public key (pk_{vi}) issued by CA
$Cert_{gsk_{vi}}(pk_{vi})$	-	certificate of vehicle i public key (pk_{vi}) issued by its group private key (gsk_{vi})
vi_{ID}	-	ID based private key of vehicle i issued by CA
$\delta_{vi_{ID}}(m)$	-	digital signature of the message m signed by ID based private key of vehicle i (vi_{ID})
$\delta_{gsk_{vi}}(m)$	-	digital signature of the message m signed by vehicle i group private key (gsk_{vi})
G_i	-	multiplicative cyclic group i
g_i	-	generator of multiplicative cyclic group G_i
p	-	order of the group
$e\ (G_1, G_2)$	-	bilinear pairing from groups G_1 and G_2
$\psi\ (g_i)$	-	isomorphism from group G_i
$avg\_mes_{LossRatio}$	-	average message loss ratio
avg_mes_{Delay}	-	average message delay
nv	-	number of vehicles
V_i^C	-	number of consumed messages by vehicle i
V_i^R	-	number of received messages by vehicle i
n	-	total number of received messages

$signTM_i$	-	signature generation time for i^{th} message
$transmissionTM_i$	-	transmission time for i^{th} message
$verifyTM_i$	-	duration time between receiving i^{th} message by a vehicle and the finishing time of its verification process
$E_{q_1}(a, b)$	-	elliptic curve over a field q_1 which is defined by equation : $y^2 = x^3 + ax + b$
H	-	SHA-1 hash function
$el_1 (x_1, y_1)$	-	a point on the elliptic curve
pk_{RSU}	-	RSU active public key
sk_{RSU}	-	RSU active secret key
gpk_{RSU}	-	group public key issued by RSU, which has six elements; namely $g_1, g_2, h, u, v,$ and w
gpk_{mm}	-	group public key issued *via* collaboration of membership and trace manager, which has five elements; namely $g_1, h, u, v,$ and w
gsk_{RSU}	-	group manager private key of RSU, which has three elements; namely $r_1, r_2,$ and γ
gsk_{vi}	-	vehicle i group secret key issued by RUS or membership manager, which has two elements; namely A_i and x_i
loc-info	-	current location of all neighbors in sender communication range
RL	-	revocation list
r	-	number of revoked vehicles in RL
z	-	number of group members
sk_{vs}	-	sender's active private key
pk_{vs}	-	sender's active public key, which is a point $el_2(x_2, y_2)$ on the elliptic curve
gsk_{vs}	-	sender's group secret key issued by RUS or membership manager, which has two elements; namely A_s and x_s
t_1	-	timestamp of safety message
$\delta_{sk_{vs}}(m+t_1)$	-	digital signature of the message m and its timestamp signed by sender's active private key using ECDSA or EC-Schnorr, which has two elements; namely sg_1 and sg_2

t_2	-	timestamp of sender's active public key
$cer_{gsk_{vs}}(pk_{vs}, t_2)$	-	digital signature of the sender active public key and its timestamp signed by sender group secret key, which has nine elements; namely T_1, T_2, T_3, c, s_1, s_2, s_3, s_4, and s_5
SM	-	signed safety message
$TMSK$	-	trace manager private key, which has two elements; namely r_1 and r_2
$MMSK$	-	membership manager private key, which has one element; namely γ
sk_{tm}	-	trace manager's active private key
pk_{tm}	-	trace manager's active public key
sk_{mm}	-	membership manager's active private key
pk_{mm}	-	membership manager's active public key
BVP	-	batch verification parameter
nq	-	number of messages in the batch verification queue
M_j	-	active public key and its time stamp of a j^{th} message in the batch verification queue
$Msign_j$	-	certificate of active public key and its time stamp of a j^{th} message (M_j) in the batch verification queue, which it has nine elements; namely $T_{1,j}$, $T_{2,j}$, $T_{3,j}$, c_j, $s_{1,j}$, $s_{2,j}$, $s_{3,j}$, $s_{4,j}$, and $s_{5,j}$

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Vehicular ad-hoc network (VANET) is referred to co-operation of vehicles, with or without Road Side Units (RSUs), over the specific short-range communication to distribute information. This recent technological innovation provides a more secure and comfortable transportation by offering solutions for road safety, transportation efficiency and passenger entertainments (ETSI, 2009; Baldessari *et al.*, 2007).

Road safety is a life and death issue. Based on U.S. Department of Transportation statistic report, transportation contributes to almost one-third of the accidental deaths of young people in the United States (USDOT, 2013). Typically, over 1.2 million people die in road accidents around the globe annually. In addition to that, every year between 20 to 50 million people experience non-fatal accidents which some leads to lifelong disabilities (WHO, 2009).

For above mentioned reasons, enhancing driving safety and traffic efficiency are the main reasons for utilizing the potential of the VANET through its Vehicle to RSU (V2R or R2V) and Vehicle to Vehicle (V2V) communication (Zeadally *et al.*, 2012; ETSI, 2009; Hartenstein and Laberteaux, 2008; Baldessari *et al.*, 2007).

VANET communications utilize Dedicated Short-Range Communications (DSRC) channel allocated in 5.9 GHz band (Kenney, 2011). Wireless Access in Vehicular Environments (WAVE) architecture explains the necessary architecture and services for VANET devices (IEEE-1609.0, 2014). The WAVE protocol stacks are included in IEEE 802.11 and IEEE 1609 standards where for physical (PHY) and Medium Access Control (MAC) layers, the IEEE 802.11 standard (IEEE-802.11, 2012) is adopted for VANET communication.

VANET applications are classified as road safety, traffic efficiency, and infotainment (Karagiannis *et al.*, 2011; ETSI, 2009). Safety applications attempt to improve road safety by providing information of roads and vehicles to predict and prevent collisions. Safety applications are involved with life circumstances of vehicles' passengers. Which make them time sensitive, and requires high levels of message integrity. These types of applications usually communicate in a local area range of few kilometres or hops (Hartenstein and Laberteaux, 2009; Olariu and Weigle, 2009).

For making VANET more trustable for users, transmitted data by VANET needs to be authenticated. However, an authenticated message might be used to trace vehicle owners via VANET. Therefore, an authentication mechanism, which protects users' privacy, is crucial (Emara *et al.*, 2015; Fan *et al.*, 2012). On the other hand, safety applications requirements have a significant role in VANET security and need to be taken into serious consideration. It is of most importance that security mechanisms of safety applications meet the specific performance conditions which without considering them, they might be unsuitable for VANET (Lin and Lu, 2015; Kavitha and Tangade, 2013; Papadimitratos *et al.*, 2008; ploessl and Federrath, 2008). Based on the literature review on VANET, the most important security services utilized by safety applications are message integrity, anonymity, non-repudiation, revocation, availability, and location authentication.

1.2 Background of Problem

Due to mobility of nodes and wireless nature of communication, VANET's security is vulnerable and it could be an inviting target of many attacks. Attacks against VANET might be dangerous for drivers and passengers, as false message or delay on sending message could lead to an accident. Therefore, transferring information through VANET needs to have authentication and message integrity security services. Since communication can lead to vehicles' tracking, authentication and integrity without protecting user privacy is insufficient. Anonymity is a very common approach to protect privacy of individuals and can be provided in communication systems by pseudonyms. VANET pseudonym authentication mechanisms are classified as symmetric and asymmetric mechanisms (Lin and Lu, 2015; Petit *et al.*, 2015; Al-Sultan *et al.*, 2014).

Comparing symmetric cryptography with asymmetric cryptography, the former is more efficient in computation and communication overhead. In symmetric schemes, access to the secret key for signing or verification of the message should be restricted as, any node can generate valid signature while it has the secret key. Thus, a node's anonymity extends to all nodes with the same secret key. However, symmetric cryptography cannot provide the non-repudiation characteristic as the main feature for accountability of drivers' actions (Yang, 2013). Hence, the use of asymmetric cryptography seems to be a more suitable approach for providing security of VANET safety applications.

Asymmetric VANET pseudonym authentication methods are categorized into three classes, namely Pseudonym Public Key Infrastructure (PPKI), Identity Based (IB), and Group Signature Based (GSB) schemes. In PPKI scheme, a set of public/private keys with certificates issued by Certificate Authority (CA) are used for anonymous authentication. However, due to the vast number of vehicles on the road, the CA certificate database could become huge. As a result, retrieving information of a malicious vehicle becomes time-consuming for authorized authority. Therefore, this authentication scheme might fail in taking the scalability as well as resulting in communication overhead (Yang, 2013; Xue and Ding, 2012). In order to overcome these issues, the majority of new PPKI schemes concentrate on providing appropriate approaches for issuing as well as changing vehicle's pseudonyms.

Armknecht *et al.* (2007) proposed a mechanism to issue pseudonyms for vehicles. They suggested vehicles produce the pseudonyms and then CA certified them. Their mechanism utilizes bilinear pairing as well as zero-knowledge proofs to generate pseudonym. In this method, for revoking a key, the CA publishes updated system parameters, which prevents the revoked vehicles to update their master key. Unfortunately, this mechanism suffers from communication overhead.

In another study, Calandriello *et al.* (2007) proposed a hybrid mechanism which is a combination of traditional PPKI and group signature scheme. Here, each vehicle holds one common group public key as well as an individual group private key. Vehicle generates a set of public/ private keys and certifies them accordingly by using its own group private key to use them as pseudonyms in communication. This mechanism solves some issues of the PPKI mechanisms; however, it has insufficient pseudonym update. In addition, this mechanism is vulnerable against tunnelling and Sybil attacks, therefore, it cannot provide availability services as an important requirement needed by safety applications.

One of the other hybrid PPKI mechanisms is the Studer *et al.* (2009) approach. They use group signature mechanism between pseudonymous provider and vehicles to securely transfer limited certified pseudonym to vehicles. Subsequently, vehicles use these pseudonyms in traditional PPKI mechanism to sign their messages. However, using the Studer *et al.* (2009) mechanism, when the number of revoked members increased, the pseudonym generation time will increase dramatically. In addition, this mechanism has insufficient key update. The other drawback of this method is that vehicles are required to obtain a new pseudonym in every 2 to 3 minutes, which could consequently result in communication overhead.

In overall, Armknecht *et al.* (2007) , Calandriello *et al.* (2007), and Studer *et al.* (2009) approaches are able to provide message integrity, anonymous authentication, non-repudiation, and revocation security services without requiring RSUs. However, location authentication is not provided by these mechanisms and they are vulnerable against Sybil attack.

On the other hand, Petit *et al.* (2015) indicated that one of the most important parameter of pseudonym usage is the changing rate. Indeed, it affects the communication, computation, and storage overhead along with the level of privacy. In the past decade, several pseudonym change methods have been proposed. Eckhoff *et al.* (2010) suggested a strategy in which, each vehicle keeps a set of pseudonyms (called pseudonym pool) and also changes its pseudonym at certain time slots rather than storing a huge amount of pseudonyms. However, tracking still becomes trivial while the attacker is able to recognise the period of pseudonym change. For addressing this issue, Yuanyuan *et al.* (2011) suggested that vehicles change their pseudonym randomly. Therefore, an adversary cannot predict the next pseudonym change. Nevertheless, tracking remains possible in which, just one or few vehicle change pseudonyms at the same time, since all other neighbours would continue using the same identity. Finally, it should be mentioned that both of these mechanisms encountering lack of location authentication.

The second type of asymmetric VANET pseudonym authentication is IB schemes which use vehicle identifier as vehicles public key to act as pseudonym. When a vehicle asked for pseudonym, the Trusted Authority (TA) extracts a private key from the vehicle's identifier (vehicle pseudonym public key) and sends it back to the vehicle. Similar to PPKI schemes, vehicles request new pseudonyms occasionally to protect user's privacy. In order to achieve location authentication services, Park *et al.* (2011) proposed an RSU based IB mechanism which was an attempt to overcome the trade-off between location privacy and location assurance. They defined a hierarchical road location base identifier system where CA provides the location based vehicle identifier and a corresponding private key for each vehicle. These private keys and identifiers are used to sign and verify messages. However, even though this mechanism can provide message integrity, anonymous authentication, and location authentication, it does not provide any solution for non-repudiation and revocation services.

In another study, Dijiang *et al.* (2011) suggested an IB mechanism named as Pseudonymous Authentication-based Conditional Privacy (PACP). This mechanism consists of two-steps. Firstly, vehicles preloaded a ticket from the main TA, which can act as long-term pseudonym. Secondly, Vehicles utilize these tickets to obtain restricted tokens from RSUs without revealing vehicles identity. Subsequently, vehicles use these tokens to communicate with each other, anonymously. Each RSU produces maps between tickets and its corresponding tokens. In the revocation phase, the TA benefits from RSUs cooperation to recognise the vehicle's identity. Unfortunately, this mechanism does not provide location authentication.

The third type of asymmetric VANET pseudonym authentication is GSB schemes, which makes it possible for a group of vehicles to generate a signature anonymously inside their group. In this method, two messages signed by the same vehicle are not linkable together, so group signature can protect user privacy. In this approach, Group Manager (GM) forms the group and it is responsible to issue or change group's parameter as well as group's public key. In the GSB mechanism, the CA is not involved in the creation of pseudonym or revocation list. Nevertheless, the main disadvantages of the GSB mechanisms is high computational cost of message signing and verifying compared to PPKI mechanisms where it can be even higher when the quantity of revoked members rise up (Armknecht *et al.*, 2007; Lin *et al.*, 2007; Zeng, 2006).

Lin *et al.* (2007) proposed a mechanism named Group Signature and Identity-based Signature (GSIS). This was the very first research that encounters with the security problems and conditional privacy in VANETs via a cryptographic approach. They presented two security mechanisms for V2V and V2R communication. In the former mechanism, group signature is employed to secure the vehicles communications. In the later feature, by using ID-based cryptography a signature scheme is implemented in the RSUs to digitally sign every message released by the

RSUs and guarantee its authenticity, in which the signature overhead may seriously be declined. They assumed that the roadside is densely covered with a number of RSUs; this assumption cannot be applied easily. In addition, they assumed that the CA serves as group manager and is responsible to extract the ID of the signature's originator. This assumption causes revocation overhead on the CA. The Lin *et al.* (2007) approach is the first GSB mechanism on VANET and many researchers followed their work (Lo and Tsai, 2016; Bayat *et al.*, 2015; Ganan *et al.*, 2015; Kumar *et al.*, 2015; Li *et al.*, 2015; Chen *et al.*, 2014). Therefore, comparing a mechanism with Lin et al. (2007) approach formed an evaluation platform which could indicate the level of improvement achieved by any new mechanism.

An RSU-based distributed key management was recommended by Min-Ho *et al.* (2011), where a part of the group key management is devoted to RSUs. An RSU manages vehicles' keys and deals with pseudonym revocation. The CA only controls the group public key and membership changes. Thereby, this mechanism can reduce the communication and computation overhead corresponded to the CA. Nevertheless, this mechanism suffers from insufficient revocation. In order to reduce revocation overhead, Sun *et al.* (2012) established an effectively distributed key management scheme in which the entire domain of VANET is divided into several sub-regions, and each vehicle needs to obtain its group secret key regularly from the regional group manager. This mechanism has the potential to decrease the revocation cost. Here, it should be noted that both of these mechanisms strongly require RSU. In addition, they are capable to provide message integrity, anonymous authentication, non-repudiation, and revocation. However, they do not provide any solution for location authentication and availability and since in these mechanisms verification is time consuming, they are not appropriate for VANET safety application.

For solving message delay problem in GSB mechanism, Malina *et al.* (2013) proposed a batch verification technique, which allow the receivers to verify a group of messages in a glance. This mechanism is capable to provide message integrity, anonymous authentication, non-repudiation, and revocation security services. It has acceptable message delay for safety application. However, if there are some malicious node broadcasting unauthorized message in the network, its performance decreases dramatically and the message delay increase drastically. Therefore, this mechanism is not suitable for securing VANET safety applications. However, with regard to message delay, this approach is one of the best mechanisms among all PPKI, IB, and GSB mechanism and worthy for comparison.

1.3 Problem Statement

One of the main challenges in developing VANET is providing suitable and integrated security mechanism, which has the potential to provide security requirements in terms of security services and computation as well as communication overhead for VANET safety applications. The majority of proposed VANET anonymous authentication mechanisms attempt to provide the main important security services i.e. message integrity, anonymity, non-repudiation, and revocation. However, they suffer from the lack of location authentication and availability as two main security services required for VANET safety applications. In addition, most of the stated VANET security mechanisms are lacking acceptable message delay, which is required by VANET safety critical applications. Moreover, most of the stated VANET security mechanisms are RSUs dependent; however, assuming the road with full RSU coverage is a bit unrealistic.

Therefore, an integrated security mechanism for VANET safety applications with acceptable message delay (less than 20 ms) with or without dependency on RSU is required (Olariu and Weigle, 2009). In this regard, this study is an attempt to overcome some of these security challenges for VANET safety applications. Accordingly, the following research question will be answered:

i. How to achieve acceptable message delay where providing authentication and message integrity for VANET safety applications with and without dependency on RSU?

ii. How to improve message delay in providing anonymity, non-repudiation, and revocation security services for VANET safety applications with and without dependency on RSU?

iii. How to provide location authentication and availability security services with acceptable message delay for VANET safety application with and without dependency on RSU?

iv. How to evaluate and analyse the performance of proposed mechanism in terms of message delay in different VANET scenarios?

1.4 Purpose of Study

The aim of this research is to design and develop suitable and integrated security mechanisms for VANET safety applications with acceptable message delay and high potential in providing message integrity, anonymity, non-repudiation, revocation, availability, and location authentication. The proposed mechanisms in this study are named as RSU-Aided Anonymous Authentication (RAAA) and Group Signature-based Anonymous Authentication (GSAA). The former mechanism is utilized for fully covered RSU areas, while the later mechanism is designed for the areas without RSU coverage. Finally, the performance of proposed mechanisms in terms of average message delay and average message loss ratio versus number of vehicles within communication range and group signature verification delay are evaluated and thoroughly analysed.

1.5 Objectives

The objectives of this research could be defined as:

i. To design and develop a hybrid RSU-aided anonymous authentication mechanism based on Group Signature (GS) and Pseudonym Public Key Infrastructure (PPKI) with location verification for VANET safety applications to improve message delay.

ii. To design and develop a hybrid non RSU-aided anonymous authentication mechanism based on Group Signature (GS) and Pseudonym Public Key Infrastructure (PPKI) with location verification for VANET safety applications to improve message delay.

iii. To evaluate and analyse the performance of the proposed mechanisms in highway and urban scenarios.

1.6 Scope of study

The scopes of this study are as follows:

i. Public key of the CA are preloaded on all vehicles.

ii. Each vehicle has an individual Electronic License Plate (ELP) decided by car producers. Every ELP is connected with a cryptographic long-term key pair and cryptographic short-term certified key pair to act as the pseudonym for message authentication.

iii. Revocation of Hardware Security Module (HSM) is out of the scope of this study.

iv. Security and privacy services below the application layer are not considered.

1.7 Significance of the Study

Attacks against VANET is dangerous for drivers and passengers and even delay on sending safety messages could lead to an accident. This research provides two enhanced anonymous authentication mechanisms for VANET safety applications that covers all security services needed by these applications. Furthermore, by providing location investigation procedure, these mechanisms can guarantee location authentication and availability services, which result in protecting the system against Sybil attack. The performance analysis of this research shows that, it can be a suitable candidate to provide security for VANET safety applications.

1.8 Summary and Organization of the Thesis

This chapter provides a brief introduction on the vehicular ad-hoc network along with defining the objectives of this project, which is followed by the significant of this research.

In Chapter 2, literature review and the research background of VANET applications' security accompanied with the available solutions as proposed by other researchers are summarized. In addition, the communication patterns and current existing standards for VANET are discussed.

Chapter 3 clarifies the methodology used in this research. All the solutions related to VANET security, are covered and discussed throughout this chapter. This includes the simulations' test-bed that is used to evaluate and validate the proposed algorithms.

In Chapter 4, the design and development of an RSU aided anonymous authentication mechanism for VANET safety applications are discussed. Furthermore, this chapter presents the result of the proposed mechanism’s simulation in NS2. In addition, to evaluate the proposed method, the comparisons of the obtained results with similar works are provided.

In Chapter 5, the design and development of an anonymous authentication mechanism for VANET safety application without dependency on RSU are discussed. In addition, the simulation of the proposed mechanism in NS2 is presented and evaluated by comparison with similar mechanisms.

In Chapter 6, these research findings are concluded and some recommendations for future works are presented.

REFERENCES

Abrougui, K. and Boukerche, A. (2013). Efficient group-based authentication protocol for location-based service discovery in intelligent transportation systems. *Security and Communication Networks*. 6 (4), 473-484.

Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H. and Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network. *Journal of Network and Computer Applications*. 37, 380-392.

Armknecht, F., Festag, A., Westhoff, D. and Zeng, K. (2007). Cross-layer Privacy Enhancement and Non-repudiation in Vehicular Communication. *ITG-GI Conference on Communication in Distributed Systems (KiVS).* February. Bern, Switzerland: 1-12.

Baldessari, R., Bodekker, B., Deegener, M., Festag, A., Franz, W., Kellum, C. C., Kosch, T., Kovacs, A., Lenardi, M., Menig, C. and Peichl, T. (2007). Car 2 Car Communication Consortium Manifesto: Overview of the C2C-CC System. *Car to Car Communication Consortium*, 1-94.

Bayat, M., Barmshoory, M., Rahimi, M. and Aref, M. R. (2015). A secure authentication scheme for VANETs with batch verification. *Wireless Networks*. 21 (5), 1733-1743.

Bellare, M., Micciancio, D. and Warinschi, B. (2003). Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In Biham, E. (Ed.) *Advances in Cryptology - EUROCRYPT 2003* (pp. 614-629). Springer Berlin Heidelberg.

Boneh, D. and Boyen, X. (2008). Short Signatures Without Random Oracles and the SDH Assumption in Bilinear Groups. *Journal of Cryptology*. 21 (2), 149-177.

Boneh, D., Boyen, X. and Shacham, H. (2004). Short Group Signatures. In Franklin, M. (Ed.) *Advances in Cryptology - CRYPTO 2004* (pp. 41-55). Springer Berlin Heidelberg.

Bossom, R., Brignolo, R., Ernst, T., Evensen, K., Frotscher, A., Hofs, W., Jaaskelainen, J., Jeftic, Z., Kompfner, P. and Kosch, T. (2009). European ITS Communication Architecture-Overall Framework-Proof of Concept Implementation. *Information Society Technologies and COMeSafety*: 1-165

Bouk, S. H., Kim, G., Ahmed, S. H. and Kim, D. (2015). Hybrid Adaptive Beaconing in Vehicular Ad Hoc Networks: A Survey. *International Journal of Distributed Sensor Networks*, 1-16.

Bresson, E., Stern, J. and Szydlo, M. (2002). Threshold Ring Signatures and Applications to Ad-hoc Groups. *22nd Annual International Cryptology Conference on Advances in Cryptology*. August. Springer-Verlag: 465-480.

Calandriello, G., Papadimitratos, P., Hubaux, J.-P. and Lioy, A. (2007). Efficient and robust pseudonymous authentication in VANET. *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*. September. Montreal, Quebec, Canada: ACM, 19-28.

CAMP (2005). Vehicle safety communications project: task 3 final report: identify intelligent vehicle safety applications enabled by DSRC. *National Highway Traffic Safety Administration, US Department of Transportation, Washington DC*: 1-156.

Chaum, D. and van Heyst, E. (1991). Group Signatures. In Davies, D. W. (Ed.) *Advances in Cryptology - EUROCRYPT '91* (pp. 257-265). Springer Berlin Heidelberg.

Chaurasia, B., Verma, S., Tomar, G. S. and Abraham, A. (2009). Optimizing Pseudonym Updation in Vehicular Ad-Hoc Networks. In Gavrilova, M. L., Kenneth, C. J., Edward, T. and Moreno, D. (Eds.) *Transactions on Computational Science IV* (pp.136-148). Springer Berlin Heidelberg.

Chen, C. Y., Hsu, T. C., Wu, H. T., Chiang, J. Y. and Hsieh, W. S. (2014). Anonymous Authentication and Key-Agreement Schemes in Vehicular Ad-Hoc Networks. *Journal of Internet Technology*. 15 (6), 893-902.

De La Fuente, M. G. and Labiod, H. (2007). Performance analysis of position-based routing approaches in VANETS. *9th IFIP International Conference on Mobile Wireless Communications Networks*. September. cork, ireland: 16-20.

Dijiang, H., Misra, S., Verma, M. and Guoliang, X. (2011). PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for

VANETs. *IEEE Transactions on Intelligent Transportation Systems*. 12 (3), 736-746.

Do, Y., Buchegger, S., Alpcan, T. and Hubaux, J. (2008). Centrality analysis in vehicular ad-hoc networks. *Ecole Polytechnique Federale De Lausanne*. technical report, TPFL/T-Labs: 1-38.

DOT, H. (2004). Vehicle Safety Communications Project Task 3 Final Report, Identify Intelligent Vehicle Safety Applications Enabled by DSRC. *National Highway Traffic Safety Administration, US Department of Transportation*: 1-156.

Dotzer, F. (2006). Privacy issues in vehicular ad hoc networks. In Danezis, G. and Martin, D. (Eds.) *Privacy enhancing technologies* (pp. 197-209). Springer Berlin Heidelberg.

Eckhoff, D., Sommer, C., Gansen, T., German, R. and Dressler, F. (2010). Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping. *IEEE Vehicular Networking Conference (VNC).* December. Jersey City, US: IEEE, 174-181.

Emara, K., Woerndl, W. and Schlichter, J. (2015). On evaluation of location privacy preserving schemes for VANET safety applications. *Computer Communications*. 63, 11-23.

ETSI (2009). Intelligent Transport Systems (ITS): Vehicular Communications; Basic Set of Applications; Definitions. *Technical Report. Version 1.1.1. ETSI TR 102 638*: .1-81.

Fan, C.-I., Hsu, R.-H. and Chen, W.-K. (2012). Privacy protection for vehicular ad hoc networks by using an efficient revocable message authentication scheme. *Security and Communication Networks*. 5 (5), 462-478.

Ferrara, A., Green, M., Hohenberger, S. and Pedersen, M. (2009). Practical Short Signature Batch Verification. In Fischlin M. (Ed.) *Topics in Cryptology – CT-RSA 2009* (pp. 309-324). Springer Berlin Heidelberg.

Festag, A., Noecker, G., Strassberger, M., Lubke, A., Bochow, B., Torrent-Moreno, M., Schnaufer, S., Eigner, R., Catrinescu, C. and Kunisch, J. (2008). NoW – Network on Wheels': Project objectives, technology and achievements. *5th international workshop on intelligent Transportation (WIT)*. March, Humborg, Germany: 211-216

Ganan, C., Munoz, J. L., Esparza, O., Mata-Diaz, J. and Alins, J. (2015). EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. *Pervasive and Mobile Computing*. 21, 75-91.

Hartenstein, H. and Laberteaux, K. (2009). *VANET vehicular applications and inter-networking technologies*: John Wiley and Sons.

Hartenstein, H. and Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*. 46 (6), 164-171.

IEEE-802.11 (2012). IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Redline. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) - Redline*: 1-5229.

IEEE-802.11p (2010). IEEE Draft Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment: Wireless Access in Vehicular Environments. *IEEE Unapproved Draft Std P802.11p /D11.0, Mar 2010*: 1-51.

IEEE-1609.0 (2014). IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture. *IEEE Std 1609.0-2013*: 1-78.

IEEE-1609.2 (2013). IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. *IEEE P1609.2/D17, September 2012*: 1-289.

IEEE-1609.3 (2015). IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services. *IEEE P1609.3v3/D3, July 2015*: 1-160.

IEEE-1609.4 (2014). IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-channel Operation Corrigendum 1: Miscellaneous Corrections. *IEEE P1609.4-2010/Cor1/D4, August 2014*: 1-24.

IEEE-1609.11 (2011). IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS). *IEEE Std 1609.11-2010*: 1-62.

Jinyuan, S., Chi, Z., Yanchao, Z. and Yuguang, F. (2010). An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks. *IEEE Transactions on Parallel and Distributed Systems*. 21 (9), 1227-1239.

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

Jung, C., Sur, C., Park, Y. and Rhee, K.-H. (2009). A Robust Conditional Privacy-Preserving Authentication Protocol in VANET. In Danezis, G. and Martin, D. (Eds.) *Security and Privacy in Mobile Information and Communication Systems* (pp. 35-45). Springer Berlin Heidelberg.

Kamat, P., Baliga, A. and Trappe, W. (2006). An identity-based security framework For VANETs. *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*. September. Los Angeles, CA, USA: ACM, 94-95.

Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K. and Weil, T. (2011). Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys and Tutorials*. 13 (4), 584-616.

Kenney, J. B. (2011). Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proceedings of the IEEE*. 99 (7), 1162-1182.

Kerry, C. F. (2013). Digital Signature Standard (DSS). *National Institute of Standards and Technology*: 1-130.

Klein Wolterink, W. (2013). *Location-based forwarding in vehicular networks*. PhD thesis, University of Twente, Netherlands.

Kroh, R., Kung, A. and Kargl, F. (2006). VANETS security requirements final version. Deliverable. *Secure Vehicular Communication (SEVCOM)*: 1-112.

Kumar, N., Iqbal, R., Misra, S. and Rodrigues, J. (2015). An intelligent approach for building a secure decentralized public key infrastructure in VANET. *Journal of Computer and System Sciences*. 81 (6), 1042-1058.

Leinmuller, T., Buttyan, L., Hubaux, J.-P., Kargl, F., Kroh, R., Papadimitratos, P., Raya, M. and Schoch, E. (2006). Sevecom-secure vehicle communication. *IST Mobile and Wireless Communication Summit*. September, canada: 1-5.

Li, C.-T., Hwang, M.-S. and Chu, Y.-P. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications*. 31 (12), 2803-2814.

Li, J., Lu, H. and Guizani, M. (2015). ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems*. 26 (4), 938-948.

Lin, X. and Lu, R. (2015). *Vehicular Ad Hoc Network Security and Privacy*. John Wiley and Sons.

Lin, X., Sun, X., Ho, P.-H. and Shen, X. (2007). GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*. 56 (6), 3442-3456.

Lo, N. W. and Tsai, J. L. (2016). An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings. *IEEE Transactions on Intelligent Transportation Systems*. 17 (5), 1319-1328.

Ma, X., Chen, X. and Refai, H. H. (2009). Performance and reliability of DSRC vehicular safety communication: a formal analysis. *EURASIP Journal on Wireless Communications and Networking*. 1-13.

Malina, L., Castella-Roca, J., Vives-Guasch, A. and Hajny, J. (2013). Short-Term Linkable Group Signatures with Categorized Batch Verification. In Garcia-Alfaro, J., Cuppens, F., Cuppens-Boulahia, N., Miri, A. and Tawbi, N. (Eds.) *Foundations and Practice of Security* (pp.244-260). Springer Berlin Heidelberg.

Mikki, M., Mansour, Y. M. and Yim, K. (2013). Privacy Preserving Secure Communication Protocol for Vehicular Ad Hoc Networks. *Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (Imis 2013)*. July. Taichung, Taiwan: 188-195.

Min-Ho, P., Gi-Poong, G., Seung-Woo, S. and Han-You, J. (2011). RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications. *IEEE Journal on Selected Areas in Communications*. 29 (3), 644-658.

Noori, H. and Olyaei, B. B. (2013). A novel study on beaconing for VANET-based vehicle to vehicle communication: Probability of beacon delivery in realistic large-scale urban area using 802.11p. *International Conference on Smart Communications in Network Technologies (SaCoNeT)*. June. Paris, France: 1-6.

Olariu, S. and Weigle, M. C. (2009). *Vehicular networks: from theory to practice*. CRC Press.

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Zhendong, M., Kargl, F., Kung, A. and Hubaux, J. P. (2008). Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*. 46 (11), 100-109.

Papadimitratos, P., Buttyan, L., Hubaux, J. P., Kargl, F., Kung, A. and Raya, M. (2007). Architecture for Secure and Private Vehicular Communications. *7th International Conference on ITS Telecommunications (ITST '07)*. June. Sophia Antipolis: 1-6.

Papadimitratos, P., Gligor, V. and Hubaux, J.-P. (2006). Securing Vehicular Communications - Assumptions, Requirements, and Principles. *Workshop on Embedded Security in Cars (ESCAR)*. Berlin, Germany: 5-14.

Park, Y., Sur, C. and Rhee, K.-H. (2011). A Privacy-Preserving Location Assurance Protocol for Location-Aware Services in VANETs. *Wireless Personal Communications*. 61 (4), 779-791.

Petit, J., Schaub, F., Feiri, M. and Kargl, F. (2015). Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Communications Surveys & Tutorials*. 17 (1), 228-255.

Ploessl, K. and Federrath, H. (2008). A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards & Interfaces*. 30 (6), 390-397.

Pradweap, R. and Hansdah, R. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Bagchi, A. and Ray, I. (Eds.) *Information Systems Security* (pp. 314-328). Springer Berlin Heidelberg.

Qin, B., Wu, Q., Domingo-Ferrer, J. and Zhang, L. (2011). Preserving Security and Privacy in Large-Scale VANETs. In Qing, S. Susilo, Wang, W. G. and Liu, D. *Information and Communications Security* (pp. 121-135), Springer Berlin Heidelberg.

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

Rongxing, L., Xiaodong, L., Haojin, Z., Pin-Han, H. and Xuemin, S. (2008). ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. *The 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, US: 1903-1911.

Rongxing, L., Xiaodong, L., Luan, T. H., Xiaohui, L. and Xuemin, S. (2012). Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *IEEE Transactions on Vehicular Technology* 61 (1), 86-96.

Sampigethaya, K., Mingyan, L., Leping, H. and Poovendran, R. (2007). AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE Journal on Selected Areas in Communications*. 25 (8), 1569-1589.

Schoch, E., Kargl, F., Weber, M. and Leinmuller, T. (2008). Communication patterns in VANETs. *IEEE Communications Magazine*. 46 (11), 119-125.

Studer, A., Shi, E., Fan, B. and Perrig, A. (2009). TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs. *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09).* Rome: 1-9.

Sun, Y., Feng, Z., Hu, Q. and Su, J. (2012). An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. *Security and Communication Networks*. 5 (1), 79-86.

Suriyapaibonwattana, K. and Pomavalai, C. (2008). An Effective Safety Alert Broadcast Algorithm for VANET. *International Symposium on Communications and Information Technologies (ISCIT 2008)*, Laos: 247-250.

Tangade, S. S. and Manvi, S. S. (2013). A Survey on Attacks, Security and Trust Management Solutions in VANETs. *Fourth International Conference on Computing, Communications and Networking Technologies (Icccnt)*, Tiruchengode, India: 1-6.

Tsai, C.-H. and Su, P.-C. (2015). Multi-document threshold signcryption scheme. *Security and Communication Networks*. 8 (13), 2244-2256.

Wagan, A. A., Jung, L. T. and Ieee (2014). Security Framework For Low Latency Vanet Applications. *International Conference on Computer and Information Sciences (Iccoins)*, Kuala Lumpur, Malaysia: 1-6.

Wahid, A., Yoo, H. and Kim, D. (2010). Unicast geographic routing protocols for inter-vehicle communications: a survey. *Proceedings of the 5th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*. Bodrum, Turkey, ACM: 17-24.

WHO (2009). Global status report on road safety: time for action. *World Health Organization*: 1-301.

Willke, T. L., Tientrakool, P. and Maxemchuk, N. F. (2009). A survey of inter-vehicle communication protocols and their applications. *IEEE Communications Surveys & Tutorials*. 11 (2), 3-20.

Xiaodong, L., Rongxing, L., Chenxi, Z., Haojin, Z., Pin-Han, H. and Xuemin, S. (2008). Security in vehicular ad hoc networks. *IEEE Communications Magazine*. 46 (4), 88-95.

Xiong, H., Beznosov, K., Qin, Z. and Ripeanu, M. (2010). Efficient and spontaneous privacy-preserving protocol for secure vehicular communication. *IEEE International Conference on Communications (ICC)*. Cape Town, South Africa: 1-6.

Xue, X. and Ding, J. (2012). LPA: a new location-based privacy-preserving authentication protocol in VANET. *Security and Communication Networks*. 5 (1), 69-78.

Yan, G., Lin, J., Rawat, D. B. and Yang, W. (2011). A Geographic Location-Based Security Mechanism for Intelligent Vehicular Networks. In Chen, R. (Ed.) *Intelligent Computing and Information Science* (pp. 693-698). Springer Berlin Heidelberg.

Yan, G., Olariu, S. and Weigle, M. C. (2008). Providing VANET security through active position detection. *Computer Communications*. 31 (12), 2883-2897.

Yong, H., Yu, C., Chi, Z. and Wei, S. (2011). A Distributed Key Management Framework with Cooperative Message Authentication in VANETs. *IEEE Journal on Selected Areas in Communications*. 29 (3), 616-629.

Yuanyuan, P., Jianqing, L., Li, F. and Ben, X. (2011). An Analytical Model for Random Changing Pseudonyms Scheme in VANETs. *International Conference on Network Computing and Information Security (NCIS)*. Guilin, China:141-145.

Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A. and Hassan, A. (2012). Vehicular ad hoc networks (VANETS): status, results, and challenges. *Telecommunication Systems*. 50 (4), 217-241.

Zeng, K. (2006). Pseudonymous PKI for Ubiquitous Computing. In Atzeni, A. S. and Lioy, A. (Eds.) *Public Key Infrastructure* (pp. 207-222). Springer Berlin Heidelberg.