UNIVERSITY OF SOUTH DAKOTA

Scalable Secret Key and Certificate Revocation List Distribution for Hierarchical Vehicular Ad-hoc Networks

by

Kastuv M. Tuladhar

A thesis submitted in partial fulfillment for the
degree of Masters of Science in Computer Science

in the

Department of Computer Science
College of Arts & Sciences

20th November, 2018

M.S. Thesis Acceptance Certificate

The undersigned, members of the Committee appointed to examine the M.S. thesis of Kastuv M. Tuladhar find it satisfactory and recommend that it be accepted.

Date: 20th November, 2018

Approved by:

Dr. Kiho Lim
Committee Chair Signature:_____

Dr. Jose Flores
Committee Member Signature:_____

Dr. Santosh KC
Committee Member Signature:_____

Dr. Ahyoung Lee
Committee Member Signature:_____

Declaration of Authorship

I, declare that this thesis titled, "*Scalable Secret Key and Certificate Revocation List Distribution for Hierarchical Vehicular Ad-hoc Networks*" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: _____

Date: 20th November, 2018

UNIVERSITY OF SOUTH DAKOTA

Abstract

Department of Computer Science
College of Arts & Sciences

Master of Science

by Kastuv M. Tuladhar

Vehicular ad-hoc networks (VANETs) have become an emerging technology that can fulfill the demand of evolving connected vehicle and growing need for Intelligent Transportation System (ITS). Certificates are used to secure vehicular communication but the certificates of vehicles need to be revoked if any vehicles are found as misbehaving nodes. In VANETs, certificate revocation list (CRL) must be quickly distributed to all vehicular nodes to prevent from undesirable communication with the malicious nodes. However, due to growing number of the certificates, the size of CRL continuously increases and this makes it difficult to manage and distribute the CRL in the vehicular networks. In this paper, an efficient and scalable scheme to distribute certificate revocation list is presented in the hierarchical architecture of VANETs. The analysis shows that proposed scheme can distribute certificate revocation list promptly throughout the networks while maintaining low CRL size.

On the other hands, there is a huge concern to safeguard increasing applications security in Vehicular Ad hoc Networks (VANETs). A group signature is one of the popular authentication approaches for VANETs which can be implemented to secure the VANET communication. However, securely distributing group keys to fast-moving vehicular nodes is still a challenging problem. In this paper, an efficient key management protocol for group signature based authentication, where a group is extended to a domain with multiple road side units. The experiment result shows that the proposed key distribution scheme is a scalable, efficient and provides a secure way to deliver group keys to vehicular nodes ensuring security features and also efficiently manages the vehicle revocation mechanism using two-bloom filter.

Approved by:
Dr. Kiho Lim
Committee Chair/Advisor Signature:_____

Acknowledgements

Firstly, I want to express deepest thanks to my advisor Dr. Kiho Lim for mentoring and guiding me throughout to complete my research. I will remember him for what I have achieved within the short interval under his guidance. I would like to extend my gratitude to all the committee members Dr. Jose Flores, Dr. Santosh KC, Dr. Ahyoung Lee, and Dr. Goodman Douglas.

Many thanks to my roommate Surya Bhandari for managing my daily life and inspiring me to complete the thesis on time. I will remember–Subrat and Sabi, for providing me a peaceful environment to work. I am grateful to Samana Paudel and Samiksha Giri for offering me many 'tea break' sessions during my dissertation preparation. I will also miss Luis Villamizar quoting me everytime *"you got this man, you can do it !"*.

Lastly, I must thank my family members for their endless support and love. I remember my elder sister Bhawana for constantly reminding me to complete the research work on time. My sister, Kamana and Sadhana has provided me motivational support during the tough time and sending a good wishes from back home.

Of course, I want to dedicate this thesis to my father and my beloved mother. Words are not enough to express my gratitude towards my parents but I promise that I will always try to make you proud.

Contents

List of Figures

List of Tables

Abbreviations

AC	**A**ccess **C**ategory
CCH	**C**ontrol **CH**annel
CRL	**C**ertificate **R**evocation **L**ist
CRLVE	**C**ertificate **R**evocation **L**ist **V**erification **E**ntity
CSMA/CA	**C**arrier **S**ense **M**ultiple **A**ccess/**C**ollision Avoidance
CWmax	**C**ontention **W**indow **M**aximum **V**alue
CWmin	**C**ontention **W**indow **M**inimum **V**alue
DSRC	**D**edicated **S**hort **R**ange **C**ommunication
EDCA	**E**nhanced **D**istributed **C**hannel **A**ccess
ECDSA	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm
MAC	**M**edium **A**ccess **C**ontrol
OBU	**O**n **B**oard **U**nit
PKI	**P**ublic **K**ey **I**nfrastructure
RSU	**R**oad **S**ide **U**nit
SCH	**S**ervice **CH**annel
TA	**T**rusted **A**uthority
V2I	**V**ehicle **to** **I**nfrastructure
V2V	**V**ehicle **to** **V**ehicle
VANETs	**V**ehicular **A**d-hoc **NET**works
WAVE	**W**ireless **A**ccess in **V**ehicular **E**nvironment
WSM	**W**AVE **S**hort **M**essage
WSMP	**W**AVE **S**hort **M**essage **P**rotocol

Chapter 1

Introduction

1.1 Motivation

The main motive of this research is to enhance the security of the Vehicular Networks. Vehicular technology has a growing demand as its taking its shape as smart, self-driving and autonomous vehicles. All the VANETs applications (like traffic congestion, weather report, collision avoidance, road safety, value added service etc) of this emerging technologies requires a secure communication to exchange the data. Prior to any communication and exchange the data, it is important to authenticate or to identify the target vehicular nodes. Authentication protocol allows the nodes (vehicles/infrastructures) to exchange the secret key to communicate securely in a wireless medium. However, the early proposed authentication schemes were not scalable and efficient. The vehicular nodes has to frequently initiate for the new secret key to establish the session after the certain coverage or in other words vehicle has to initiate for the authentication with every RSU along its route. Further, it is a important yet a challenge to exchange the secret key to the target vehicle through the open wireless network where any nodes can intercept the open and unencrypted packets. This research paper has attempted to provide secure and efficient key distribution mechanism for the successful authentication in the VANETs. By utilizing the hierarchical VANETs structure, the authentication scheme can utilized in the group of infrastructures which can re-utilize the same secret key for large coverage area and longer duration –making the scheme scalable.

To reduce the misbehaving activities in VANETs, after detecting the malicious nodes or misbehaving activities, it can be prohibited to access the network. One of the approach is to distribute the list of revoked certificates of malicious nodes to the entire nodes of VANETs is using Certificate Revocation List (CRL). However, due to the growing size of CRL, it requires the excessive bandwidth and storage size. To solve this issue, in this

research paper, the same hierarchical VANETs structure will help to group the certain number of vehicles. Thus, the vehicle only requires to store the CRL within the given group of infrastructures. Further, utilizing the dual bloom filter, the CRL size can be further compressed. The hierarchical VANETs also helps to distribute the CRL for the global synchronization.

1.2 Contribution

This research paper can be sub-divided into two parts: CRL distribution and the secure key distribution.

• **CRL Distribution**
The CRL size in current scenario is not suitable for distribution because of its heavy size. To reduce the CRL size and make it suitable for distribution, the idea od implementing the hierarchical architecture is implemented that will subdivide the CRL to the small section. Further, employing the two bloom filter makes it free from the false positive and further compress the CRL into the suitable range. The synchronization of the local and the global CRL prevent the malicious node from entering into the domain.

• **Secure Key Distribution**
The frequent key establishment in the VANETs has is not scalable use. In other words, a sufficient time of key establishment can be saved using the group key that can be employed it the larger domain. This paper employes the group key for the vehicle that can be used for larger coverage of the domain. To securely distribute the group key, Diffie-Hellman protocol has been applied. The approach can be used in multiple areas like airplanes, trains, autonomous moving/flying objects to save the key establishment time.

1.3 Document Organization

The dissertation is organized in the five chapters and an appendix. Chapter 2 provides the brief introduction of the Vehicular Ad-hoc Networks (VANETs), IEEE Standards, layered based standards (physical, MAC, network and application), and security attack and requirements of the VANETs. Chapter 3 introduces about the certificate revocation list and its challenges in detail. It also contains the proposed model, synchronization scheme and utilization of the dual bloom filter. The analytical evaluation of the approach is also provided in the same chapter. Chapter 4 discusses the authentication scheme of the VANETs and its challenges in detail. It also contains the key idea of our protocol

and its evaluation and analysis. Chapter 5 contains the list of future work that will be performed to authenticate the vehicle even in the infrastructure-less environment. It has discusses the ADAS sensors and how the sensor data can be utilized to perform the authentication of the vehicles.

Chapter 2

Vehicular Ad-hoc Networks

2.1 Introduction

Vehicular Ad-hoc Networks (VANETs) is a sub-class of Mobile Ad-hoc Networks (MANETs) with unique features, such as fast-moving vehicular nodes, dynamically changing topology and short interaction time between vehicular nodes. In VANET vehicles can communicate with each other called as inter-vehicle communication or Vehicle-to-Vehicle communications (V2V) or vehicles can connect to infrastructure that is road side units(RSU) is called as vehicle-to-roadside(V2R) or Vehicle to Infrastructure communication (V2I) [2]. The RSUs are located along the road to provide extensive coverage of the services to vehicular nodes. Vehicular nodes are equipped with on-board units (OBU) which is a communication and computation device that stores, computes and transmits the information collected from the roads. Besides providing the security services, VANETs also support various applications related to safety messages, traffic management, and infotainment services [3]. Numerous car manufacturers and telecommunication industries are teaming up to equip car with the advanced technologies which will allow passengers and drivers to communicate with each other also with the roadside units locating in the critical sections of the road such as every traffic light, intersections/stop signs [1].

2.1.1 IEEE Standards

IEEE 802.11 is a data sheet for physical layer (PHY) and media access control (MAC) for the implementation of WLAN in 2.4,3.6, 5 and 60 GHz frequency bands [4]. The IEEE Vehicular Technology Society has been developing a series of trial-use standards for Wireless Access in Vehicular Environments (WAVE). The communication protocol stack for generalized vehicular environment is shown in Figure 2.2 [5].

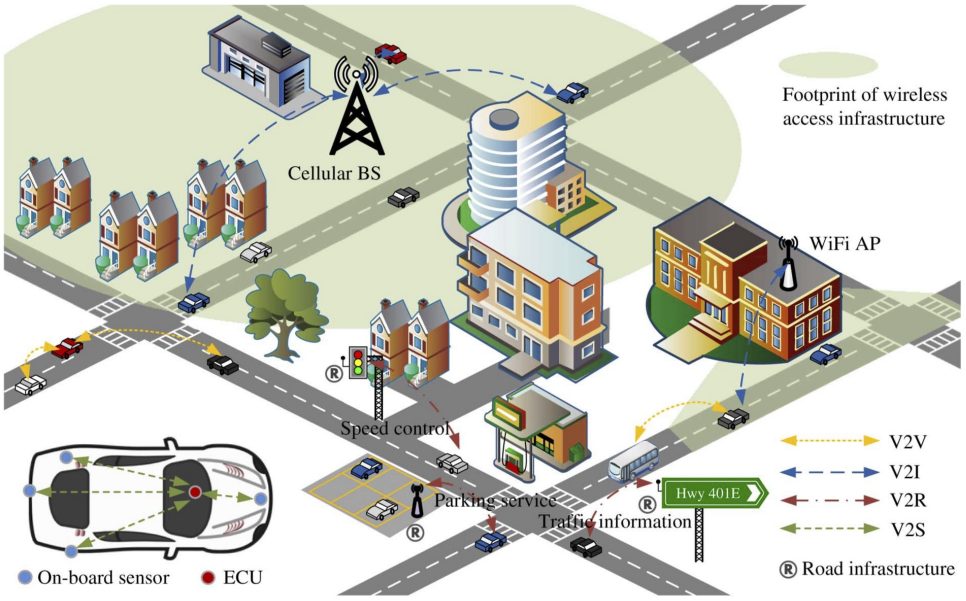

FIGURE 2.1: Typical Vehicular Ad Hoc Networks (VANETs) architecture [1]

A Dedicated Short-Range Communications (DSRC) provides the one-way or two-way short-range to medium-range wireless communication channels for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) which is covered in IEEE Standard 802.11p [6, 7]. IEEE 802.11p is one of the recent approved amendments to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It appended some enhancements to the latest version of 802.11 that required to support applications of Intelligent Transportation Systems (ITS). IEEE 802.11p Standard has sub-divided into four parts: application layer (IEEE 1609.1), security services (IEEE 1609.2), multichannel operation (IEEE 1609.4), and network services (IEEE 1609.3). The main aim of IEEE 1609.2 (security services) is to produce single security standard in the vehicular communication that can deal with confidentiality, integrity, authenticity, and authorization.

2.1.2 Physical Layer Standard

There are 9 channels in IEEE 802.11p each has a frequency band as described in Figure 2.3 [8]. Two channels CH172-5.860 GHz and CH184-5.920 GHz are safety dedicated channels. CH172 is dedicated to provide security solutions while CH184 is reserved for congestion control on the other channels. Channel CH178-5.890GHz is dedicated control channel responsible to control the transmission broadcast and link establishment. The remaining channels are allocated for bi-directional communication. The pair of (CH174, CH176) and (CH180, CH182) can be combined to form single 20 MHz channel CH 175

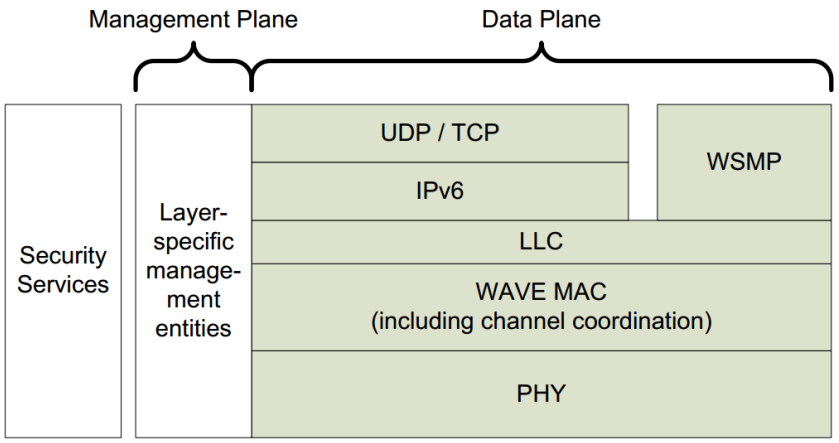

FIGURE 2.2: WAVE reference model

and 181 respectively. There is also 5 MHz band placed as a guard band (GB) in the beginning at 5.85 GHz.

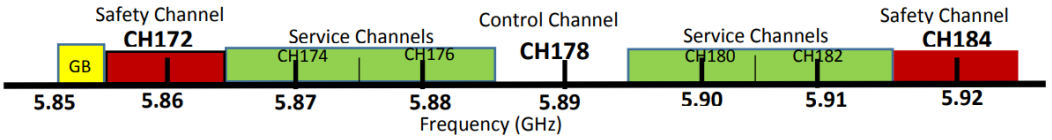

FIGURE 2.3: IEEE 802.11p Channel Frequency Band

2.1.3 Medium Access Control (MAC) layer

The primary reason for packet drop are packet collision and poor radio receptions that prevent nodes to receive the data sent over wireless medium. A carrier sense multiple access and collision avoidance (CSMA/CA) approach is utilized in DSRC [9] in order to allow the fair access of the medium. The each node sense the medium before sending the data. If it's idle, node wait for fixed arbitration inter-frame space (AIFS) time plus a random time between and minimum contention window (CW_{min}) value and sends the data. The prioritization in DSRC uses Enhanced Distributed Channel Access (EDCA) that is based on IEEE 802.11e. There are four access categories (AC) defined under EDCA. The control channel and service channel have different parameters for different ACs. Table 2.1 shows the EDCA parameters for the control channel and the wait time (t_w) is calculated using values $aCW_{min} = 15$ and $aCW_{max} = 1023$ [10].

Control Channel					
ACI	AC	CW_{min}	CW_{max}	AIFS	t_w
0	Background	aCW_{min}	aCW_{max}	9	$264\mu s$
1	Best Effort	$\frac{aCW_{min}+1}{2}$-1	aCW_{min}	6	$152\mu s$
2	Video	$\frac{aCW_{min}+1}{4}$-1	$\frac{aCW_{min}+1}{2}$	3	$72\mu s$
3	Voice	$\frac{aCW_{min}+1}{4}$-1	$\frac{aCW_{min}+1}{2}$	2	$56\mu s$

TABLE 2.1: EDCA parameters for DSRC

2.1.4 Network Layer Standards

There are two different network layer protocols supported by WAVE: IPv6 and WAVE Short Message Protocol (WSMP) specified in IEEE1609.2 [5]. A WAVE Short Message (WSM) is a message format for WSMP that may be sent on either control or service channel. WSMP acts as a transport layer protocol replaying TCP and UDP. The control channel do not allow IPv6 traffic whereas WSMP is allowed on both control and service channel. Similarly, WSMP does not use IP address or MAC address to identify the source or destination, thus, it helps to increase the user anonymity. The WSM header is just 22 bytes in length whereas IPv6 contains 40 bytes and requires 8 more bytes for UDP header. IEEE1609.2 [5] suggests certificate revocation list to use WSM.

2.1.5 Application Layer: Security Services

IEEE 1609.2 [5] has categorized WAVE security services into two domain i.e. WAVE Internal security services and WAVE higher layer security services. WAVE Internal Services are -Secure data service (SDS): it deals with transforming unsecured protocol data units (PDUs) into secured protocol data units ($SPDUs$) to be transferred between entities. An entity that uses the secure data service is referred to as a secure data exchange entity ($SDEE$). Higher layer WAVE security deals with -Certificate revocation list (CRL) verification entity ($CRLVE$) that validates incoming CRLs and passes the related revocation information to the security services management entity ($SSME$) for storage, and -peer-to-peer certificate distribution ($P2PCD$) entity that enables the peer-to-peer certificate distribution.

2.2 Security Attacks

VANETs is an open wireless medium, thus, there are chances of many possible attacks. The attacks can be categorized in multiple ways. On the basis of the *goals:* attackers can

create or avoid congestion, cause accidents, track vehicles or perform DOS attacks. On the basis of *actions:* attackers can insert bogus warning (like congestions), misrepresent the location of the accident, suppress the message or perform jamming. On the basis of *execution*, attackers can execute single or multiple Sybil attacks, or collude multiple or independently.

Attackers in VANETs can be *insider or outsider*. The insiders are the valid user on the VANETs and the outsiders are intruder those who have limited attack options. There are also *malicious or rational attackers*. Malicious attackers does not have personal benefits but intends to harm the other users whereas rational attackers seeks the personal benefits and are more predictable in attacking. Attackers can also leads to *active or passive* attacks. Active attackers generates harmful messages and participates in the network while passive attackers eavesdrop or track the users.

One of the popular categorizations of the attacks in VANETs has been mentioned in [11, 12] on the basis of confidentiality, integrity, authentication and availability.

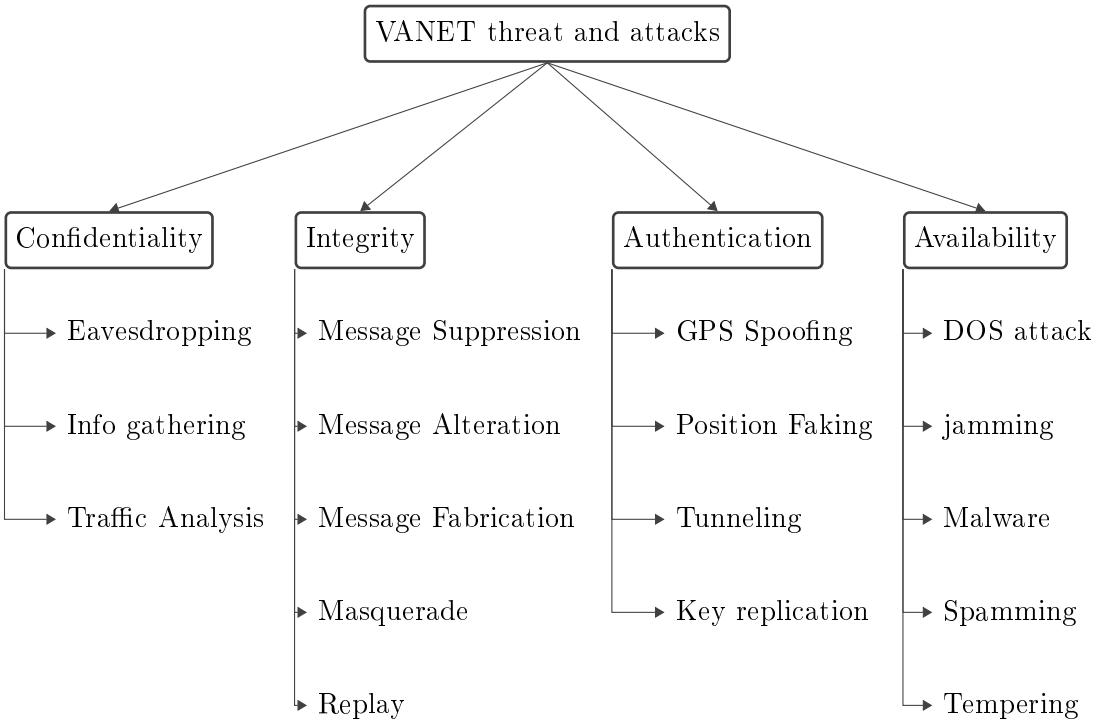

FIGURE 2.4: Classification of VANETs Attacks

2.2.1 Network Attacks

In this research,, we will concern mostly in those attacks that will effect the network and communication medium between the infrastructures and the vehicular nodes.

2.2.1.1 Denial of service (DOS) Attack

The attacker in this attack tries to jam the channel of the communication medium so that other nodes will have problem in accessing the network. The purpose of this attack is to prevent the authentic user to access the medium. The attacker can either attacks the vehicular nodes or the network infrastructures such as RSU (access points) or both. If the attacker launches the DOS attacks from the multiple locations with different time slots then it is called *Distributed DOS (D-DOS) attack*. A typical DOS attack scenario is shown in Figure 2.5 where the attacker is jamming the network such that other will not be able to access the medium, such attacks could lead to accident.

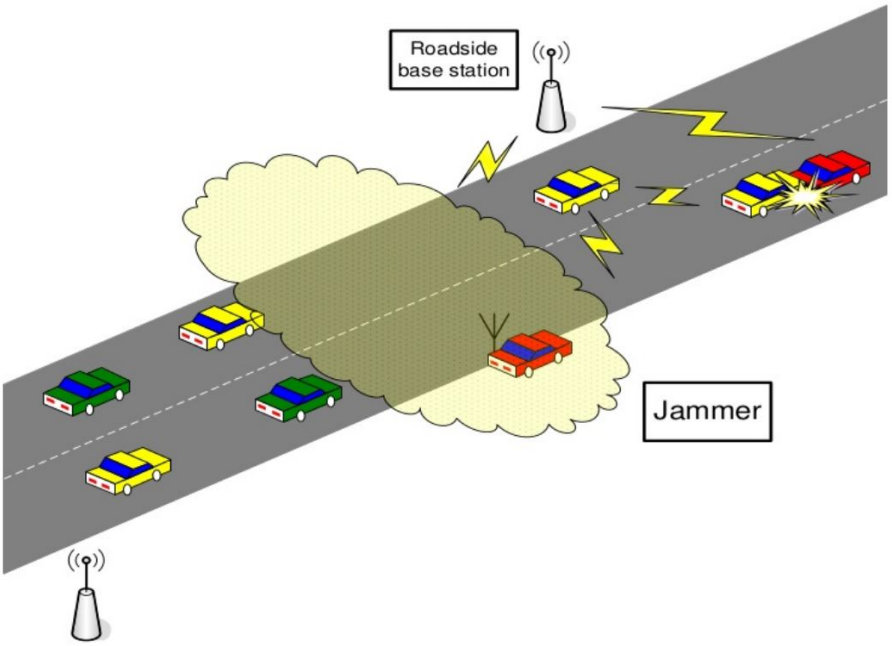

FIGURE 2.5: DOS attack scenario

2.2.1.2 Sybil Attack

The attacker in this attack creates the multiple duplicate vehicles with the same identity on the road. The purpose of this attack is to manipulate other vehicles on the road for the benefit of the attacker. Attacker may use such attack to redirect the or change the route of the other vehicles, a typical Sybil attack scenario [13] is shown in the Figure 2.6 where the malicious vehicle is providing the fake road congestion alert to the RSU which is broadcasting the alert through out the it's coverage area.

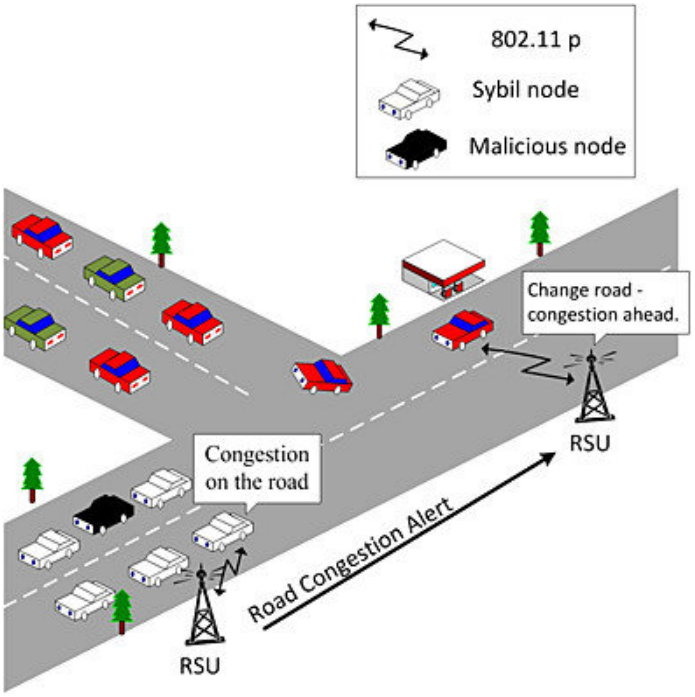

FIGURE 2.6: Sybil attack scenario

2.2.1.3 Node Impersonation

The attacker in this attack changes the identity in order to prevent from detecting. Attacker can use such attack when they are responsible for some attack and it hides the identity before being detected. The another scenario of node impersonation is also a message tempering attack. As in the Figure 2.7, vehicle A sends the actual location of the accident (Location X) to the vehicle B, however, for some reason vehicle B decides to change the location (Location Y) of the accident and forwards to the RSU. The RSU then sends the ambulance to the wrong location.

2.2.1.4 Man in the Middle Attack (MiM)

The attacker in this attack listens to the communication established between the vehicles and pretends to be one of them and replies to another. The vehicle can injects false information or find out the crucial information using this attack [14]. One of the other possibility is the attacker can perform *Replay attack* that sends out same message the other vehicle replies during the conversation or it can drop the crucial forwarding packets that carrying the vital information about accidents. As in the Figure 2.8, the vehicle B is pretending to be A and C and communicating back and forth. This form of attack can be more vulnerable that *eavesdropping attack* as it can directly communicate with the nodes instead of listening to it.

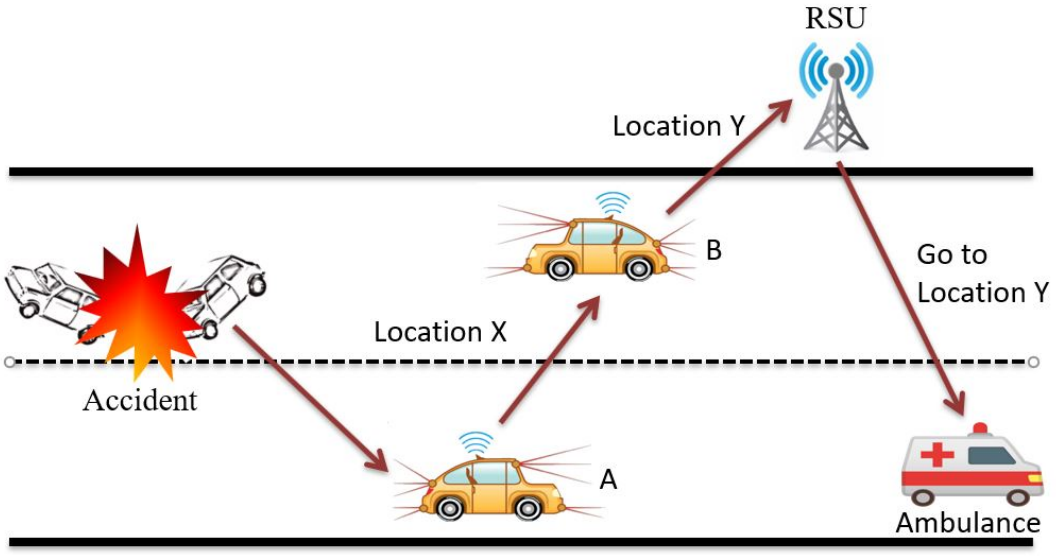

FIGURE 2.7: Node Impersonation attack scenario

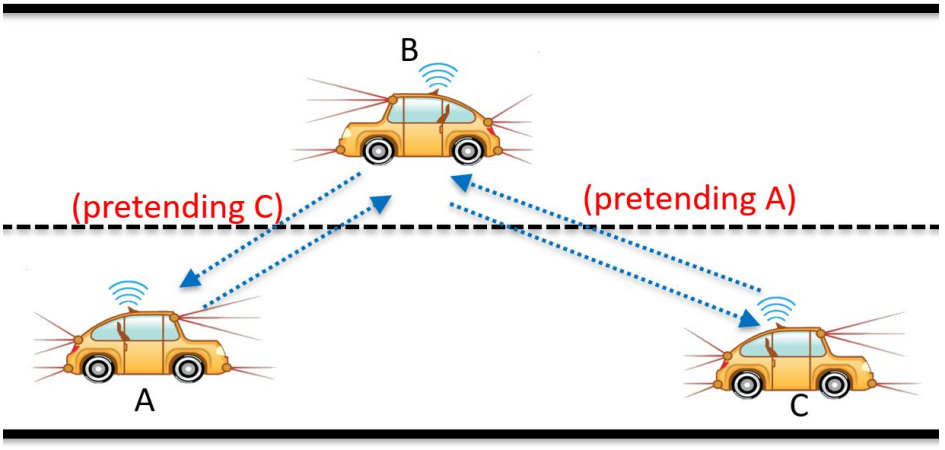

FIGURE 2.8: MiM attack scenario

2.2.1.5 Other attacks

There are still a various types of attacks in VANETs [15] that has are worth mentioning such as *Malware/Spam:* attacker sends Spam or Malware to gain the access of the vehicle or to consume transmission latency and network bandwidth, *Brute-force attack:* attacker tries to crack the authentication key or find personal information using hit-and-trial methods, *Black hole attack:* attacker declares itself as a shortest path for the routes and consumes all the data from the vehicular nodes that can be dropped or modified. Besides there are also attacks on the hardware of the vehicles like tampering the vehicular device, cheating the GPS information, damaging the sensors or gaining un-authorized access to the infrastructure.

2.3 Security requirements in VANETs

VANET applications contains the exchange of the messages such as emergency, traffic conditions, road accidents that requires the data communication between the nodes. The message content can have impact on the drivers' actions to the vehicle. Malicious node can alter the message content by various possible attacks such as spreading bogus information, Denial of service (DOS) attack, replay, traffic jams, hardware tampering etc [16]. Following security requirements has to be fulfilled in VANETs in order to overcome above mentioned challenges [17]:

2.3.1 Authentication

Authentication is the one of the main requirement of all the communication. In VANETs, the sender and receiver are required to know at-least some of the information regarding the identification, location and other properties. All the messages and users are required to authenticate for the secure communication. Authentication controls the level of authorization for the vehicular nodes. A proper authentication of vehicle can control many types of attacks such as: Sybil attacks can be prevented if each vehicles are properly authenticated, if vehicle want to avoid congestion and pretends to be number of other vehicles then the powerful authentication mechanism can pretend, if not then be able to detect such illegal acts. There are several authentication approaches, Kargl et al. [18] proposed for ID authentication that can identify the transmitter message in a unique manner. Similarly, property authentication can help to determine what kind of entity is communicating (a car/ an RSU etc) and location authentication helps to find the node position when location application is required.

2.3.2 Integrity

Integrity assures that the message from the sender to the receiver is intact and unaltered between the transmission phases. The receiver will only be able to justify the actual identity of sender [19]. Integrity can protect from the unauthorized access and alteration of the data. Acceptance of the corrupted message violates the integrity. Integrity can be achieved if the system can prevent the attackers from altering the message since the message must be trusted. The attacker can be avoided by through the proper authentication. A proper security protocol can ensures that the data are not compromised if the signature is appended in the message in a secure way.

2.3.3 Confidentiality

It refers to the confidentiality of the message between vehicle of infrastructure that any entities between them should not be able to understand. It can be achieved using the proper encryption mechanism [20, 21] that can protect user profile and, information and contents. However, message confidentiality depends upon the applications of the VANETs, for example, safety related messages should not be confidential however a toll payment message by vehicle must be confidential. Such confidentiality in the message can be achieved using public key or symmetric key in the message. Similarly, session key can be applied in the V2I communication where all the messages during the session can be encrypted using session key and they are also attached to the Message Authentication Code (MAC) for message authentication [22].

2.3.4 Non-repudiation

Non-repudiation refers to validating undeniable evidence about the claimed event or action in order to resolve the disputes to prove the incident has occurred or not occurred. It allows to generate the solid proof for the system that can identify the attacker who cannot deny the performed actions [23]. To support this approach, can information (trip, speed, route, violation etc) will be stored in the Tamper Proof Device (TPD) that can only retrieved by authorized officials [20, 21].

2.3.5 Availability

VANETs should be operating smoothly even in the presence of faults or malicious conditions. It requires system to be fault tolerant and resilient to attacks along with survival protocols that resume the operation even after removing the faulty nodes [24]. It also deals with the robust communication protocol that can reach all the vehicular nodes even during the critical weather condition or during the natural disasters like hurricane, icy-condition, heavy snow etc.

2.3.6 Access Control

Access control determines the rights and privilege level for the vehicle for certain applications or access to the network, message , encryptions etc. For example, the sensitive message from the law enforcing authority must not be heard by other nodes in the network. Such access to specific services provided by the infrastructure to other nodes

should be determined by the local policies. Moustafa et al. [25] has provided a model that requires service tickets as the credential for various services.

2.4 Employing VANET Security

After taking into account about the security requirements of VANETs and the fact that different entities and data are at stake, the security can be achieved by employing the digital signatures. a symmetric cryptography using shared secret keys.

2.4.1 Public Key Infrastructure (PKI)

Digital signatures can be asymmetric cryptography where each entity has a public/private key pair. Each entity can use the private key to generate the unique digital signal that can be used to sign the outgoing message. The main components of a public key infrastructure are the users, the certificates, and the certificate authority (CA). Private keys are used to sign the message cryptographically while public keys are used to authenticate the message. PKI based keys are utilized in VANETs for the node authentication, further, the signed message also provides the message integrity. Any change in the message will cause signature verification to fail. PKI signatures has a certain validity lifetime period [26]. The encryption used in VANETs are specified by IEEE 1609.2 standard to be elliptic curve encryption: Elliptic Curve Digital Signature Algorithm (ECDSA) which are generally 224-bit and 256-bit.

2.4.2 Certificates

Certificates binds the public key to an entity that serves as a proof that the public key belongs to that user. The Certificate Authority (CA) provides the certificate upon the request from the user. The CA is a trusted source thus the user must trust it in order to validate the certificate. To authenticate the node, the identity of the user must specified, however, the user does not want their true identity to be known in the surrounding. Thus, there is a trade-off in authenticity and the confidentiality of the user in VANETs. Several researchers [27, 28] have proposed the solution using the pseudonym certificates –a short-lifetime certificate that do not contain the true identity informations, however during disputes the CA can track back to its true identity. The long term certificates and the pseudonyms can be linked using the vehicle chassis number, plate number, drivers license etc. Typically, multiple pseudonyms are assigned to the users to increase the user anonymity. For all the user that misbehave/attacks or perform the illegal activities, their

certificates will be revoked and the list of such nodes will be notified to entire VANETs using certificate revocation list (CRL).

IEEE 1609.2 has specified to use the non-anonymous authentication with elliptic curve digital signature algorithms (ECDSA) along with CRL. The certificate issued by CA also has an identification number calculated by using SHA-256 hash of the certificate. The size of the certificate identification number can be 64 bits up to 80 bits. The certificate includes the 256-bits ECDSA[1], 32 bytes of public key and 28 bytes private key associated to the user. Every pseudonyms has to store the certificate and the private key associated with it.

[1] 224-bits ECDSA signature for OBU and 256-bits ECDSA for TA

Chapter 3

Certificate Revocation List

3.1 Introduction

Certificates are issued to vehicle for the security of the communication as it can be used in an authentication of the node or used while sending/receiving message. However, if the vehicle performs the illegitimate behavior/act as per Misbehavior Detection Schemes (MDS) [29, 30] then the certificates of such misbehaving vehicle has to be revoked as soon as possible before it starts to communicate or victimize the other nodes.

Several approaches have been studied for the certificate revocation: Online certificate status protocols (OCSP) [31] and Certificate Revocation Lists (CRLs). OCSP contains the real-time interactive certificate status server where the updated information of the revoked certificates is stored. During the communication, the nodes send the query packet about the status of the certificate to the server and the server replies a response about the revocation status of the given certificate. However, OCSP is not suitable for VANETs due to 1) latency/delay: the certificate query has to reach the certificate status server for every communication that will add up latency/delay which is critical in delay sensitive and dynamic topology of the VANETs; 2) infrastructure availability: it is not applicable in the rural area where there are no sufficient infrastructure; 3) scalability: OCSP approach is not scalable as the network will be flooded with the status query and its response, also the size of the vehicular nodes will increase with time. On the other hand, CRL [26, 32] consists the list of the certificates that are revoked by the TA. The CRL is provided to the vehicles, thus, vehicles can lookup and compare locally to find out the status of the certificate which is the reason it is preferred in VANETs. However, there are still some challenges for management and distribution arisen due to the CRL size and scalability is not considered on those schemes.

When certificates are issued, TA also assigns the expiration date/time. When it expires, certificates are no longer valid to be used for authentication. In order to protect the user privacy and anonymity, certificates can be updated frequently [33]. The frequency of the certificate update has been studied by Haas et al. [32] that the vehicle will need approximately 25,000 certificates to be renewed in five years. If the size of each certificate is approximately 100 Bytes, the storage size of the certificates for one vehicle would be 2.5 MBytes. If a malicious vehicle is detected, all the certificates of the malicious node must be revoked. In addition, the certificate lists of the stolen vehicles also should be added to CRL as it could be used for malicious purpose. For instance, a total of 4.3 million vehicles has been stolen from 2011 to 2016 [34]. Even with only one certificate per vehicle is considered, the total size of the certificates to be revoked would be 431 MBytes. Such a high number of revoked certificates could result in large CRL size that must be propagated throughout the whole network. Managing large CRL is one of the challenging issues in VANETs because it causes the excessive consumption of the network resources and computational overhead.

In an effort to reduce the size of the CRL, several CRL compression approaches have been proposed using a bloom filter [35, 36]. Bloom filter [37] is a probabilistic data structure which is used to compress the data by comparing the element in its data set due to this feature it can also be used to reduce message overhead [38]. Using bloom filter, certificates ID are hashed with the hash functions and stored in the fixed size bit vector to form Compressed Certificate Revocation List (C^2RL). The node can hash the certificate and compare with the bit vector of the bloom filter to validate the certificate. However, the hash of the multiple certificates can set the same bit vector multiple times which arises the problem of a false match whose rate is the false positive rate (FPR). As a result, CRL could point out the valid certificate as a revoked certificate.

In order to address management and distribution of certificate revocation list, Hass et al. [32] proposed an epidemic manner to distribute CRL (through car-to-car), Ying et al. [39] proposed peer-to-peer CRL distribution, and Rabieh et al. [40] proposed distributing CRL through broadcast. However, these approaches have not considered the impact of distributing CRL size in the large area with many vehicles. For example, considering a large number of vehicle in US, generally vehicles in California do not need to store the CRL of the vehicles in New York. Thus, we propose an efficient and scalable certificate revocation scheme to address the issues mentioned above. Using the proposed scheme, an appropriate revocation list is delivered to each region such that the size can be decreased dramatically and the up-to-date CRL can be distributed in a timely manner through hierarchical architecture of VANETs.

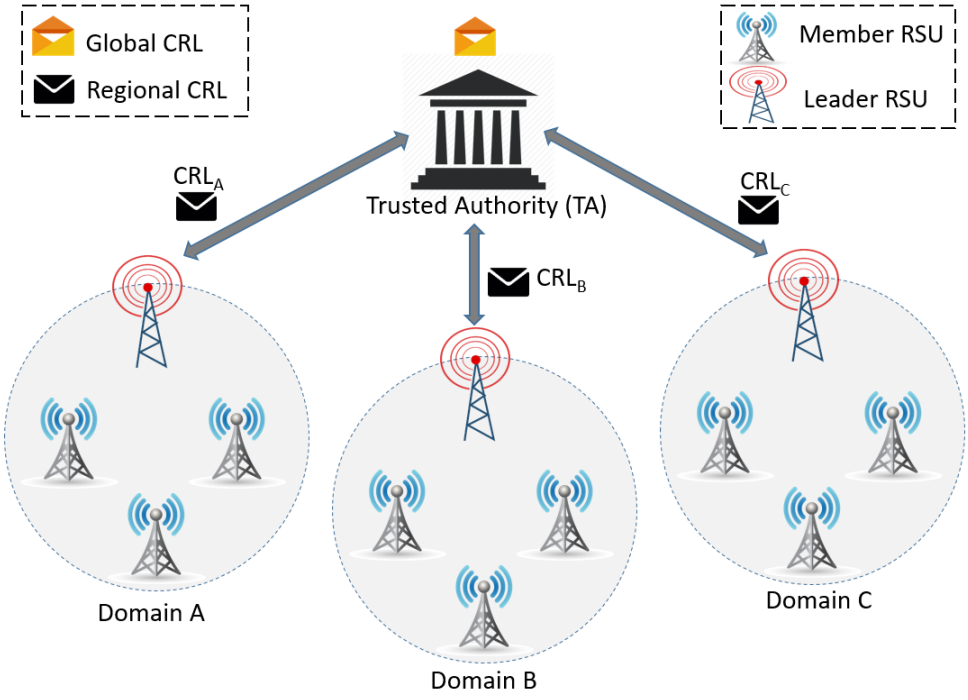

FIGURE 3.1: CRL distribution in hierarchical VANETs

3.2 System Model

We assume that the following key components are present in the network: a Trusted Authority, Road Side Units, and Vehicle Nodes that are hierarchically classified [41, 42]. The overview of the system model is illustrated in Fig. 3.1.

- **Trusted Authority (TA):** Vehicles are registered and the certificates are issued by the trusted authority. TA are securely connected with RoadSide Units(RSUs). TA generates and maintains the global CRL. TA further prepares the regional CRLs and distributes them to the appropriate regions. TA also provides a response to the revocation status query from any regions.

- **Road Side Unit (RSU) and Domain:** RSUs are the infrastructures deployed along the road-side that communicates with the vehicles and the TA. A group of RSUs forms a domain. The number of RSUs in a domain can be considered upon the requirement of the geography, resource capacity, and demography. A domain size is defined as the desired number of vehicles that can be accommodated by the number of RSUs within a geographic region. The CRL valid for a domain is called regional CRL.

- **Leader-Road Side Units (L-RSU) & Member-Road Side Units (M-RSU):** RSUs are further classified into leader RSUs (L-RSU) and member RSUs (M-RSU). The L-RSU is the leader of a regional domain. The L-RSU coordinate with the TA manages

M-RSUs & the vehicles around its vicinity. The L-RSU is responsible to manage and distribute regional CRL inside the domain. It can also send the revocation status query to authenticate the certificate of the vehicle.

- **Vehicular Nodes:** Vehicular nodes are equipped with the on-board unit (OBU) that serves the purpose of computation, communication, location services and interface for interaction. Vehicles communicate with each other or with RSUs through a wireless protocol which is defined under the IEEE Standard 1609.2-standard for the wireless access in the vehicular environment (WAVE) [5]. Vehicles stores the certificates and CRL in the tampered proof device (TPD) [43] for the security purpose. Prior to communication, a vehicle confirms the authenticity of the communicating node by comparing the certificate in its CRL list.

3.3 Proposed Scheme

Haas et al. [32] has discussed the requirement of the CRL and focused on the distribution aspects using epidemic manner. Rigazzi et al. [35] proposed to revoke the certificate in a compressed form of CRL by using a bloom filter and demonstrated CRL distribution in urban and rural scenarios. The scheme presented by Wang et al. [44] utilized the TPD to revoke the malicious vehicle by deleting the identity of the node from its storage. Although the previous revocation schemes are widely used in VANETs, distributing certification revocation list of a large number of vehicles are not well addressed. In order to utilize the certificate revocation list in the real VANET environments, it is important to consider the growing size of the CRL. Papadimitratos et al. [36] introduced a mechanism to reduce the size of the revocation list by dividing the standard CRL into small-scale CRL, but it does not keep the track of the malicious nodes traveling between the regions and has not provided a scalable approach to be applied in VANETs. Thus, in order to address exceedingly large CRL size and scalability of CRL distribution, we propose a scheme in a hierarchical architecture of VANET where CRL is segmented into two types: large-scale CRL called global CRL and small-scale CRL called regional CRL. The global CRL contains the list of all revoked certificates in the networks and the regional CRL contains the list of revoked certificates which is valid for the given region (domain). The regional CRL is proactively and reactively synchronized with the global CRL by the TA, thus the malicious nodes are detected when traveling from one domain to another.

Fig 3.2 shows the updated version of the Public Key Infrastructure in hierarchical VANETs from RFC 5280 [26]. A domain consists of a L-RSU, M-RSUs, and vehicular nodes. The L-RSU manages M-RSUs and the vehicle nodes inside the domain. The

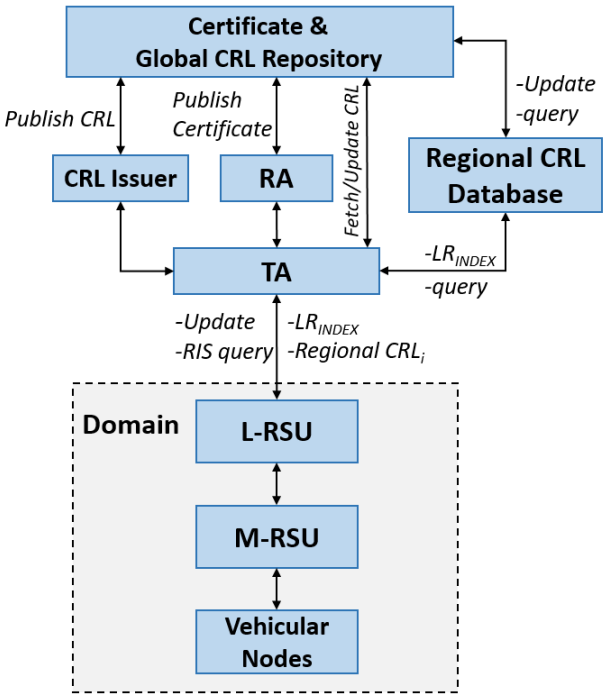

FIGURE 3.2: Public Key Infrastructure in hierarchical VANET

L-RSU is distinguished by the unique identifier called leader RSU index (LR_{INDEX}). When a vehicle enters a domain, a query about the revocation status information (RIS) is sent to TA by the L-RSU. The L-RSU is responsible for sending RIS query to the TA in case of dispute and also sends the update if any misbehaving nodes are detected within the domain using misbehaving node detection algorithms such as MDS [45]. The L-RSUs are connected with the TA and authorized to distribute the regional CRL in a domain.

The PKI entities consist of the trust authority which also serves as a Certificate Authority (CA). The TA is connected with the Registration Authority (RA) where the vehicles are registered initially and the vehicle certificates are issued. Similarly, the TA is also connected with the CRL Issuer which is responsible to publish the certificate revocation lists. The TA, the RA and the CRL Issuer are connected together with Certificate & Global CRL repository that serves the database for all certificates i.e., legit and the revoked. The TA can synchronize, fetch and update the CRL anytime. The regional CRL database is connected to the global CRL database and the TA. The TA provides the LR_{INDEX} of the L-RSU on the basis of which the regional CRL database constructs the regional CRL. The TA can query about the regional CRLs and global CRL for any malicious nodes. Similarly, the regional CRL and global CRL can query each other for update and synchronization.

The size of the CRL is influenced by the number of vehicles in the given geographic region of the domain. To protect private information and anonymity of vehicle, the certificates of vehicles are frequently updated in a short time interval [46]. The appropriate regional CRL size can be achieved by considering the required number of vehicles in a domain. If a number of vehicles inside a domain are (N_D), then the average number of vehicles in a domain can be calculated as average N_D and the total segmented regional CRLs can formulate the global CRL as follows:

$$\text{Average } N_D = \frac{\text{total \# of vehicles}}{\text{total \# of domains}}$$

$$\text{CRL}_{Regional_1} + \text{CRL}_{Regional_2} + \ldots = \text{CRL}_{Global}.$$

Depending upon the number of vehicles to accommodate in the domain, the domain size can be dynamically adjusted such that the desired size of the regional CRL can be accomplished. Thus, our proposed scheme provides a scalable and applicable solution not only to reduce the CRL size but also to manage CRL efficiently in VANETs.

3.3.1 Certificate Revocation List Synchronization

In the hierarchical VANETs with PKI entities, it is crucial to integrate the L-RSUs together with the TA and synchronize the global and the regional CRLs. This allows tracking malicious nodes entering from one domain to another. Our previous work [41] studied the hierarchical architecture of VANETs to allow secure communication in the domain. Extending the previous work, vehicles can acquire the regional CRL valid within a domain when initiating communication within the domain.

Fig 3.3 illustrates the method to synchronize the regional CRL of a domain with the global CRL. A vehicle can enter inside any domain either from the M-RSU or from the L-RSU as shown in the step 1. When the vehicle initiates for the connection setup, it also sends the certificate to the M-RSU. The M-RSU forwards the request to the L-RSU. The L-RSU sends its LR_{INDEX} and its RIS query that contains the identifier of the vehicle certificate to the TA as shown in the step 2. The TA then inquires global CRL database and updates the regional CRL with respect to the LR_{INDEX} if necessary. The TA then sends the response to the L-RSU with updated regional CRL if the entering node is malicious otherwise acknowledge the response which is shown in a step 3. Note that the TA also periodically sends the updated regional CRLs to the domains. After receiving the response from the TA, the L-RSU then checks if the certificate of the vehicle is revoked or not. If the certificate is revoked, the L-RSU then distributes the updated regional CRL inside the domain and aborts the communication initiation process with the revoked vehicle. Otherwise, for the valid certificate, the L-RSU provides the updated regional

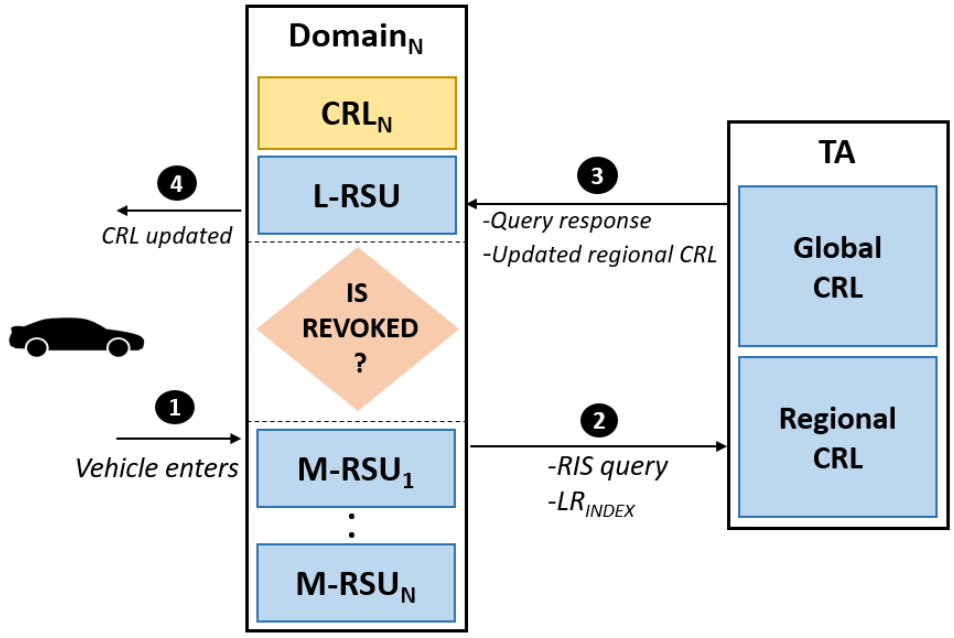

FIGURE 3.3: CRL synchronization flow

CRL to the vehicle that can be used inside a domain. For instance, when a malicious vehicle travels from Los Angeles to New York City and tries to initiate communication in New York City, the TA can verify if the certificates of the vehicle are revoked from the global CRL, and update the regional CRL, so that the malicious vehicle cannot use its certificates within the domain in New York City. Therefore, under the proposed scheme, malicious nodes are not able to use revoked certificates in any regions.

3.3.2 Utilizing Dual Bloom Filter

When the size of CRL is minimized, it can be efficiently managed and distributed in VANETs. Using bloom filter, the size of certificate revocation list can be reduced to the fixed value, however, it still suffers from false positive issues which can misidentify the valid and revoked certificates. To address the false positive issue, the proposed scheme adopts the two bloom filter.

Figure 3.4 shows the revocation mechanism of the dual bloom filters. It is obvious that CRL can be efficiently managed and distributed when the CRL size can be minimized. However, using the bloom filter for CRL revocation reduced the CRL size to the fixed value but it suffers from the false positives which can misidentify the valid and revoked certificates(false matches). The proposed scheme adopts the dual bloom filter proposed by Rabieh et al. [40] that can minimize misidentifying the valid certificates as the revoked certificates. Thus, when a vehicle wishes to validate a certificate, it compares with the

first bloom filter that contains the revoked certificates. Note that the bloom filter has a property that there are no false negatives.[1] When there is a match in the first bloom filter, then the certificate is compared with the second bloom filter that contains the valid certificates. If there is a match in both CRL, the vehicle sends the RIS query message to the L-RSU which is then forwarded to the TA and the probability of a match in both dual bloom filter is called certificate verification failure probability (CVFP). Thereby, using the dual bloom filter, the size of certificate revocation list can be reduced by compression and misidentifying certificates can be minimized.

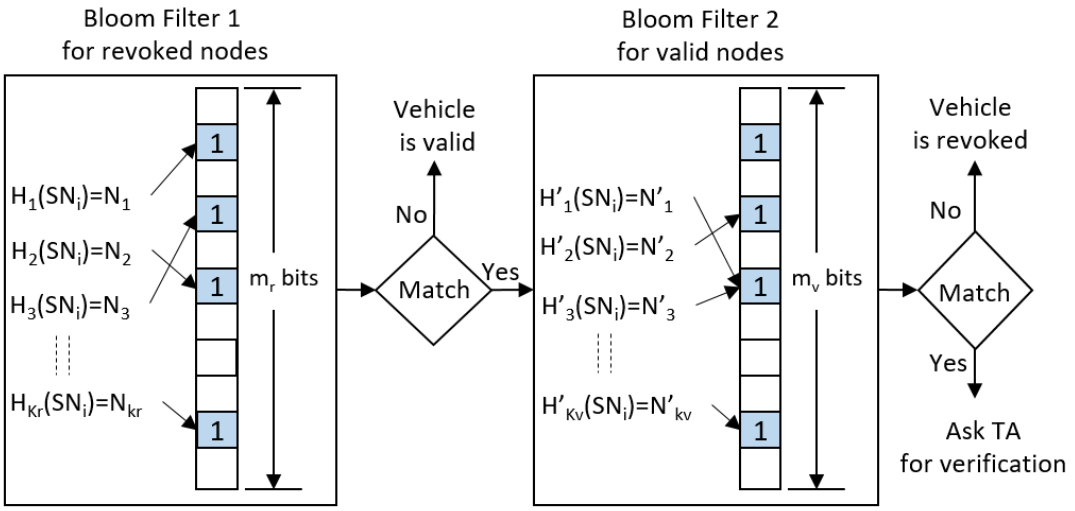

FIGURE 3.4: Dual bloom filter for revocation list

Let the size of the two bit vectors of the bloom filter are m_r and m_v for the revoked and valid certificates. The serial number (SN_i) of the certificates (N_r-revoked and N_v-valid) are hashed with two different hash functions of sizes K_r and K_v respectively and stored in the designated bit vectors. The SN_i of the certificate is hashed and compared in the first bloom filter and if matched then compared with the valid bloom filter. Equation 3.1 and Equation 3.2 show the false positive rate of the dual bloom filter for the revoked certificate (FPR_r) and valid certificates (FPR_v), and Equation 3.3 shows the certificate verification failure probability (CVFP) of the dual bloom filter [40]

$$FPR_r = \left(1 - \left(1 - \frac{1}{m_r}\right)^{K_r N_r}\right)^{K_r} \tag{3.1}$$

[1] In bloom filter, if there is no match then it is sure that the certificates are not in a hashed in the given bloom filter

$$FPR_v = \left(1 - \left(1 - \frac{1}{m_v}\right)^{K_v N_v}\right)^{K_v} \tag{3.2}$$

$$CVFP = P_r\,(\text{the certificate is revoked}) \times FPR_v + P_r\,(\text{the certificate is valid}) \times FPR_r. \tag{3.3}$$

3.4 Analytical Evaluation

In order to analyze the performance of the proposed scheme, we first evaluate the expected CRL size in the hierarchical VANET using the two bloom filters and then we find the optimum CRL size by varying the domain size.

3.4.1 Certificate Revocation List Size

In the proposed scheme, we modified the CRL format [5] for regional CRLs, which is shown in TABLE 3.1. The modified version contains additional fields: LR_{INDEX}, Hash functions and the bit vectors of the two bloom filters as it represents the domain and the revocation list based on the dual bloom filter. The hash functions contain the number of independent hash functions K_r and K_v that hashed the bit vector m_r and m_v of the dual bloom filter. In addition, it contains the key components of CRL that are a version, unsigned part (craca_id, Issue Date, Next CRL, PriorityInfo, & additional fields), ECDSA Signature, and the signed part (Certificate). The CRL version provides the information about its latest release. The unsigned field contains the: craca_id, Issue Date, Next CRL, PriorityInfo, which provides the information about the CA identity, issued CRL time stamp, estimated time for next CRL arrival and the CRL priority. The TA then signs the unsigned portion and append into ECDSA signature. The size of the regional CRL in this approach is (126.5 + K_r + K_v + m_r + m_v) bytes.

The expected size of the CRL can be found with the values of K_r, K_v, m_r and m_v. Let us consider the scheme is using five different SHA-256 hash functions $\{H_1(), H_2(), ...H_5()\}$ for both bit vectors so that $K_r = K_v = 160$ bytes[2]. Rabieh et al. [40] has provided the values of the m_r, m_v for different certificate verification failure probability(CVFP). For CVFP=0.05: m_r=8*N_r & m_v=3*N_v ; CVFP=0.1: m_r=8*N_r & m_v=1.5*N_v and CVFP=0.15: m_r=6*N_r & m_v=N_v. With the assumption of 10% of the total certificates

[2]With the SHA-256 hash functions, it takes 32 bytes for each hash function

Field	**Desciption**		**Size(Bytes)**
Version	Certificate	Uint8	2
craca_id	CA_id field	SIZE(8)	8
Issue Date	CRL issued time stamp	Uint32	8
Next CRL	Next Expected CRL	Uint32	8
PriorityInfo	CRL Priority	Uint8	2
LR_{INDEX}^*	L_{RSU} *Index ID**	*Uint5**	*2.5**
Hash functions*	*For revoked Certificate**	*Domain Variable**	K_r^*
	For valid Certificate*	*Domain Variable**	K_v^*
Two Bloom Filter*	*Revoked bit vector**	*Domain Variable**	m_r^*
	valid bit vector*	*Domain Variable**	m_v^*
Signature(ECDSA)	$(r + s)$	Data-Encryption	64
Certificate	Public Key of TA	Authentication	32

TABLE 3.1: Regional CRL format

(N) are revoked, then revoked certificates are $N_r = 0.1 * N$ and valid certificates are $N_v = 0.9 * N$.

Fig 3.5 shows the size of the regional CRL against the number of vehicles with three different verification failure probabilities. Considering one certificate assigned to one vehicle, it is observed that the least CFVP has the highest size of CRL. For the 40,000 vehicle, with CFVP=0.05, CRL size is 18 Kbytes; CFVP=0.1 has CRL size 11 Kbytes and CFVP=0.15 CRL size is 8 Kbytes. It is obvious that there is a trade-off between the least CVFP and high CRL size, however, if the CVFP is very high, there will be high retransmission for the RIS query and it also adds the latency during the communication which is not suitable for the VANETs communication. An appropriate value of CVFP can be set by taking account of network parameters like resource utilization, latency/delay requirement.

The proposed scheme provides the benefit of reduced CRL size with hierarchical domains. Even when the average number of car sale in the U.S. is considered, which is 6.3 million every year [47], approximately 63 million cars are sold for last 10 years. With CFVP of 0.1, revocation probability=10% & one certificate per vehicle, the global CRL size will be 17 Mbytes. With the same parameter, if we assume that each domain contains only 10,000 vehicles then the regional CRL will be only 11 Kbytes. The CRL size is thus reduced by a factor of 1600 times which can reduce unessential network usage.

3.4.2 Optimal domain size

Regional CRL sizes can vary with the domain size. With the increase in the number of the domain, we can get the small CRL size. We have set LR_{INDEX} to 2.5 Bytes

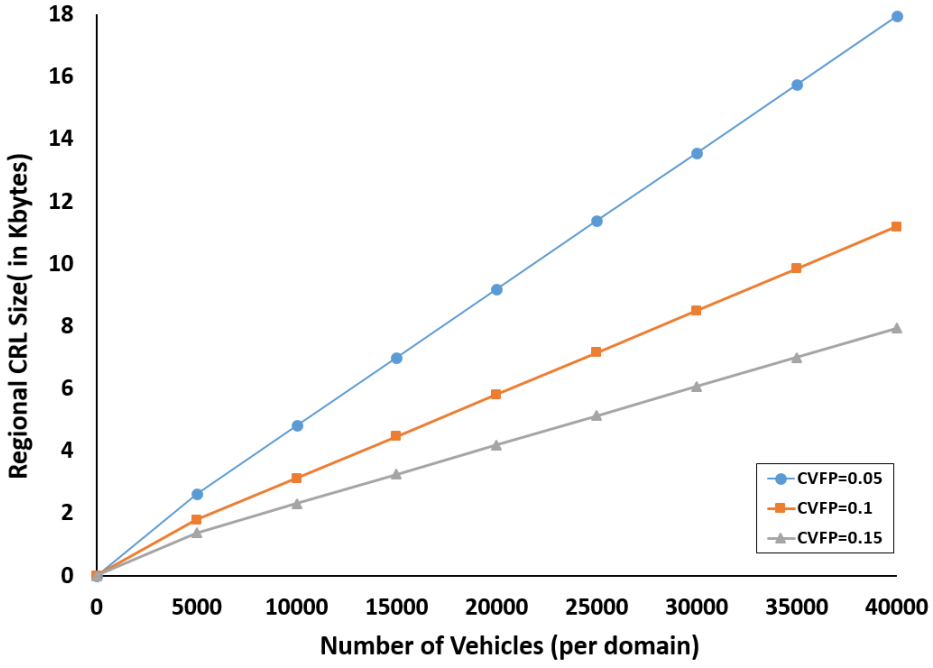

FIGURE 3.5: Regional CRL Size with the domain size

(Table 3.1) that will provide (2^{20}) possible number of domains (also number of L-RSUs). There are 2.5 billion vehicles registered from 2007 to 2017[47]. With the considered value of LR_{INDEX}, a number of vehicles per domain will be (2.5 billion $\div$ 2^{20}) i.e. 2300 vehicles per domain. The optimal value of the domain size can be chosen if we have the desired value of the CRL size. If the number of vehicles increases in a domain, infrastructures can be added and the domain size can be adjusted dynamically as per requirement.

Fig 3.6 shows the relationship between the CRL size and the number of domains with three CVFP values 0.05, 0.1 and 0.15. We select total vehicles N=40,000 and assumed 10% probability for the revocation. We assume that with increase in the domain size, the vehicles will be divided symmetrically distributed per domain. It can be observed that with the increase in the number of domains the CRL size decreases. This is because as the number of domain increases, there will be less number of vehicles per domain and thus the number of revoked certificates is also lower compared to the revoked certificates in the global size. The CRL size of the one domain provides the global CRL size whereas the number of domain begin to increment it gives the regional CRL size.

3.5 Conclusion

In this chapter, an efficient scheme to address CRL distribution and management in the global scale of hierarchical VANETs is proposed. The global CRL is segmented into many regional CRLs which can be distributed efficiently through hierarchical VANETs.

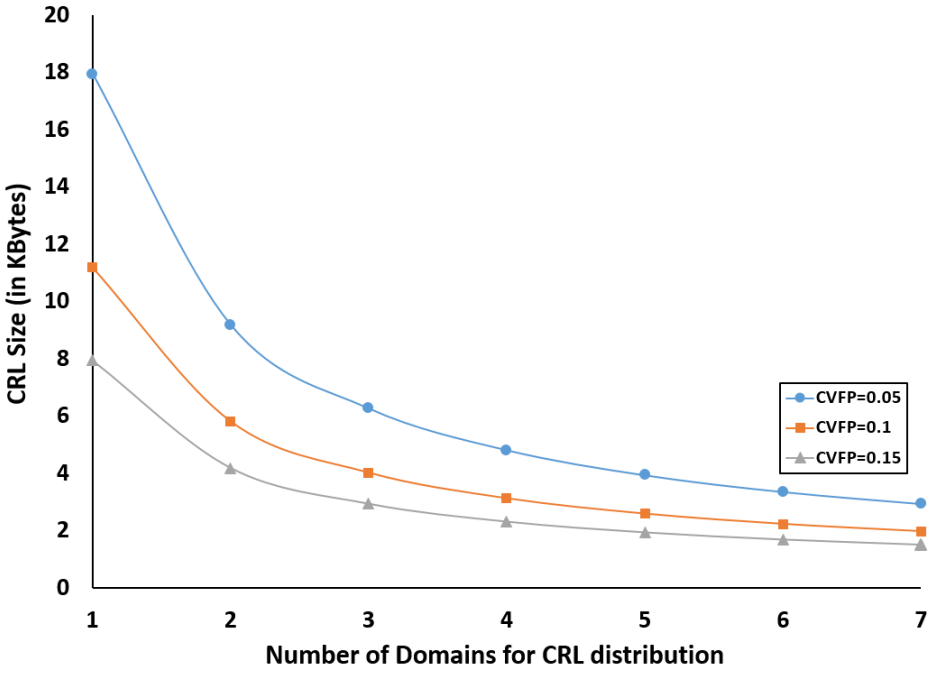

FIGURE 3.6: CRL size with number of domains

Moreover, this scheme utilized the dual bloom filter to minimize the false positive rate as well as the size of CRL. Through the analytical evaluation, it is shown that the expected value of compressed CRL size can be achieved, which is significantly less than the global CRL size. Also, the domain size can be dynamically adjusted with the required regional CRL size or the number of vehicles within a domain.

Chapter 4

Authentication in VANETs

4.1 Introduction

Vehicles exchanges the information related to the weather, road-side emergency, broadcasting alerts, navigations/maps and entertainment services through the shared wireless communication. Since network is shared, the privacy of the user and the message integrity of the vital information are required to secure the driving environment safe and sound. Thus, VANETs must provide the following security requirements [20] to assure the protection in its applications: 1) user privacy information should not be associated with any type of messages during the transmission, 2) attackers should not be able to identify the vehicle by analyzing the messages to ensure privacy, 3) nodes must not deny the authenticity of the signature and the message originated from it, 4) only the desired vehicles can decrypt or verify the intended messages, 5) integrity and authenticity of message should be guaranteed in communication.

4.2 Challenges in group signature

The group signature [48] is a privacy and security scheme that forms a group from the set of users but the users remain anonymous to each other. Boneh et al. [49] then proposed the short group signature where multiple group private keys are assigned to a single group public key. Many approaches employed the short group signature; Hao et al. [50] in Distributed Key Management (DKM) scheme used the trusted authority to generates and manages the group keys; Chim et al. [51] in VANET-based secure and privacy-preserving navigation (VSPN) scheme applied the trusted authority to design and classify the users and also to distribute the group keys among the user groups and update them in the revocation procedure. The practice of designing trusted authority

to perform such activities (managing and distributing the group keys) [51, 52], leads VANET architecture centralized and the trusted authority to bear the high amount of load. As the nodes in VANET interacts with the multiple infrastructures while moving, the trusted authority has to initiate, distribute and monitor the group keys of all the vehicles as well as revoke the certificates when necessary. Due to the centralized key management, it can affect the networks adversely in terms of the performance, for an instance, when a system maintenance is required or backbone link is broken, the service would not be available until the situation is resolved. Although, the group keys are used for the secure V2V and V2I communications, there is still a challenge in delivering the group keys securely from the key generator to vehicular nodes and if the transmitted group keys are intercepted by the attacker then it might impact on the networks severely. Thus, it demands an efficient manner to deliver the secret keys to vehicular nodes. In regard to the group keys in VANET, it has only been applied to the set of nodes confined within in the coverage of a RSU [50, 51]. The RSU issues the keys to the vehicles only within its range, so the vehicle has to perform the key initialization process to get a key with every RSU along its movement. If a group can be widened to a large space then the vehicle can share the same key in the larger area of the several RSU range utilizing key for a longer period of time.

Vehicles are authenticated using the certificates issued by TA that has a expiration time. To preserve the privacy and anonymity of the user, the certificates are frequently updated [33]. Upon detection of the malicious mode, all the certificates that are held by such nodes must be revoked through the Certificate Revocation List (CRL). The growing CRL size creates another issue in VANET. To describe it further, a total of 4.3 million vehicles has been stolen from 2011 to 2016 [34]. Even with considering one certificate (size of 100 Bytes approx.) to one vehicle, the total size of the certificates to be revoked would be 431 MBytes. With the large size of certificates to be revoked creates the large CRL size. Such large CRL must be propagated throughout the entire vehicular network which is a challenging issues in VANETs as it demands the excessive consumption of the resources.

To overcome the above-mentioned issues, in this research paper, a hierarchical based topology of VANET is proposed that comprises a number of RSUs as a domain with a leader RSU that manages the domain. The group based signature scheme intends to provide secure, scalable and efficient key management solution in the VANETs. In addition, prior to issue key for the node, our scheme authenticate the vehicle credential using the CRL list that allows the legitimate vehicles to communicate within the domain. Further, to securely deliver the keys to vehicular nodes, a shared symmetric key is used between a vehicle and an RSU which is much faster and has a low computation overhead. The shared symmetric key can be securely provided to the vehicle with the use

of Diffie-Hellman key exchange protocol [53]. Thus utilizing short group signature and secure key distribution approach, vehicles can freely communicate in an entire domain of several RSU ranges with the same group keys, and the centralized work load of the trusted authority can be distributed to the group of leader RSUs. Furthermore, with the distribution of the updated CRL in each domain, we aim to minimize the CRL size within the VANETs such that vehicular nodes achieves the secure, efficient and scalable key management mechanism with small sized revocation list.

4.3 Related Work

Many research papers have focused to address the security and privacy challenges in VANETs. Attacks to track the location of vehicles and reveal the identity of drivers must be prevented to preserve the privacy of drivers. A basic idea to protect the privacy is proposed in [27] where the real identity of the vehicle is replaced by a pseudo identity called pseudonyms. To keep the location privacy throughout the vehicle movement, pseudonyms should be dynamically updated, otherwise, the location of vehicles can be tracked through the static pseudonyms update, and driving pattern can be identified by eavesdroppers. This problem can be addressed using the set of pseudonyms where each pseudonym is used for a certain amount of time. The new and old pseudonyms have to be performed secretly so that it cannot be sneak by eavesdroppers. For this propose, mix-zone [54] and silent-period [55] have been proposed to enhance the security of the pseudonym schemes, where the silence represents the area with dynamic traffic such that the node varies dynamically and the mix sone represents the area where the pseudonyms can be replaced. However, finding the silence zone and mix zone is not easy, it requires extra computation and this scheme overlooks the potential of the attacker. Further, an AMOEBA scheme was proposed by Sampigethaya et al. [56] for the privacy preservation of the node, where vehicles form groups and all the group members forwards messages to their group leaders. This scheme preserves the privacy of all the group members by risking the privacy of the group leader, but it has not incorporated the threat of the privacy loss of its group members if the group leader is compromised.

Chaum et al. [48] introduced group signatures for anonymous authentication such that a member of a group can anonymously sign the message on behalf of the group. However, due to the large size of group signature, it was not practical. Boneh et al. [49] re-constructed and made the signature of size under 200 bytes which is suitable for practical application. By the use of bilinear mapping , it has several group private keys corresponding to one group public key. Under this scheme, the receiver can verify the validity of the group signature without knowing the identity of the group member, but

the identity can be revealed when necessary. Sun et al. [28] proposed a pseudonymous authentication for vehicular communication, where the group signature is used to provide security, anonymity and traceability property. Similarly, in a distributed key management framework [50], the group signature based scheme is used for the key management and distribution. In this scheme, a group is formed within each RSU area, where an RSU distributes the group keys to its group members. However, this scheme did not consider the overhead of frequent key establishments. As an example, if a vehicle is required to enter the new RSU then it has to initiate the key establishment process over again. Further, the paper has not discussed the way to deliver the group keys in a secure manner between the node and the infrastructure.

Several schemes have been proposed for the signature scheme in the VANET. Zhang et al. [57] devised IBV, which is identity based (ID-based) signature to realize batch verification of the signature that can reduce the verification time of the signature, however, any malicious vehicle can forge the signature and it cannot detect the invalid signature. EPAS [58] is also an IBV based protocol which is modified further to reduced the verification time. Ravi et al. [59] implemented ECDSA as a message authentication scheme for VANET and Huang et al. [60] proposed ABAKA scheme for the batch authentication and key agreement. Both algorithm has used the ECDSA scheme for message authentication. Although, verification time in both ECDSA and ABAKA is quite lower than other scheme, the usage of elliptic curve in the every message adds the large computational overhead. Thus, in this paper, we will compare the performance of our algorithm with the above mentioned scheme in terms of the delay.

An anonymous authentication scheme [20] is proposed to provide the features of authentication, integrity, repudiation, and privacy which were not present in pseudonym schemes. Each vehicle requires storing the large preloaded anonymous public/private key pairs and authority has to handle key pairs for its distributions. Pseudonymous authentication scheme [61, 62] is a kind of anonymous authentication scheme that uses pseudonyms certificate instead of the real vehicle identity. Certificate revocation lists(CRL) have to be updated and stored for the all the revoked vehicles which make this scheme less efficient.

With the growing nodes in the VANET, it needs to consider the existence malicious node and such nodes must be revoked promptly. In order to distribute the information quickly Certificate Revocation Lists (CRLs) is used. Since the CRL has to be distributed widely and quickly, it is needed to be compressed as much as possible. [32, 35] have proposed the use of bloom filter to compress the CRL to use efficiently in the VANET. Similarly, [40] has used two bloom filter to compress the CRL as well as deal with the false positive associated in the bloom filter. In our scheme, the CRL can be distributed in

a hierarchical manner followed from the TA to the leader RSU and then to the member RSU, which will be more efficient than broadcasting through the TA.

In this paper, the main goal is to design an efficient protocol that a group key can utilize in the larger domain of multiple RSUs instead of the limited boundary of one RSU so that vehicles can communicate in the larger area with the same group keys. Under our scheme, each domain will be provided a domain leader, called the leader RSU which will be responsible for the issuance of group keys to the vehicles within the domain and maintaining the records. This not only alleviates the burden from the trusted authority in the key management and distribution process but also provides scalability to the system. In addition, group private keys can be securely distributed to vehicles once vehicles set up a symmetric secret key with the RSU using Diffie-Hellman key exchange protocol [53]. Thus, this scheme can provide the efficient and scalable approach to utilize the group keys and deliver the group keys securely in vehicular networks.

4.4 Proposed Model

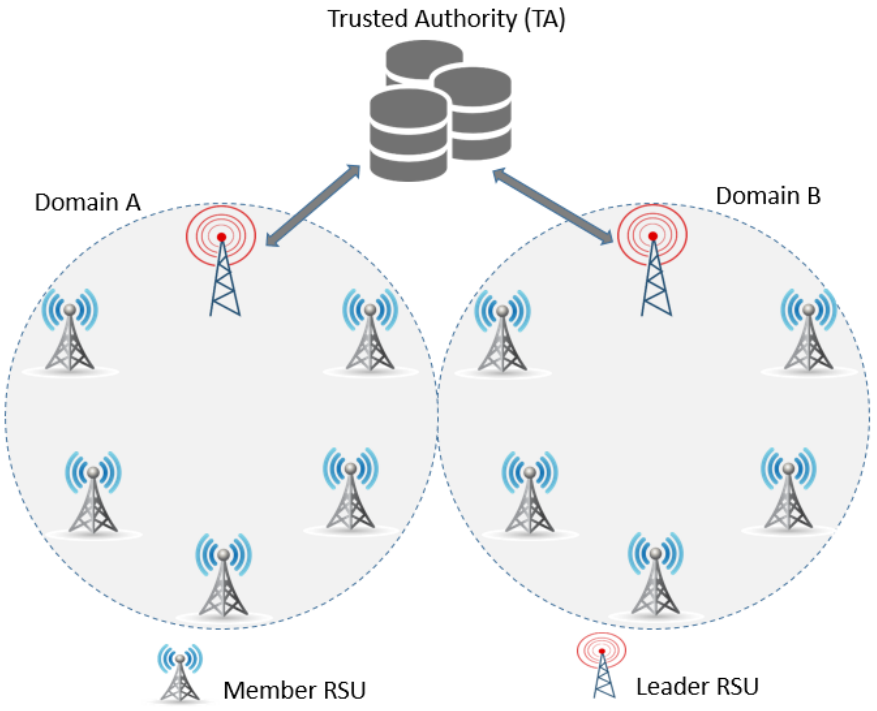

FIGURE 4.1: Overview of the Proposed Model

In the network, it is assumed that the following key components: a Trusted Authority, Road Side Units, and Vehicle Nodes. In Figure. 4.1, the overview of the system model is illustrated.

- **Trusted Authority (TA):** Vehicles are registered by the trusted authority and provided the certificates. TA and RSUs are securely connected by the stable backbone network. TA can help RSUs to identify the real identity of vehicles when an investigation is required. TA prepares the regional CRL and also distributes it to the specific region. TA also provides a response to the revocation status query from any regions. TA has the highest level of security protection in the VANET architecture and we assume that the TA cannot be compromised.

- **Road Side Units (RSU) and Domain:** RSUs are the infrastructure deployed along the road side which play an important role in key management, message authentication/verification, and message dissemination. A group of RSUs forms a domain. The number of RSUs within a domain can be determined based on the geographical status, infrastructure capacity, deployment plan and vehicle demography. A domain size is defined as the desired number of vehicles that can be accommodated by the number of RSUs within a geographic region. The group key and the CRL are valid for a domain is called regional CRL.

- **Leader Road Side Units (L-RSU):** RSUs are further classified into member RSUs (M-RSU) and leader RSUs (L-RSU). The L-RSUs coordinate with the trusted authority and generates the group private keys and group public keys for the vehicles. The L-RSUs also manage and maintain the database of the group keys and the regional CRL that for its domain. Upon detecting suspicious behavior, the L-RSUs communicate with the TA to reveal the identity of the malicious vehicle or it can also send the query to TA to authenticate the certificate of the vehicle. Since the leader RSUs play a crucial role in key generation and management process, we assume that the L-RSUs are equipped with the trusted platform modules with high level of security protection and cannot be compromised.

- **Member Road Side Units (M-RSU):** Unlike L-RSUs, M-RSUs do not perform the key generation and management process and do not take part in CRL management, but instead M-RSUs can help vehicles to obtain the group keys and updated regional CRL provided by the leader RSU. Thereby, M-RSUs are semi-trust with the medium security level.

- **Vehicular Nodes:** Vehicular nodes are vehicles on the road which are equipped with an on-board unit (OBU) for computation and communication, a global positioning system (GPS) for location service, and an interface for interacting with drivers. Vehicles can communicate with each other or with RSUs through the radio defined under the IEEE Standard 1609.2 [5], which is a standard for the wireless access in vehicular environment (WAVE). During the communication, vehicles are

required to use the group keys and its own public and private key pairs for the authentication and encryption/decryption. Such keys are stored in a tampered proof device (TPD) [43] for the security purpose. Before any communication, vehicle validates the authenticity of the communicating node by comparing the certificate in he CRL list. We assume that vehicles obtain the public keys of the RSUs when registered by the TA, and update them routinely.

4.5 Proposed Scheme

In this section, the basic idea behind the protocol is presented and then describe the protocol in detail. The notation used in this paper is listed in Table 4.1.

TABLE 4.1: Notations

Notation	Description
R_i	an RSU i
V_i	a vehicle i
$L\text{-}RSU$	a leader RSU
$M\text{-}RSU$	a member RSU
T_s	a time-stamp
C_{V_i}	certificate of V_i issued by the TA
gpk	a group public key
$gsk[v_i]$	a group private key of a vehicle V_i
SK_{V_i}	Private key of V_i
PK_{V_i}	Public key of V_i
dgt	digital signature
$K_{V_i\_MR}$	shared secret key between V_i and $M\text{-}RSU$
FPR	False Positive Rate
N_v,N_r	Number of valid vehicles and revoked vehicles
m_v,m_r	Bit vector length of valid and revoked vehicles
K_v,K_r	Hash functions of valid and revoked vehicles
LR_{Index}	Leader RSU Index

4.5.1 Basic idea behind the protocol

The proposed protocol utilizes short group signature protocol [28, 50] to generate a group private key. In our scheme, the leader RSU issues group private keys within a domain as a key generator. In a domain which consists of multiple RSUs, there are one group

public key and many corresponding group private keys so any member of a domain can sign messages under the name of the domain and the signed messages can be verified by other members using the group public key. Note that member RSUs help the key establishment process, but they do not generate or issue any keys. This provides small overhead compared to other group signature schemes and group private keys can be retrieved from signatures using tracing keys. Also, the same group key can be used with multiple RSUs within a domain without having to initiate a key establishment process. Fig. 4.2 illustrates how vehicles can request a group private key to the leader RSU within a domain.

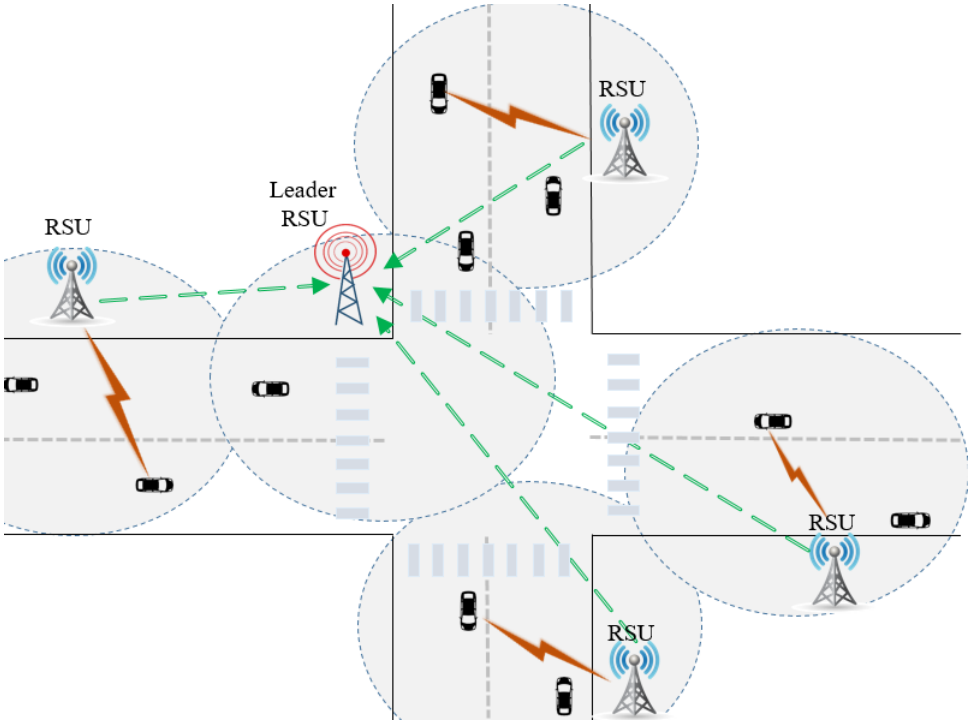

FIGURE 4.2: Group Key Request to Leader RSU

4.5.2 Short Group Signature

Boneh et al. [49] proposed the short group signature and has implemented in many literatures [63, 64]. The working of short group signature is as follows:

4.5.2.1 Key Setup

In order to generate the cryptographic system, the trusted authorities generates the two bilinear multiplicative groups G_1 and G_2 with the generators g_1 and g_2 of the prime order p. Let χ be a computable isomorphism from G_2 to G_1 with $\chi(g_2)=g_1$. Now, parameters are selected by the trusted authority $h_t \xleftarrow{R} G_1 \setminus \{1_{G_1}\}$ and $\xi_1, \xi_2 \xleftarrow{R} Z_p^*$ randomly and

set $u, v \in G_1$, such that $u^{\xi_1} = v^{\xi_2} = h$, where Z_p^* is a multiplicative group of order $p-1$. TA randomly selects $\psi \xleftarrow{R} Z_p^*$ and then set $w = g_2^{\gamma}$. The private key can be derived as $gmsk_t = (\xi_1, \xi_2)$ and $gmsk_m = (\psi)$ respectively and the group public key for the vehicles in the domain can be derived as $gpk = (g_1, g_2, u, v, h, w)$.

4.5.2.2 Membership Registration

As the vehicle approaches towards the domain, the registration process is initiated. Here, a tuple (A_i, x_i) of each vehicle i with the vehicleâĂŹs group private key $gsk[i]$ is maintained by the membership manager which is in our case an infrastructure. For the selection of private key, a random number λ is chosen such that $A_i \leftarrow g_1^{1/(\lambda + x_i)}$. By using ψ, authority selects $x_i \leftarrow Z_p^*$

Thus, the trusted authority saves the pair (A_i, ID_i) for the future purpose. After the completion of the registration, the assigned private key will be transmitted securely to the vehicle which will be covered in the subsequent sections.

4.5.2.3 Signing

After receiving the group public key and group private key, the vehicle can transmit the message. Before that, the signing procedure has to be completed which is detailed as:

First, selects the exponents $\alpha, \beta \xleftarrow{R} Z_p$ and encrypts A_i, (T_1, T_2, T_3), where $T_1 \leftarrow u^{\alpha}$, $T_2 \leftarrow v^{\beta}$, $T_3 \leftarrow A_i h^{(\alpha+\beta)}$.

Compute $\delta_1 \leftarrow x\alpha, \delta_2 \leftarrow x\beta$. Picks the random values r_α, r_β, r_x, r_{δ_1} , r_{δ_2} from Z_p. Compute R_1, R_2, R_3, R_4, R_5 as:

$R_1 \leftarrow u^{r_\alpha}$, $R_2 \leftarrow v^{r_\beta}$

$R_3 \leftarrow e(T_3, g_2)^{r_x}.e(h, w)^{-r_\alpha - r_\beta}.e(h, g_2)^{-r_{\delta_1} - r_{\delta_2}}$

$R_4 \leftarrow T_1^{r_x}.u^{-r_{\delta_1}}, R_5 \leftarrow T_2^{r_x}.v^{-r_{\delta_2}}$

Now the challenge c can be obtained using above values and the message M

$c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_p$

Compute s_α,s_β,s_x,s_{δ_1},s_{δ_2} where: $s_\alpha = r_\alpha + c\alpha$,

$s_\beta = r_\beta + c\beta, s_x = r_x + cx, s_{\delta_1} = r_{\delta_1} + c\delta_1, s_{\delta_2} = r_{\delta_2} + c\delta_2$

Now, the message signed in the combination of the parameters above
$\sigma \leftarrow (T_1, T_2, T_3, c, s_\delta, s_x, s_{\delta_1}, s_{\delta_2})$

4.5.2.4 Verification

After receiving the signed message, the receiver first assures the validity if the packet has arrived within the allowed time window. The receiver now recomputes the parameters to perform the signature verification by rebuilding the challenge c by itself. The following parameters $(R_1, R_2, R_3, R_4, R_5)$ are reconstructed as follows:

$\tilde{R_1} \leftarrow u^{s_\alpha}/T_1^c, \tilde{R_2} \leftarrow u^{s_\beta}/T_2^c$

$\tilde{R_3} \leftarrow e(T_3, g_2)^{s_x}.e(h, w)^{-s_\alpha - s_\beta}.e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}}.(e(T_3, w)/e(g_1, g_2))^c$

$\tilde{R_4} \leftarrow {T_1}^{s_x}/u^{s_{\delta_1}}$, $R_5 \leftarrow T_2^{s_x}/v^{s_{\delta_2}}$

Then, $\tilde{C}$ is re-computed from:

$$\tilde{C} = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$$

After computing the challenge now the receiver verifies if the value of $\tilde{C}$ matches with the value of c in the signature contained in σ. If the message is genuine then the receiver sends the message intact to the trusted group members otherwise it will drop the message.

4.5.2.5 Key Retrieval

Retrieve operation is performed when there is a dispute to identify the real identity of the signature generator. Trusted authority checks the validity of the signature and computes A_i as:

$$A_i \leftarrow T_3/(T_1^{\xi_1}.T_2^{\xi_2})$$

Algorithm 1: Group Key Generation

1: $V_i \rightarrow M_{RSU}$: Send message m_1.
m_1: $(g, p, A, \{g, p, A \| T_s\}_{SK_{V_i}}, C_{V_i})$
2: $M_{RSU} \rightarrow V_i$: Send message m_2.
m_2: $((B)_{PK_{V_i}}, \{A \| B \| T_s\}_{SK_{MR}}, C_{MR})$
3: $V_i \rightarrow M_{RSU}$: Send message m_3 Ack and Request.
m_3: $((B \| T_s)_{SK_{V_i}}, (Req)_{K_{V_i - MR}})$
4: $M_{RSU} \rightarrow L_{RSU}$: Forwards request to L_{RSU}
via message m_4.
m_4: $(ID_{LR}, ID_{MR}, \{Req, C_{V_i}, T_s\}_{PK_{LR}})$
5: L_{RSU} checks CRL list: Proceed if certificate of V_i is not found in CRL list.
6: $L_{RSU} \rightarrow M_{RSU}$: Issues a group key and send msg m_5.
m_5: $(ID_{LR}, ID_{MR}, \{gpk, gsk[v_i], T_s, dgt_L\}_{PK_{V_i}})$
7: $M_{RSU} \rightarrow V_i$: Sends message m_6.
m_6: $(m_5, HMAC(m_5))$
8: V_i receives the group key$\rightarrow gpk, gsk[v_i]$.
9: Message Signing: Vehicle v_i signs message in the combination of the following parameters .
$\sigma \leftarrow (T_1, T_2, T_3, c, s_\delta, s_x, s_{\delta_1}, s_{\delta_2})$
10: Message Verification: The receiver verifies by matching c with $\tilde{C}$
$\tilde{C} = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
11: **if** $\tilde{C}$ matches c **then**
message is genuine
12: **end if**

The authority can now lookup to its saved database to identify the real identity from the element A_i.

4.5.2.6 Membership revocation

If the vehicle is found compromised, its keys are identified by the TA. The provided group private key $gsk[i]$ to the vehicle i is associated with the A_i through the tuple and thus the identity ID_i will be revealed. The identified vehicle will be added in the CRL-based revocation scheme and the updated CRL will be distributed to all the valid vehicular nodes and hence the vehicle will be excluded from the system.

4.5.3 Secure Key Distribution Scheme

In this section, a protocol to securely distribute secret keys is proposed while protecting the networks from attackers. It is assumed that the leader RSU is fully trusted and the member RSUs are semi-trusted with possibilities of compromise. In our protocol, vehicles can sign message under the name of the group using group private key. Since there is

only one group public key which corresponds to many group private keys, other vehicles receiving the message can verify the message using the group public key. Besides, while the privacy of the message sender is protected by using group identity, the real identity can be revealed if the authorities need to obtain user information for legal investigation. The detailed process is illustrated in Fig. 4.3.

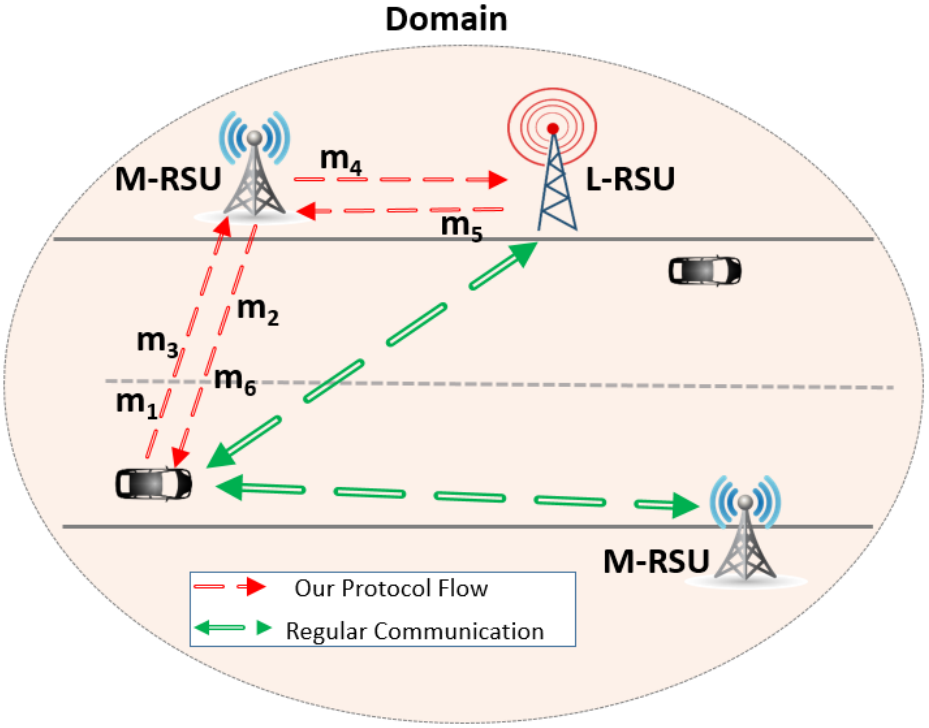

FIGURE 4.3: Protocols Figure

As a vehicle enters an area of a domain, which consists of the leader RSU and many member RSUs, it can communicate with any RSU to securely obtain group public/private key pair. The secure key distribution scheme is based on the Diffie-Hellman key agreement protocol [53] for mutual authentication and sharing a symmetric key. When a vehicle V_i detects a nearby RSU by beacon messages, V_i initiates the protocol by sending m_1. In the protocol, A, B, g, p are the elements of the Diffie-Hellman key agreement, where g is primitive root $mod\ p$, p is a prime number, T_s is a timestamp, a is the secret integer kept by V_i, b is the secret integer kept by the RSU ($M\text{-}RSU$ or $L\text{-}RSU$), and C_{V_i} is the certificate of V_i issued by the TA. Also, A and B are defined as $A = g^a\ mod\ p$ and $B = g^b\ mod\ p$ respectively. In the message m_1, $\{g, p, A \| T_s\}$ are encrypted with the private key SK_{V_i} of V_i so V_i can be authenticated by the RSU after checking the validity of the timestamp and decrypting it using the public key PK_{V_i} of V_i. Note that T_s is used to prevent the replay attack. Once the $M\text{-}RSU$ receives this message, it sends m_2 by encrypting B with the public key PK_{V_i} of V_i and encrypting $\{A \| B \| T_s\}$ with the private key SK_{MR} of $M\text{-}RSU$. Upon receiving the message m_2, V_i sends an acknowledgement

(m_3) for having received B by encrypting it with the private key SK_{V_i} of V_i. At this point, g^{ab} serves as the secret key $K_{V_i\_MR}$ between V_i and M-RSU and this shared symmetric key is used for the following communication. Along with the acknowledgement, V_i also sends a $Request, C_{V_i}$ to M-RSU for requesting a group secret key pair. Since only L-RSU can issue the group secret keys, M-RSU sends m_4 on behalf of V_i. Note that messages are encrypted using the public key of the sender for communication between RSUs so that only L-RSU can decrypt and read the content of messages. After verifying the identity of V_i, L-RSU issues a group public key/group private key $\{gpk, gsk[v_i]\}$ and sends it (m_5) with a T_s and a digital signature $dgt_L = E(H(M), SK_{LR})$ to M-RSU, which is communicating with V_i. By attaching the digital signature, the vehicle ensures that the group key is issued by the leader RSU for the domain. Finally, M-RSU generates a keyed-hash message authentication code (HMAC) using the shared symmetric key $K_{V_i\_MR}$, and sends it with m_5 received from the L-RSU to V_i. This completes the secure key distribution process and the vehicle V_i can sign a message with $gsk[v_i]$ and verify messages with gpk for the communication within the domain.

When a vehicle senses an incident such as traffic jam, accident, inclement weather, bad road condition, etc., it shares the information with nearby vehicles or vehicles within the same domain so that the drivers can take appropriate action based on the information. When a message is broadcasted to the networks, the vehicle signs it using the group private key $gsk[v_i]$ issued by L-RSU. Note that if the message needs to be disseminated further than the communication range of the vehicle, then it can be forwarded through other vehicles or other RSUs using dissemination mechanism such as [65]. When vehicles within the domain receive the message, they can verify the message using the group public key gpk and use the information. Even if the message is authenticated, there are still possibilities that the content of the message could be malicious or false. For instance, an attacker could send fake messages claiming an accident at a certain location to take advantage of traffic on the road (i.e., traffic detour). If a false message is found, then a vehicle reports it to the authorities or L-RSU. Since L-RSU can retrieve the real identity of the vehicle from the group private key $gsk[v_i]$, it can perform investigation process using a verification system such as [66]. Note that our scheme is proposed to securely and efficiently distribute group public/secret keys and address scalability issues, whereas mitigating broadcast overhead and evaluating message contents are out of the scope.

4.6 Evaluation and Analysis

4.6.1 Security Analysis

In this section, a thorough analysis of the security strength of the proposed scheme is presented towards the various attack models discussed in the Section 4.4.

4.6.1.1 Source authentication, privacy

When group keys are assigned to vehicles for communication, the leader RSU provides group keys only after the identity of vehicles are validated. Furthermore, the leader RSU maintains a database of the group keys, certificates, shared secret keys and the time-stamps of the vehicles in the domain. If a vehicle signs a message using its group private keys, then the leader RSU can trace its identity with the help of the TA when necessary. Also, vehicles are assigned group keys for a domain, so vehicles do not use their private information hence the privacy of vehicles are preserved.

4.6.1.2 Anonymity

Once a vehicle is registered within a domain, the vehicle is provided with the group key for communication. Due to the feature of the group signature, the vehicle will remain anonymous to other group members. After changing a domain, the vehicle needs to update group keys for further communication. Note that the original identity can be tracked down by the leader RSU when required.

4.6.1.3 Non-repudiation

A vehicle cannot deny the authenticity of the signature or the message it has sent. Since the leader RSU maintains the database of issued group private keys, it can find the identity of the signer from its table because only a vehicle having the group private key can generate the same signature.

4.6.1.4 Man in the middle attack

In our protocol, the key establishment process is based on Diffie-Hellman key agreement protocol to share a symmetric key for further communication. The Diffie-Hellman protocol is prone to the man-in-the-middle attack [67], however, our protocol does not

suffer from this attack due to the following reasons: As a vehicle V_i initiate the key establishment process, with a member RSU or a leader RSU, it encrypts the contents of the message using its own private key PK_{V_i}. A legitimate vehicle with public/private key pair issued by the TA can try to launch the man-in-the-middle attack, however, the message sender can be traced by RSUs and the TA.

4.6.1.5 Other attacks

Sybil attack This is a type of security attack which is possible when a malicious node can use the multiple identities while communicating. In our protocol, a group key is assigned to a vehicle by the RSU after validating its certificate where the certificate is issued by TA, thus, only a legitimate vehicle can get the group key and only one group key is assigned to the specified vehicle. And the vehicle encrypts the outgoing message using the group key which is provided by the RSU. Hence, a vehicle cannot use multiple group keys to communicate i.e. a malicious node cannot communicate with the multiple identities.

Replay attack Replay attack in VANET occurs when the adversary re-injects the previously received message or the packets. Such attacks can be prevented using the time stamps on the message. Our protocol has used the time stamps to avoid replay attack.

Message alteration attack Such attacks are performed to modify, delete or alter the content of the existing message. In our scheme, we used the group signature which is itself a signature and only the sender can create it. If the vehicle encrypts the message using the group private key, then the RSU decrypts it using the group public key and examine the integrity of the message. Hence, the fabrication/alteration attack is prevented. However, for the relay messages, the vehicle can deny or delete the message which is supposed to be forwarded to the next vehicle. Handling un-cooperative nodes have been studied in the ad-hoc context and similar approach can be implemented.

Collusion attack Even if the vehicle colludes and sends the fake messages, no matter how many vehicles collude, they have to use the group private keys for the communication and their original ID can be traced by the authority in such occasion. Further, if the multiple vehicles are colluded to send the fake messages, such messages will be reported to the RSU by the genuine vehicles and the authority will trace such colluding malicious vehicles.

Revoking malicious/misbehaving node If the node is found misbehaving then such nodes must be detected and such nodes must be revoked from the vehicular networks. Due to the use of CRL management system, our system is secure against such misbehaving nodes.

4.6.2 Performance Evaluation

In order to evaluate the performance of our proposed scheme, our protocol is simulated in the Network Simulator NS-2 [68] and the mobility simulator SUMO [69] with IEEE 802.11p protocol. The size of the map in the topology is 3600 meters by 3600 meters. The vehicles move randomly with the average speed 51km/hr (which is the average speed of vehicles in the U.S.) [70] within a domain. Through our simulation, it is observed that the use of group key in a domain can reduce the time required for the vehicle to establish the key with multiple RSUs within the domain. It is also observed that a vehicle can use the same group key for a longer period of time with the increase in the size of a domain.

4.6.3 Key Establishment

Vehicles are required to use group keys to communicate in a group. When the domain of multiple RSUs is not considered, vehicles have to perform the key exchange procedure with each and every RSUs separately. After a vehicle receives a group key from each RSU, it can communicate within the group. However, the vehicle has to perform the same procedure again as it reaches the area covered by another RSU. This repetitive task of the group key exchange is inefficient and un-scalable. By using the concept of the domain, a vehicle can communicate in the entire domain with the one group key under our protocol. Thus, we evaluate the number of key exchanges performed by vehicles as they travel through multiple RSUs.

Figure 4.4 shows how the average number of key establishment changes as the vehicles are moving with/without using domains. Note that each domain is the area covered by four RSUs and it is assumed that the vehicles move randomly. It is observed that during the time interval of 240 seconds, the vehicle exchanged 16 distinct key establishments while moving without domains. On the other hand, when vehicles are moving in the domains, the vehicles exchanged only four distinct keys during the same time interval.

It is also necessary to analyze the time difference while performing the group signature with domain and without domain for evaluating efficiency. The computation time of the group signature was studied in [28] and it was measured that the signing delay is 3.6 ms and the verification delay is 7.2 ms. Using the same data in the observation

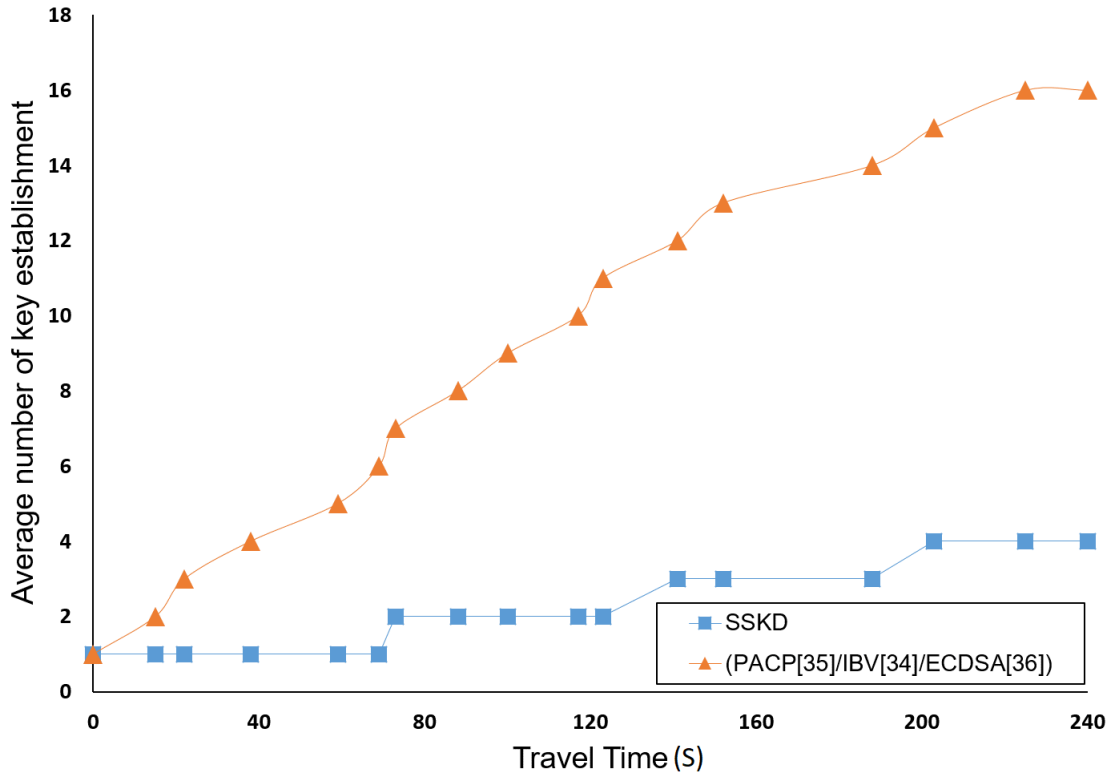

FIGURE 4.4: Average Number of Key Establishment

above, the signing and verification process of the 16 key establishments without using domain takes 16*(3.6+7.2) ms (172.8 ms). On the other hand, while using the domain size of four RSUs, the time taken for signing and verification of four key establishments is 4*(3.6+7.2) ms (43.2 ms).

Note that the leader RSU and member RSUs use a symmetric key for their communication and the time taken to forward the key from the leader RSU to a member RSU can be neglected because the RSUs are interconnected with the stable link.

Thus, with the domain size of only four RSUs, the time-taken for key establishment of the randomly moving vehicles is 43.2 ms which is 400% more efficient compared to the 172.8 ms (time taken for key establishment without domain).

It is worth mentioning that, in practice, the domain size is likely higher, so it can be expected that more efficiency can be provided.

4.6.4 Group Key Utilization

Group key utilization time is the time that the vehicle travels inside the domain after establishing the key. Group key utilization time can be used to consider the frequency of

the group key usage in the specific size of the domain and also helps to understand the average travel time of the vehicles in the domains of different size. For this evaluation, we simulate the randomly moving vehicles with different number of road side units within a domain.

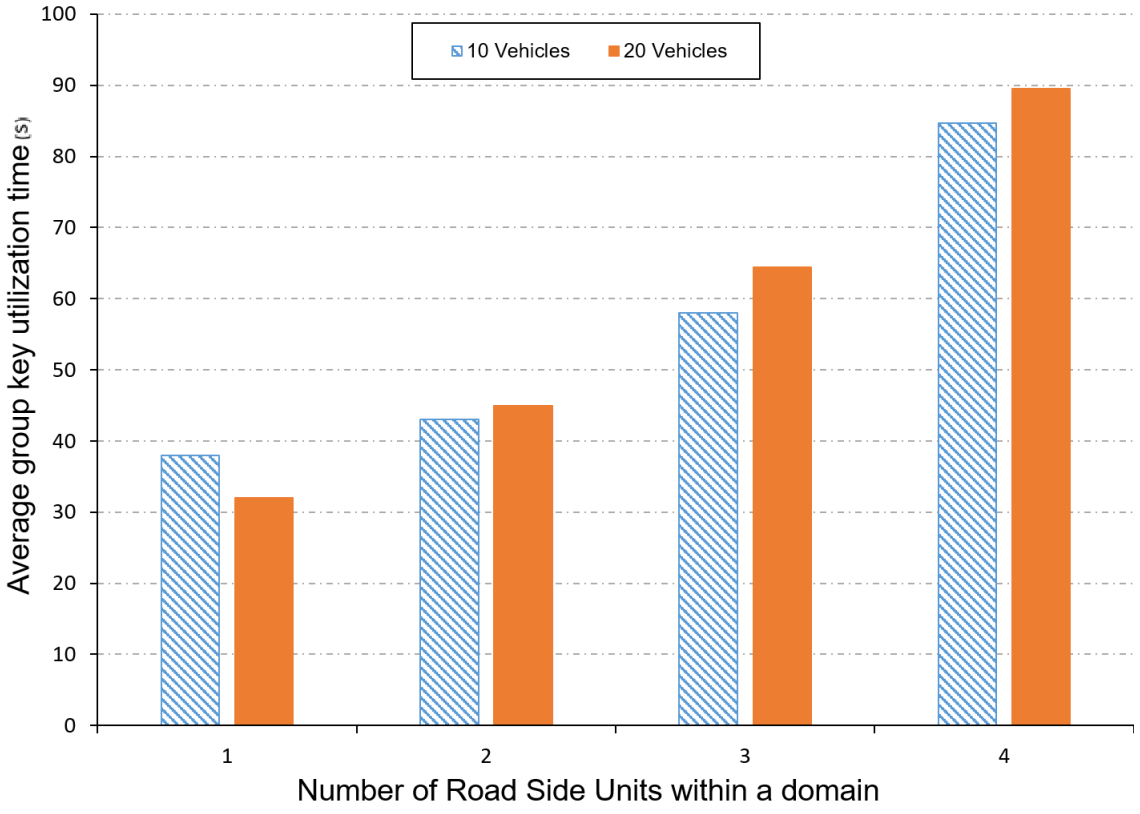

FIGURE 4.5: Group Key Utilization

Fig 4.5 shows the group key utilization time for different size of vehicles after receiving the group keys under the different size of domain. It is observed that the vehicles spends around 30-40 seconds in one RSU on average . When the domain size is increased with two RSUs, the average travel time is slightly increased to around 45 seconds, and the average travel time is continuously increasing as the size of the domain increases. When there are four RSUs within a domain, it is observed that the moving vehicles utilize the group key about 200% more than the moving vehicles without having a group key for the domain. Thus, with the increase of the domain size, the vehicles use the same group keys for a longer period of time.

4.6.5 Communication Overhead

In this subsection, the performance of the proposed scheme is evaluated and analyzed in terms of the verification delay with other schemes because the key generation and

signing takes similar constant time for all the schemes. In the scheme, when the vehicle establishes the group key and sends the message for VANET communication, the receiver (M-RSU or another vehicle) checks the authenticity of the requesting vehicle by comparing the challenge. The receiver has to compute R1, R2 , R3 and R4. Computing R3 is the most expensive part of the verification process. It consists of three multiplication, four pairing operations.

$$\tilde{R_3} \leftarrow e(T_3, g_2)^{s_x}.e(h, w)^{-s_\alpha - s_\beta}.e(h, g_2)^{-s_{\delta_1} - s_{\delta_2}}.(e(T_3, w)/e(g_1, g_2))^c$$

From the experiment in cryptographic pairing in [71] in the MNT curve, which observes processing time for an MNT curve [72] of embedding degree k = 6 and 160-bit q, running on an Intel Pentium IV 3.0 GHZ machine. The following results are obtained which consists the multiplication time ($Tmul = 0.6ms$), pairing time ($Tpar = 4.5ms$) and T_{mtp} is time for map-to-point in hash operation.

Thus, the timing for verification of in our proposed scheme is: $3Tmul + 5Tpar$

Here we compare our signature algorithm scheme which is based on Boneh-Boyen-Shacham (BBS) Group Signatures [49] with the other related signature algorithms schemes like IBV [57], PACP [73], ECDSA [59], EPAS [58] and ABAKA [60] in terms of the verification delay. ECDSA is the signature algorithm used in IEEE1609.2 standard, while PCAP uses BLS scheme that is a short group signature scheme performed for the signature aggregation. Identity Based Verification (IBV) and ABAKA are the typical batch verification schemes adopted in VANET for anonymity and security, while EPAS is an identity based signature schemes with the conditional privacy.

The computational overhead of the schemes is given in the Table 4.2.

TABLE 4.2: Delay comparison of various signature schemes

Scheme	Verification Overhead	Delay
SSKD:	$3T_{mul} + 5T_{par}$	24.3 ms
IBV [57]:	$3T_{par} + T_{mtp} + T_{mul}$	14.7 ms
PACP [73]:	$4T_{par} + 2T_{mtp}$	12 ms
ECDSA [59]:	$4T_{mul}$	2.4 ms
EPAS [58]:	$5T_{mul}$	5 ms
ABAKA [60]:	$7T_{mul}$	4.2 ms

The verification overhead in BBS Scheme seems to be costlier compared to the other approaches. However, BBS scheme has feature of group signature where a multiple group public keys can be assigned for a single group private key which is suitable for the authentication of vehicle. BBS scheme takes a larger time to verify the signature but in

our approach, when a vehicle reaches in the domain, it asks for the key only once and it will be verified throughout the domain. For example, for a single vehicle signature, our scheme takes $3 * 0.6 + 5 * 4.5 = 24.3$ ms whereas IBV scheme takes 14.7 ms. But considering the domain size of 3 RSU (minimal), our approach still takes 24.3 ms whereas IBV will take 14.7 * 3 = 44.1 ms. Thus, BBS scheme in our approach outperforms other signature schemes.

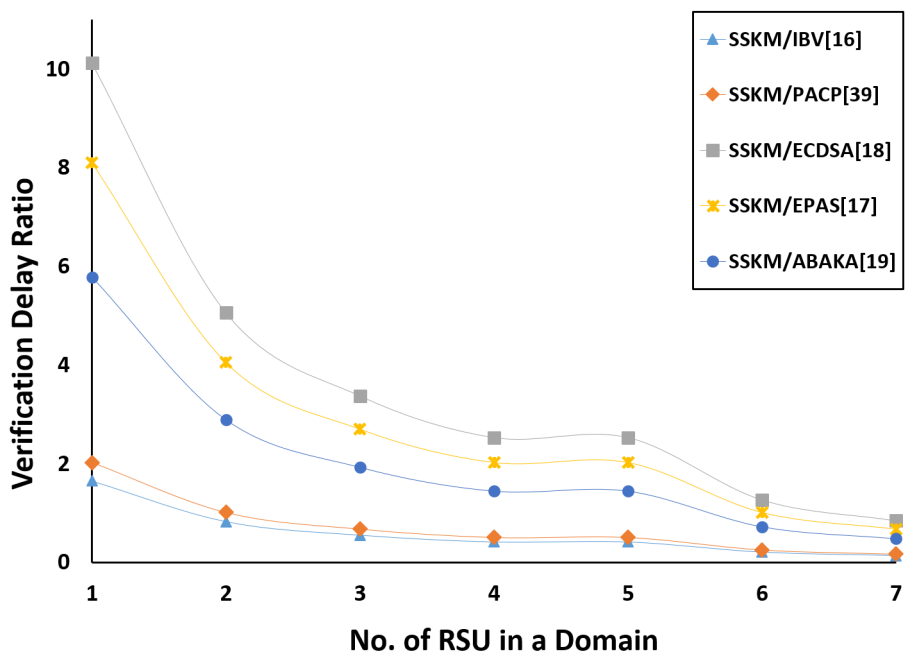

FIGURE 4.6: Verification Delay Ratio with multiple Schemes

Figure 4.6 shows the ratio of our scheme over other related schemes with respect to the verification time delay. As the domain can accommodate number of RSUs in our scheme, the ratio will keep decreasing as the number of RSU in the domain keep increasing. It can be seen that as the domain contains the 7 RSUs, the ratio of verification delay time is below one for all the schemes, that entails that the delay associated by our scheme is less than the other signature. Thus, with the increase in the domain size, the efficiency of our scheme also increase.

4.7 Conclusion

In this chapter, an efficient, scalable and secure key distribution scheme for group signature based authentication is proposed. The scheme provides the scalable solution for the security of the vehicular networking by using the concept of domain with multiple RSUs so that a group key can be utilized for a longer period of time. In addition, by

splitting the role of the RSU to member RSU and leader RSU, our approach provides the distributed key management mechanism. Furthermore, the scheme offers the secure key exchange protocol which allows that group keys can be securely delivered to vehicular nodes. Huge CRL size has been a concern in the VANET, through our approach, the utilization of the two bloom filter in a hierarchical topology allows the minimum CRL size that can be distributed in a small region so that efficient and effective CRL management and distribution is achieved. The possible security threats have been analyzed under and the performance is evaluated in NS-2. The experiment results show that our key distribution scheme is a scalable, efficient and secure solution to vehicular networking.

Chapter 5

Future Works

5.1 Introduction

In recent years, vehicular technology has taken its shape as smart vehicle systems and pilot assisted self-driving vehicles. There is a growing importance of vehicle-to-vehicle (V2V) communications as vehicles cooperatively share their traffic information (collected by sensors) with each other to improve driving safety, traffic efficiency and convenience [3, 74, 75]. In order to secure V2V communications, authentication has been carried out in the presence of the central trusted authority and infrastructures. The previous approach of authentication and revocation will not function in the infrastructure-less environment where only V2V communications are prevalent. All the modern/autonomous vehicles are well equipped with the multiple sensors and the sensor data can be utilized to verify the shared surrounding objects between the vehicles. If the shared objects are verified then the vehicles can be authenticated and the information can be shared and utilized such as certificate revocation list. Further, if the vehicle is faking its claimed position then the sensors can detect the malicious behavior and sensor data can be utilized as a testimony for the certificate revocation of the misbehaving vehicles.

5.2 ADAS Sensors

In efforts to improve the road safety and driving efficiency, modern vehicles have advanced driver-assistance systems (ADAS) [76], that senses the driving environment and warn the drivers if any immediate threats are found to minimize the human error. The advancement in the sensing technology and sensor fusion is leading the vehicles towards connected vehicles (CV) and fully autonomous vehicles.

Following are the elements of ADAS Sensors whose applications are shown in Figure 5.1 [77].

- RADAR(long range and short range): The radar system can identify objects from 15m up-to 150m. However, it cannot detect the object behind the large objects as signals are reflected (Eg: Pedestrians behind the large truck). Usage: range, object detection and classification, mapping, speed signs, blind spot detection etc.
- LiDAR: It increases the point cloud informational density, when the objects are close to the car itself. However, farther objects are hard to classify due to low information. Usage: range, object detection and classification, mapping, speed signs, blind spot detection etc.
- Camera: Visual information and storage of the surrounding.
- Ultra-Sound: The time taken of the reflection of ultrasonic sound wave provides the distance of the object.
- Thermal Imaging: It senses the imaging of camera in both daylight and night light conditions

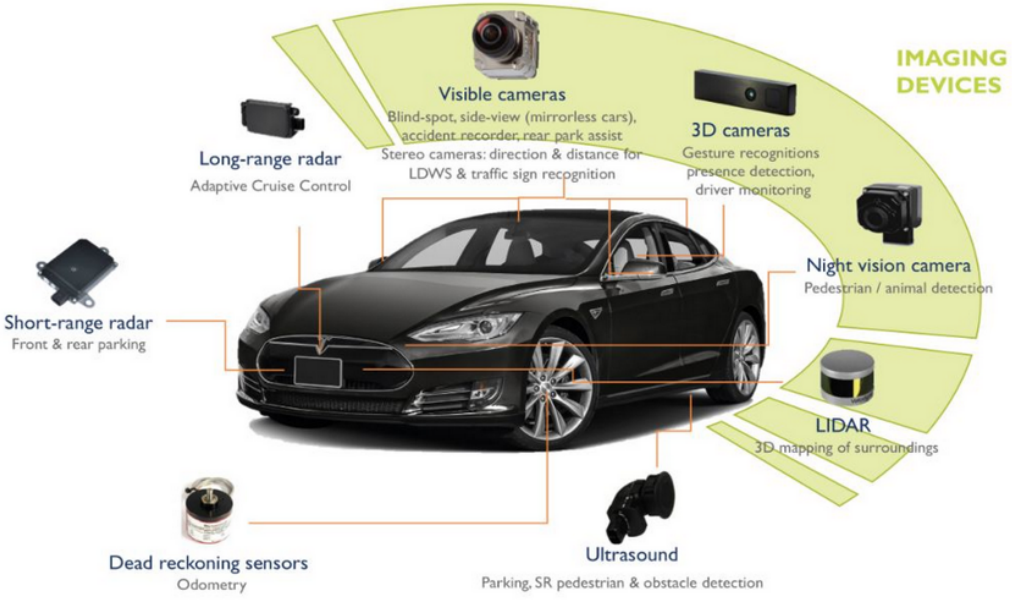

FIGURE 5.1: ADAS sensors and its application

5.3 Challenges with infra-structured VANETs

There is no doubt that the vehicular technology has taken its shape as smart vehicle systems and autonomous driving systems. The US Department of Transportation (DOT)

has conducted connected vehicle (CV) pilot deployment program [78] for real-world feasibility. However, it is likely to take some time to fully deploy the infrastructure. Further, in rural area context, V2V will be dominant over V2I. We have discussed about the approach of performing the authentication and certificate revocation in the hierarchical VANETs. Figure 5.2 shows the authentication in two scenario i.e. scenario 1 with infrastructure and scenario 2 without infrastructure.

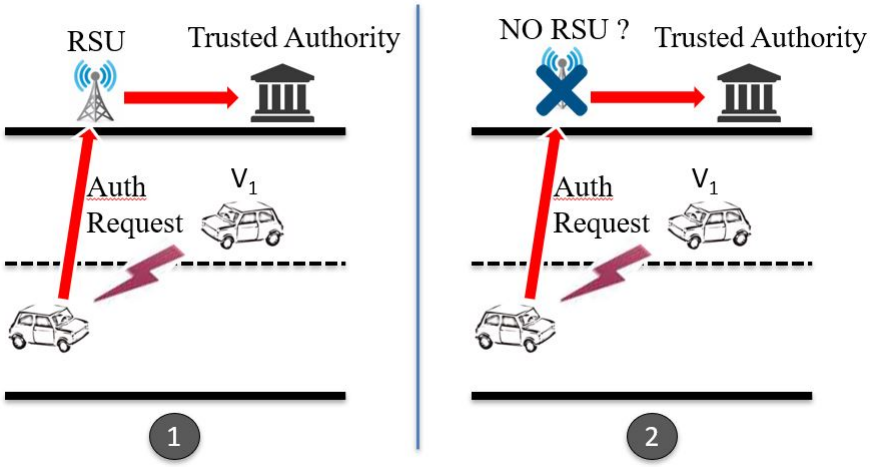

FIGURE 5.2: Scenario 1: Infrastructure Vs Scenario 2: Infrastructure-less VANETs

5.4 Authentication in infrastructure-less VANETs

To address the above issue, the future will be utilizing the sensor data that can provide the fingerprint of the surrounding objects and can be utilized to match the existence of the target vehicle in the proximity of the periphery. This method will utilize the existing sensors of the vehicles without the additional hardware cost. This method will not require PKI certificates for authentication which will beneficial as the huge packet size is one of the drawback of PKI system. The proposed model for authentication in an infrastructure-less VANETs is shown in Figure 5.3. The sensor data from the Lidar, Radar, Camera and ultrasonic sensors will be fused together to increase the accuracy and efficiency of the authentication algorithm.

5.5 Conclusion

Infrastructures for vehicular communication are not readily available yet, even though self-driving vehicles are cruising on the roads. Therefore, and an alternative solution is

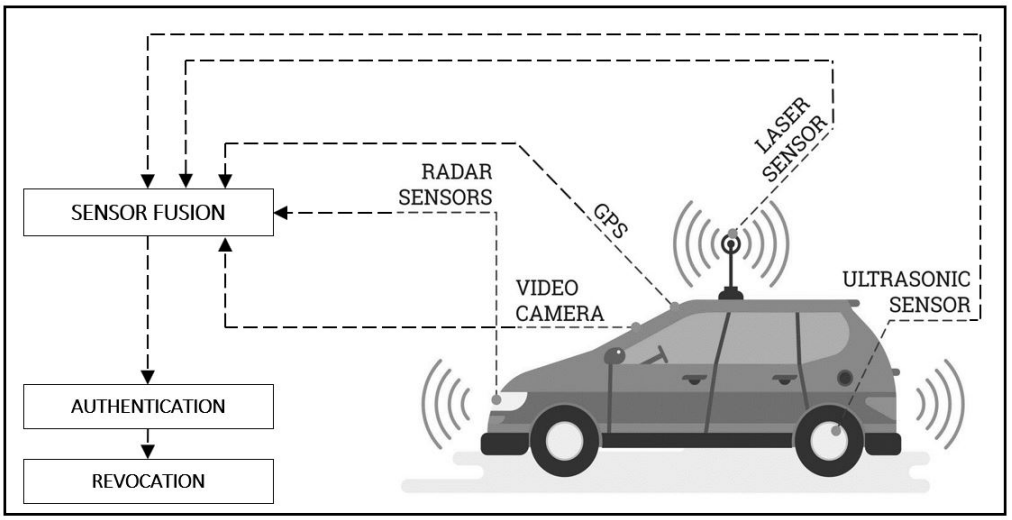

FIGURE 5.3: sensor fusion for authentication in infrastructure-less VANETs

necessary to support the areas where the infrastructure is not available. To authenticate the vehicles in the infrastructure-less environment, both vehicles has to detect the surrounding objects and agree that the vehicles are present in the claimed location. The sensor-fused data can be combination of the point cloud image mapping of the object (lidar image) with the image from the camera and distance from the ultra-sonic sensors or radar. After performing the similarity of the locality information of the objects, vehicles can be authenticated.

Appendix A

An Appendix

A.1 NS-2 Vehicle Mobility Sample Code

```
set ns [new Simulator]
# Create a nam trace datafile.
set namfile [open AODV_final.nam w]

set Time [open time.tr w]
set TIME_start [clock clicks -milliseconds]
# *** Throughput Trace ***
#This Block Is For Congestion Window Trace file. Here 25
   sample trace file
set cwnd1 [open cwnd1.tr w]
set cwnd2 [open cwnd2.tr w]
set cwnd3 [open cwnd3.tr w]
set cwnd4 [open cwnd4.tr w]
set cwnd5 [open cwnd5.tr w]

#This Block Is For Bandwidth Calculation Trace file. Here 25
   sample trace file
set b1 [open b1.tr w]
set b2 [open b2.tr w]
set b3 [open b3.tr w]
set b4 [open b4.tr w]
set b5 [open b5.tr w]

$ns namtrace-all $namfile
```

```
# ----- Setup wireless environment. ----
set wireless_tracefile [open AODV_final.trace w]
set topography [new Topography]
$ns trace-all $wireless_tracefile
$ns namtrace-all-wireless $namfile 3000  1600
$topography load_flatgrid 3000  1600

#TN means Total number of  wireless node
global TN
set TN 100
set god_ [create-god $TN]
#global node setting
$ns node-config -adhocRouting AODV \
                     -llType LL \
                     -macType Mac/802_11\
                     -ifqLen 100 \
                     -ifqType Queue/DropTail/PriQueue \
                     -antType Antenna/OmniAntenna \
                     -propType Propagation/TwoRayGround \
                     -phyType Phy/WirelessPhy \
                     -channel [new Channel/WirelessChannel] \
                     -topoInstance $topography \
                     -agentTrace ON \
                     -routerTrace ON \
                     -macTrace ON \
             -movementTrace ON

# Create wireless nodes.

#Here X and Y is the axes
set x1 160
set y1 150
set x2 350
set y2 200
.
.
.

#Setting node position block
```

```
        for {set i 0} {$i < $TN} {incr i} {
            set node($i) [$ns node]
            $node($i) random-motion 0
            $ns at 0.0 "$node($i) label Node_($i)"
            $ns initial_node_pos $node($i) 50.000000
        }
        for {set j 0} {$j < $TN} {incr j} {

            set Tcp($j) [new Agent/TCP]
            $ns attach-agent $node($j) $Tcp($j)
            $ns color 1 "black"
            $Tcp($j) set fid_ $j
            $Tcp($j) set packetSize_ 512
            $Tcp($j) set window_ 20
            $Tcp($j) set windowInit_ 1
            $Tcp($j) set maxcwnd_ 0
            #Set TCPSink
            set TcpSink($j) [new Agent/TCPSink]
            $ns attach-agent $node($j) $TcpSink($j)
            $TcpSink($j) set packetSize_ 210
            #Set Trafic Source

            set Ftp($j) [new Application/FTP]
            $Ftp($j) attach-agent $Tcp($j)
            $Ftp($j) set maxpkts_ 2048
        }

#Animate Few of node
$ns at 10.000000 "$node(0) setdest 160 450 75"
$ns at 10.000000 "$node(1) setdest 343.017365 158.321411
   12.667036"
$ns at 10.000000 "$node(2) setdest 943.017365 58.321411
   16.667036"
$ns at 4.000000 "$node(3) setdest 2755 360 20"
$ns at 10.000000 "$node(4) setdest 960 1320 10"
$ns at 10.000000 "$node(5) setdest 343.017365 258.321411
   11.667036"

#Connect Source to destination
```

```
$ns connect $Tcp(0) $TcpSink(15)
$ns connect $Tcp(1) $TcpSink(25)
$ns connect $Tcp(16) $TcpSink(41)
$ns connect $Tcp(31) $TcpSink(42)
$ns connect $Tcp(46) $TcpSink(7)

# Traffic Source actions.
$ns at 0.020000 "$Ftp(0) start"
$ns at 0.020000 "$Ftp(1) start"
$ns at 0.020000 "$Ftp(16) start"
$ns at 0.020000 "$Ftp(31) start"
$ns at 0.020000 "$Ftp(46) start"


#Custom Proc To get time
    proc getTime {file} {
        global ns
        set time 0.2
        set now [$ns now]
        puts $file "$now"
        #Re Call
        $ns at [expr $now + $time] " getTime $file"
    }

    $ns at 0.0 "getTime $Time"

#Custom Proc To calculate congestion window
    proc calcCwnd {tcpSource file} {
        global ns
        set time 0.2
        set now [$ns now]
        set cwnd [$tcpSource set cwnd_]
        puts $file "$cwnd"
        #Re Call
        $ns at [expr $now + $time] " calcCwnd $tcpSource
           $file"
    }

#Custom Proc To calculate Bandwidth
```

```
    proc calcByte {sink file} {
        global ns
        set time 0.2
        set bw0 [$sink set bytes_]
        set now [$ns now]
        puts $file " [expr {$bw0 / $time * 8 / 1000000}] "
        #Reset
        $sink set bytes_ 0
        #Re Call
        $ns at [expr $now + $time] "calcByte $sink  $file "
     }

# Run the simulation
proc finish {} {
        global ns namfile
        $ns flush-trace
        close $namfile

# Mobility generations
$node_(0) set X_ 1660.21
$node_(0) set Y_ 1887.04
$node_(0) set Z_ 0
$ns_ at 0.0 "$node_(0) setdest 1660.21 1887.04 0.00"
$ns_ at 1.0 "$node_(0) setdest 1659.96 1888.46 1.44"
$node_(1) set X_ 2046.02
$node_(1) set Y_ 1177.89
$node_(1) set Z_ 0
$ns_ at 1.0 "$node_(1) setdest 2046.02 1177.89 0.00"
$ns_ at 2.0 "$node_(0) setdest 1659.42 1891.53 3.12"
$ns_ at 2.0 "$node_(1) setdest 2046.83 1175.48 2.54"
$node_(2) set X_ 4567.59
$node_(2) set Y_ 2539.32
$node_(2) set Z_ 0
$ns_ at 2.0 "$node_(2) setdest 4567.59 2539.32 0.00"
$ns_ at 3.0 "$node_(0) setdest 1658.55 1896.53 5.08"
$ns_ at 3.0 "$node_(1) setdest 2048.22 1171.33 4.37"
$ns_ at 3.0 "$node_(2) setdest 4565.21 2538.41 2.54"
$node_(3) set X_ 694.62
$node_(3) set Y_ 3006.37
```

```
$node_(3) set Z_ 0
$ns_ at 3.0 "$node_(3) setdest 694.62 3006.37 0.00"
$ns_ at 4.0 "$node_(0) setdest 1657.39 1903.14 6.71"
$ns_ at 4.0 "$node_(1) setdest 2050.35 1165.03 6.65"
$ns_ at 4.0 "$node_(2) setdest 4561.07 2536.82 4.43"
$ns_ at 4.0 "$node_(3) setdest 693.96 3004.88 1.63"
$node_(4) set X_ 2606.42
$node_(4) set Y_ 2377.78
$node_(4) set Z_ 0
```

A.2 SUMO mobility generator–manhattan vehicle model

LISTING A.1: bash version, xml implement, and python to create tracefile

```
$polyconvert --osm-files  manhattan.net.xml --type-file
   osmPolyconvert.typ.xml -o manhattan.poly.xml

$python /usr/local/src/sumo-0.25.0/tools/randomTrips.py -n
   manhattan.net.xml -r manhattan.rou.xml -e 50 -l

<------manhattan.sumo.cfg---------->
<configuration>
        <input>
                <net-file value="manhattan.net.xml"/>
<route-files value="manhattan.rou.xml"/>
                <additional-files value="manhattan.poly.xml"/
                   >
        </input>

<time>
<begin value="0"/>
<end value="100"/>
<step-length value="0.1"/>
</time>
</configuration>

$sumo-gui manhattan.sumo.cfg
```

```
$sumo -c manhattan.sumo.cfg --fcd-output manhattan.sumo.xml

$python /usr/local/src/sumo-0.25.0/tools/traceExporter.py --
   fcd-input manhattan.sumo.xml --ns2config-output manhattan.
   tcl --ns2mobility-output mobility.tcl --ns2activity-output
    activity.tcl
```

Bibliography

[1] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. Security in vehicular ad hoc networks. *IEEE communications magazine*, 46 (4), 2008.

[2] Panos Papadimitratos, Arnaud De La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *IEEE Communications Magazine*, 47(11), 2009.

[3] Hannes Hartenstein and Kenneth Laberteaux. *VANET vehicular applications and inter-networking technologies*, volume 1. John Wiley & Sons, 2009.

[4] Giuseppe Bianchi. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on selected areas in communications*, 18(3):535–547, 2000.

[5] IEEE Standard 1609.2. Standard for wireless access in vehicular environments–security services for applications and management messages. *IEEE Xplore*, pages 1–240, 2016.

[6] Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040. IEEE, 2008.

[7] Aymen Sassi, Faiza Charfi, Lotfi Kamoun, Yassin Elhillali, and Atika Rivenq. Ofdm transmission performance evaluation in v2x communication. *arXiv preprint arXiv:1410.8039*, 2014.

[8] AM Abdelgader and Wu Lenan. The physical layer of the ieee 802.11 p wave communication standard: the specifications and challenges. In *Proceedings of the world congress on engineering and computer science*, volume 2, page 71, 2014.

[9] *IEEE Std 1609.4-2016 (Revision of IEEE Std 1609.4-2010): IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation*. IEEE, 2016. URL https://books.google.com/books?id=D9UtnQAACAAJ.

[10] Stephan Eichler. Performance evaluation of the ieee 802.11 p wave communication standard. In *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pages 2199–2203. IEEE, 2007.

[11] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[12] Jesús Téllez Isaac, Sherali Zeadally, and José Sierra Camara. Security attacks and solutions for vehicular ad hoc networks. *IET communications*, 4(7):894–903, 2010.

[13] Khaled Rabieh, Mohamed MEA Mahmoud, Marianne Azer, and Mahmoud Allam. A secure and privacy-preserving event reporting scheme for vehicular ad hoc networks. *Security and Communication Networks*, 8(17):3271–3281, 2015.

[14] Ajay Rawat, Santosh Sharma, and Rama Sushil. Vanet: Security attacks and its possible solutions. *Journal of Information and Operations Management*, 3(1):301, 2012.

[15] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7–20, 2017.

[16] Tim Leinmuller, Robert K Schmidt, Elmar Schoch, Albert Held, and Gunter Schafer. Modeling roadside attacker behavior in vanets. In *GLOBECOM Workshops, 2008 IEEE*, pages 1–10. IEEE, 2008.

[17] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. Vanet security surveys. *Computer Communications*, 44:1–13, 2014.

[18] Frank Kargl, Zhendong Ma, and Elmar Schoch. Security engineering for vanets. In *4th Workshop on Embedded Security in Cars (escar 2006)*. Citeseer, 2006.

[19] Subir Biswas and Jelena Misic. Proxy signature-based rsu message broadcasting in vanets. In *Proceedings of the 25th Biennial Symposium on Communications (QBSC)*, pages 5–9. IEEE Kingston, ON, 2010.

[20] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of computer security*, 15(1):39–68, 2007.

[21] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in vanets. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37. ACM, 2004.

[22] Ashwin Rao, Ashish Sangwan, Arzad A Kherani, Anitha Varghese, Bhargav Bellur, and Rajeev Shorey. Secure v2v communication with certificate revocations. In *2007 Mobile Networking for Vehicular Environments*, pages 127–132. IEEE, 2007.

[23] Bryan Parno and Adrian Perrig. Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)*, pages 1–6. Maryland, USA, 2005.

[24] Yi Qian and Nader Moayeri. Design of secure and application-oriented vanets. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2794–2799. IEEE, 2008.

[25] Hassan Takabi, James BD Joshi, and Gail-Joon Ahn. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, (6):24–31, 2010.

[26] Peter Yee. Updates to the internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, RFC5280. 2013.

[27] Matthias Gerlach. Assessing and improving privacy in VANETs. *ESCAR, Embedded Security in Cars*, 2006.

[28] Xiaoting Sun, Xiaodong Lin, and P-H Ho. Secure vehicular communications based on group signature and id-based signature scheme. In *Proceedings of IEEE ICC International Conference, 2007.*, pages 1539–1545. IEEE, 2007.

[29] Sushmita Ruj, Marcos A Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. On data-centric misbehavior detection in vanets. In *Vehicular technology conference (VTC Fall), 2011 IEEE*, pages 1–5. IEEE, 2011.

[30] Rasheed Hussain, Sangjin Kim, and Heekuck Oh. Privacy-aware vanet security: Putting data-centric misbehavior and sybil attack detection schemes into practice. In *International Workshop on Information Security Applications*, pages 296–311. Springer, 2012.

[31] Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. X. 509 internet public key infrastructure online certificate status protocol-ocsp. Technical report, 1999.

[32] Jason J Haas, Yih-Chun Hu, and Kenneth P Laberteaux. Efficient certificate revocation list organization and distribution. *IEEE Journal on Selected Areas in Communications*, 29(3):595–604, 2011.

[33] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in vanets. In *in Proceedings of European Workshop on Security in Ad-hoc and Sensor Networks*, pages 129–141. Springer, 2007.

[34] U.S. Department of Justice. Federal bureau of investigation, 2018. URL https://www.iii.org/fact-statistic/facts-statistics-auto-theft.

[35] Giovanni Rigazzi, Andrea Tassi, Robert J Piechocki, Theo Tryfonas, and Andrew Nix. Optimized certificate revocation list distribution for secure V2X communications. *arXiv preprint arXiv:1705.06903*, 2017.

[36] Panagiotis Panos Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux. Certificate revocation list distribution in vehicular communication systems. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, pages 86–87. ACM, 2008.

[37] Haoyu Song, Sarang Dharmapurikar, Jonathan Turner, and John Lockwood. Fast hash table lookup using extended bloom filter: an aid to network processing. *ACM SIGCOMM Computer Communication Review*, 35(4):181–192, 2005.

[38] Tat Wing Chim, Siu-Ming Yiu, Lucas CK Hui, and Victor OK Li. SPECS: Secure and privacy enhancing communications schemes for vanets. *Ad Hoc Networks*, 9(2): 189–203, 2011.

[39] Gao Ying and Zhan Jiang. Research on crl distribution in P2P systems. In *Proceedings of Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 574–577. IEEE, 2009.

[40] Khaled Rabieh, Mohamed MEA Mahmoud, Kemal Akkaya, and Samet Tonyali. Scalable certificate revocation schemes for smart grid ami networks using bloom filters. *IEEE Transactions on Dependable and Secure Computing*, 14(4):420–432, 2017.

[41] Kiho Lim, Kastuv M Tuladhar, Xiwei Wang, and Weihua Liu. A scalable and secure key distribution scheme for group signature based authentication in vanet. In *Proceedings of the 8th IEEE Ubiquitous Computing, Electronics & Mobile Communication Conference IEEE UEMCON*. IEEE, 2017.

[42] Kiho Lim and Kastuv M Tuladhar. Trajectory based pre-key exchange scheme for seamless vehicular networks connectivity. In *Proceedings of the 15th Consumer Communications & Networking Conference (IEEE CCNC)*, pages 1–5. IEEE, 2018.

[43] Sholom S Rosen. Tamper-proof electronic processing device, July 11 2000. US Patent 6,088,797.

[44] Mingzhong Wang, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang. LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication. *Computing*, 98(7):685–708, 2016.

[45] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and Jean-Pierre Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8), 2007.

[46] Rongxing Lu, Xiaodong Lin, Tom H Luan, Xiaohui Liang, and Xuemin Shen. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Transactions on Vehicular Technology*, 61(1):86–96, 2012.

[47] The Statistics Portal. U.S. vehicle registrations, 2018. URL https://www.statista.com/statistics/199974/us-car-sales-since-1951/.

[48] David Chaum and Eugène Van Heyst. Group signatures. In *Advances in CryptologyâĂŤEUROCRYPTâĂŹ91*, pages 257–265. Springer, 1991.

[49] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *Crypto*, volume 3152, pages 41–55. Springer, 2004.

[50] Yong Hao, Yu Cheng, Chi Zhou, and Wei Song. A distributed key management framework with cooperative message authentication in vanets. *IEEE Journal on selected areas in communications*, 29(3):616–629, 2011.

[51] Tat Wing Chim, Siu-Ming Yiu, Lucas CK Hui, and Victor OK Li. VSPN: VANET-based secure and privacy-preserving navigation. *IEEE Transactions on Computers*, 63(2):510–524, 2014.

[52] Rongxing Lu, Xiaodong Lin, Haojin Zhu, P-H Ho, and Xuemin Shen. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In *Proceeding of IEEE INFOCOM 27th Conference on Computer Communications, 2008.*, pages 1229–1237. IEEE, 2008.

[53] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[54] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. Mix-zones for location privacy in vehicular networks. In *Proceedings of ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, number LCA-CONF-2007-016, 2007.

[55] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing wireless location privacy using silent period. In *Proceedings of Wireless Communications and Networking Conference, 2005 IEEE*, volume 2, pages 1187–1192. IEEE, 2005.

[56] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran. AMOEBA: robust location privacy scheme for VANET. *IEEE Journal on Selected Areas in Communications*, 25(8), 2007.

[57] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, P-H Ho, and Xuemin Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 246–250. IEEE, 2008.

[58] Xuedan Jia, Xiaopeng Yuan, Lixia Meng, and Liang-min Wang. Epas: Efficient privacy-preserving authentication scheme for vanets-based emergency communication. *JSW*, 8(8):1914–1922, 2013.

[59] Kalkundri Ravi and SA Kulkarni. A secure message authentication scheme for vanet using ecdsa. In *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*, pages 1–6. IEEE, 2013.

[60] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien. Abaka: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 60(1):248–262, 2011.

[61] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in vanet. In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pages 19–28. ACM, 2007.

[62] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin Shen, and Jinshu Su. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Transactions on Vehicular Technology*, 59(7):3589–3603, 2010.

[63] Jinhua Guo, John P Baugh, and Shengquan Wang. A group signature based secure and privacy-preserving vehicular communication framework. In *2007 Mobile Networking for Vehicular Environments*, pages 103–108. IEEE, 2007.

[64] Yong Hao, Yu Cheng, and Kui Ren. Distributed key management with protection against rsu compromise in group signature based vanets. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, 2008.

[65] Kiho Lim and D Manivannan. An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. *Vehicular Communications*, 4:30–37, 2016.

[66] Maxim Raya, Panagiotis Papadimitratos, Virgil D Gligor, and J-P Hubaux. On data-centric trust establishment in ephemeral ad hoc networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages 1238–1246. IEEE, 2008.

[67] Ronald L Rivest and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393–394, 1984.

[68] NS-2. http://nsnam.sourceforge.net/wiki/index.php.

[69] simulation of urban mobility. http://sumo.dlr.de/index.html.

[70] Insurance Institute of highway safety. http://www.iihs.org/iihs/sr/statusreport/article/43/1/1, Jan 2008.

[71] Mike Scott. Efficient implementation of cryptographic pairings. In *Online]. http://www. pairing-conference. org/2007/invited/Scott slide. pdf*, 2007.

[72] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for fr-reduction. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 84(5):1234–1243, 2001.

[73] Dijiang Huang, Satyajayant Misra, Mayank Verma, and Guoliang Xue. Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets. *IEEE Transactions on Intelligent Transportation Systems*, 12(3):736–746, 2011.

[74] Todd Litman. *Autonomous vehicle implementation predictions*. Victoria Transport Policy Institute Victoria, Canada, 2017.

[75] M Mitchell Waldrop et al. No drivers required. *Nature*, 518(7537):20, 2015.

[76] Olaf Gietelink, Jeroen Ploeg, Bart De Schutter, and Michel Verhaegen. Development of advanced driver assistance systems with vehicle hardware-in-the-loop simulations. *Vehicle System Dynamics*, 44(7):569–590, 2006.

[77] Yole DÃľveloppement. Mems and sensors development, 2018. URL http://www.yole.fr/index.aspx.

[78] U.S. Department of Transportation. Intelligent transportation systems, 2018. URL https://www.its.dot.gov/pilots.