On Board Unit Based Authentication for V2V Communication in VANET

Saroj Kumar Biswal

Department of Computer Science and Engineering
National Institute of Technology
Rourkela – 769008, India

On Board Unit Based Authentication for V2V Communication in VANET

Dissertation submitted in

May 2014

to the department of

Computer Science and Engineering

of

National Institute of Technology, Rourkela

in partial fulfillment of the requirements

for the degree of

Master of Technology

(Specialiazation in Information Security)

by

Saroj Kumar Biswal

(Roll 212CS2364)

under the supervision of

Prof. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology

Rourkela – 769008, India

Dedicated to my Parents and the Almighty GOD..

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769008, India. www.nitrkl.ac.in

May , 2014

Certificate

This is to certify that the work in the thesis entitled *On Board Unit Based Authentication for V2V Communication in VANET* by *Saroj Kumar Biswal*, bearing roll number 212CS2364, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* with specialization of *Information Security* in *Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Prof. Ashok Kumar Turuk
Computer Science and Engineering, NIT Rourkela

Acknowledgement

This dissertation, though an individual work, has benefited in various ways from several people. Whilst it would be simple to name them all, it would not be easy to thank them enough.

The enthusiastic guidance and support of Prof. Ashok Kumar Turuk inspired me to stretch beyond my limits. His profound insight has guided my thinking to improve the final product. My solemnest gratefulness to him.

I am very much grateful to Prof. Sanjay Kumar Jena and Prof. Banshidhar Majhi for his ceaseless support throughout my research.

I am also obliged to all the Professors of Computer Science Department for their recommendation and wise remarks at diverse phases of this thesis work that were really thought provocative.

Many thanks to my fellow research colleagues. It gives me a sense of happiness to be with you all. Special thanks to SriChandan Sir, Biswajit, Rohit, Biswojit and Sourav whose support gave a new breath to my research.

Above all, this would not have been possible without the love and affection of my family. This thesis work is dedicated to my family , who have been a consistent source of love, affection, support and strength all these years. I would like to express my heart-felt gratitude to them. There have been ups and there have been downs and the cycle is likely to continue.

Saroj Kumar Biswal

saroj25kumar@gmail.com

Author's Declaration

I, Saroj Kumar Biswal bearing Roll No 212CS2364 understand that plagiarism is defined as any one or the combination of the following

1. Uncredited verbatim copying of individual sentences, paragraphs or illustrations (such as graphs, diagrams, etc.) from any source, published or unpublished, including the internet.

2. Uncredited improper paraphrasing of pages or paragraphs (changing a few words or phrases, or rearranging the original sentence order).

3. Credited verbatim copying of a major portion of a paper (or thesis chapter) without clear delineation of who did or wrote what.(Source: IEEE, the Institute, Dec. 2004)

I have verified that all the thoughts, declarations, charts, outlines,etc., that are not an after-effect of my work, are credited properly. Long expressions or sentences that must be used verbatim from published literature have been clearly recognized using quotation marks.

I affirm that no part of my work could be considered as written falsification and I assume full responsibility if such a dissension happens. I understand completely well that the guide of the thesis may not be in a position to check for the likelihood of such incidences of counterfeiting in this work..

Saroj Kumar Biswal
Roll No: 212CS2364
Department of Computer Science and Engineering

Abstract

The recent developments in wireless communication technologies along with the plummeting costs of hardware allow both V2V and V2I communications for information exchange. Such a network is called Vehicular ad Hoc Network (VANET) which is very important for various road safety and non-safety related applications. However, Due to the wireless nature of communication in VANETs, it is also prone to various security attacks which are originally present in wireless networks. Hence to realize the highest potential of VANET, the network should be free from attackers, there by all the information exchanged in the network must be reliable i.e. should be originated from authenticated source.

However, authentication of vehicles using a PKI based architecture which is mostly based on V2I communication and solely depends on Road side Units, might fail in case of absence of proper infrastructure. Moreover PKI based solutions incur more communication overhead due to repeated connections with the Trusted Authority every time you want to authenticate a vehicle.

Hence, this thesis work gives an OBU based authentication mechanism which allows the vehicle to authenticate each other for V2V communication when there is lack of proper infrastructure. Here each vehicle is capable of generating a pair of self-certified public/private key pair which can be verified by any other vehicle using a predefined secret key given by Trusted Authority. The grouping concept used in order to lower the communication overheads. The Vehicle in close proximity of each other form a group and select a group leader, who is then responsible for generating a group public and private key pair for communication with group leader. A vehicle can obtain the group key by authenticating itself to the group leader.

Our proposed scheme also preserves the privacy of the vehicle but can reveal the identity in liability issues. The security analysis of the proposed scheme shows that it can indeed operate with limited support of infrastructure and can become a fully self-organized system.

***Keywords*:** VANET, V2V communications, security, authentication, vehicular communication

Contents

Certificate iii

Acknowledgement iv

Declaration v

Abstract vi

List of Figures x

List of Tables xi

Acronyms xii

1 Introduction 1

1.1 VANET Overview 2

1.1.1 Intelligent Transportation System 2

1.1.2 Vehicle to Vehicle Communication 4

1.1.3 Vehicle to Infrastructure Communication 4

1.1.4 Routing Based Communication 4

1.2 Distinguished Features of VANET 5

1.3 Applications of VANET 6

1.4 Communication Standards for VANET 6

1.4.1 Dedicated Short Range Communication (DSRC) 6

1.4.2 Wireless Access in Vehicular Environment (WAVE) (IEEE 1609.11p) 7

1.5 Components Needed for VANET Security Architecture 8
1.5.1 Event Data Recorder (EDR) 8
1.5.2 Trusted Component (TC) 8
1.5.3 Electronic Licence Plate (ELP) 8
1.5.4 Vehicular Public Key Infrastructure (VPKI) 8
1.5.5 Authentication 9
1.5.6 Privacy 9
1.5.7 Secure Positioning 9
1.6 Security Threats to VANET 9
1.6.1 Threats to Availability 10
1.6.2 Threats to Authenticity 11
1.6.3 Threats to Confidentiality 11
1.6.4 Threat to Privacy 12
1.7 Challenges towards security of VANET 12
1.8 VANET Projects Across the World 13
1.8.1 In European Union 14
1.8.2 In USA 14
1.8.3 In Japan 15
1.9 Motivation 16
1.10 Objective 16
1.11 Organization of Thesis 17

2 Literature Review **18**
2.1 Literature Review 18
2.1.1 RSU Based Authentication 18
2.1.2 Pseudonym Based Authentication 19
2.1.3 Group Based Authentication 19
2.2 Summary 20

3 On Board Unit Based Authentication for V2V Communication in VANET **21**

3.1 Network Model 22
3.2 Assumptions 22
3.3 Notation 23
3.4 Generation of Check Value 24
3.5 Generation of Anonymous public/private Key pairs 24
3.6 Authentication 25
3.7 Summary 26

4 Experiment and Results **27**
4.1 Authentication by Group Leader 27
4.2 Privacy 28
4.3 Group joining and leaving 28
4.4 Summary 29

5 Conclusion and Future Work **31**

List of Figures

1.1 Intelligent Transportation System 3
1.2 DSRC Bandwidth Allocation [8] 6
1.3 WAVE protocol Stack [8] 7
1.4 Recent Projects in European Union, USA and Japan. 15

List of Tables

3.1 Notations 23

4.1 Summary of Characteristics of Various schemes discussed in literature and our proposed scheme 30

Acronyms

Acronym	Description
VANET	Vehicular Ad-hoc Network
OBU	On Board Unit
RSU	Road Side Unit
PKI	Public Key Infrastructure
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
ELP	Electronic License Plate
TC	Trusted Component
TA	Trusted Authority
SHA	Secure Hash Algorithm

Chapter 1

Introduction

The vehicular ad hoc network (VANET) is a kind of wireless ad hoc network which deploys the concept of continuous varying vehicular motion. Here, the moving vehicles act as nodes. It is an active area research right now and emerging type of network aimed at improving safe driving, traffic optimization and some other services through vehicle to infrastructure communication (V2I) or vehicle to vehicle communication (V2V). It plays an important part in intelligent transportation system (ITS) [18] which is described in section1.1.1 Each vehicle communicate send and receive messages by On Board Unit (OBU) and equipped with Event Data Recorder, GPS, Trusted component etc. The Roadside Units (RSU) are responsible for broadcasting safety messages periodically.

With recent advances in the development of Wireless communications protocols and plummeting costs of hardware needed, along with the automobile industrys desire to increase road safety and gain competitive edge in the market , Vehicles are equipped with latest communication hardwares, GPS etc. hence becoming Computers on Wheels or computers networks on wheels [1]

But wireless communication is itself susceptible to various attacks, hence the security of VANET cannot be undermined. Some malicious vehicle may send false information into the network to gain unfair advantage on the road or to cause serious accidents. Hence the sender vehicles should be authenticated by the receiver before taking any action based on the received safety message. Normally origin authentication is provided by digital signature with the help of certification services. In VANET, a Trusted Authority (TA) serves the purpose, but it involves huge communication over-head and also a vehicle have to communicated with TA

via RSUs. Now RSUs are fixed infrastructures along the road, which periodically broadcast safety related information, Typically RSUs placed over every 300m to 1 km and they broadcast at the interval of every 300ms. Hence placing RSUs along a long highway to provide omnipresent infrastructure is not feasible economically for now. Hence vehicle should be able to authenticate others with limited help from TA or fixed infrastructure. Also in VPKI, the public keys are bound to identity of the vehicles in certificates, hence an eavesdropper may track the sending vehicle, but we need to protect the privacy as well.

Hence in our research, we propose an OBU based authentication scheme for V2V communication, where the vehicles generate self-certified public/private key pairs with the help of a check value computed by TA and initially given to Vehicles during registration. The Check value is computed via one way hash chaining mechanism. The same check value is given to multiple vehicles in order to achieve privacy. But a tracking hint is attached to all the sent messages by default, which can later be used to identify a vehicle. Also group formation is done, so that all the vehicles send their messages to Group leader, then the Group leader sends the aggregated message to all for reducing communication overhead. Our research is solely focused on authentication of vehicles, hence it is possible that an legitimate vehicle of the network i.e. authenticated vehicle may send false information with malicious intent. Hence in that case, reliability of messages comes into scene, which is beyond the scope of our research. But We assume that vehicle do evaluate reliability of messages using existing optimal schemes, which can later be used for revocation purpose.

The rest of the thesis is organized as follows. The introduction of VANET, its overview, various security aspects are given in Section 1. Some existing methods in literature are discussed in Section 2. The proposed scheme and its various aspects are given in section 3. In section4, we analyze the performance and security aspects of our proposed scheme.Finally Section 5 concludes the thesis.

1.1 VANET Overview

1.1.1 Intelligent Transportation System

In ITS, each vehicle acts as sender, receiver and router to broadcast the information to the vehicular network or transportation agency, which then used

the information to ensure safe, free-flow of traffic. The vehicles must be configured with On Board Units (OBU), and the Road Side Units (RSU) must be present at fixed intervals for communication to occur. RSUs are connected to the backbone network which is assumed to be secure and free from security attacks. RSUs and Trusted Authority (TA) are static in nature and together forms the fixed infrastructure. The number and distribution of RSUs depends on the communication protocol to be used. The possible configurations in ITS are vehicle to vehicle, vehicle to infrastructure and routing based communications [3] the following figure 1.1 depicts a typical ITS.

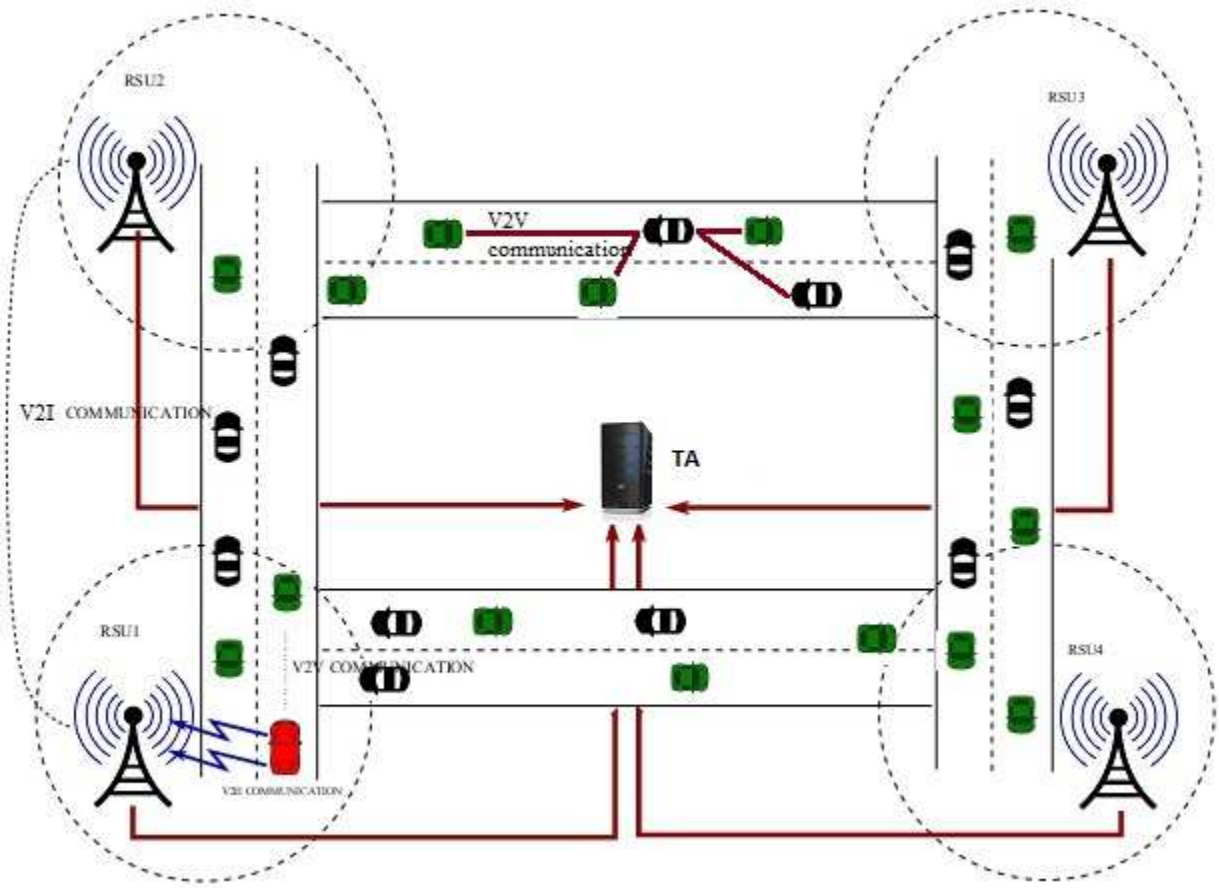

Figure 1.1: Intelligent Transportation System

1.1.2 Vehicle to Vehicle Communication

It is multi-hop multicast/broadcast communication used to transmit traffic related information over multiple hops to a group of receivers. ITS is generally concerned with the road ahead and not on the road behind. ITS mainly used two types of message forwarding techniques, Nave Broadcasting and Intelligent Broadcasting [3].

- Naive Broadcasting : believes in periodic broadcasting of messages at regular intervals. If the message comes from behind then the vehicle ignores the message, but if the message comes from a vehicle ahead then the receiving vehicle send its own broadcast message to the vehicles behind it. The limitations of naive broadcasting method is that large numbers of broadcast messages are generated, hence increases network overhead.

- Intelligent Broadcasting : overcomes the above limitation by using acknowledgements, hence limiting the number of message broadcasts. If the event-detecting vehicle receives the same message from behind it, it assumes that at least one vehicle in the back has received it and will be responsible for further transmitting the message. Hence it ceases broadcasting.In our research, we are mostly focusing on V2V communication only.

1.1.3 Vehicle to Infrastructure Communication

Also known as V2I communication. here the Road Side Unit (RSU) broadcasts message to the vehicles in the vicinity. This type of configuration provides ample amount of bandwidth link between communicating parties. Mostly used for traffic optimization messages.

1.1.4 Routing Based Communication

Its a multi-hop unicast method where a message is transmitted in a multi-hop fashion until it reaches the desired vehicle. It is combination of both V2V and V2I communication. Mostly used for both safety and non-safety message transmission, infotainment services etc.

1.2 Distinguished Features of VANET

Vehicular ad hoc Network (VANET) is a unique kind of MANET where the nodes are mobile vehicles. The similarity between these two networks is characterized by the movement and self organization of nodes. But the main difference between VANET and MANET is, the nodes move in random but predictable manner but at much higher speeds in VANET. The nodes in VANET possess substantial power resources, which is an advantage over traditional ad hoc networks.

VANET can be distinguished from other ad-hoc networks by the following properties:

- Highly Dynamic Topology :The topology of VANET is always changing due to high speed of movement of vehicles.
- Sporadic Network Connectivity : Due to the same high speed movement of vehicles, the connectivity of the VANET changes frequently. The network is sparsely connected, when the vehicle density is low.
- Geographic type of Communication : The VANETs mostly used geographical broadcasting aimed at a particular geographic region. The Rode Side Units (RSU) often broadcast various traffic optimizatior, safety related application which will be received by the vehicles currently residing in their coverage area.
- Mobility Modeling and Prediction :It plays an important role for designing the protocols for VANET. In VANET, the movement of vehicles are constrained by highways, street roads which can't be changed. Hence given the map of current geographic location and approximate speed of vehicle, the position of vehicle in the future can be determined.
- Hard Delay Constraints : In life threating accidents or situations, where the emergency safety message (ESM) should reach other vehicles as soon as possible, there should not be slightest delay or network interruption.
- Sufficient Energy and Storage : The nodes (vehicles) have ample energy and computing power (including both storage and processing).
- Different Communication Environments : Relatively simple highway traffic scenarios and complex city traffic scenarios.

1.3 Applications of VANET

The main applications of VANET are categorized into following two categories. They are as follows:

- Safety related applications: such as co-operative lane merging and collision avoidance. This kind of applications deals with life-threating conditions where the existence of a service may prevent life-endangering accidents.
- Non-safety related applications : such as traffic optimization, electronic toll collection, congestion pricing system, infotainment services.

1.4 Communication Standards for VANET

1.4.1 Dedicated Short Range Communication (DSRC)

It is developed by USA and is a short to medium range communications service that is used for V2I and V2V communication. The United states Federal Communications Commission (FCC) had allocated 750 MHz of spectrum i.e from 8.5 GHz to 9.25 GHz to be used by DSRC. [8]. DSRC spectrum has 7 channels with each channel 100 Mhz wide. Out of 7 channels, six channels are used for service purpose and remaining one for control purpose. The following figure 1.2 shows the bandwidth allocation of DSRC Spectrum.

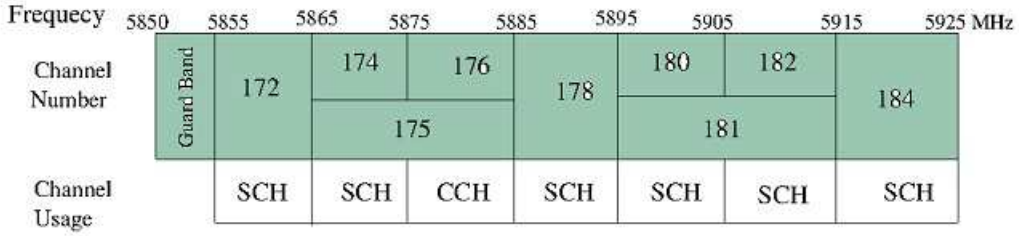

Figure 1.2: DSRC Bandwidth Allocation [8]

1.4.2 Wireless Access in Vehicular Environment (WAVE) (IEEE 1609.11p)

In 2003, American Society for Testing and Materials (ASTM) sets ASTM-DSRC which was totally based on 802.11 MAC layer and IEEE 802.11a physical layer [8]. The main problem with IEEE 802.11a with Data Rate of 54 Mbps is it suffers from multiple overheads. Vehicular scenarios demands high speed data transfer and fast communication because of its high topological change and high mobility. For this the DSRC is renamed to IEEE 802.11p Wireless Access in vehicular Environments (WAVE) by the ASTM 2313 working group. This works on MAC layer and physical layers. WAVE consists of Road Side Unit (RSU) and On-Board Unit (OBU). WAVE uses OFDM technique to split the signals. The following figure 1.3shows the WAVE, IEEE 802.11p, IEEE 1609 and OSI model.

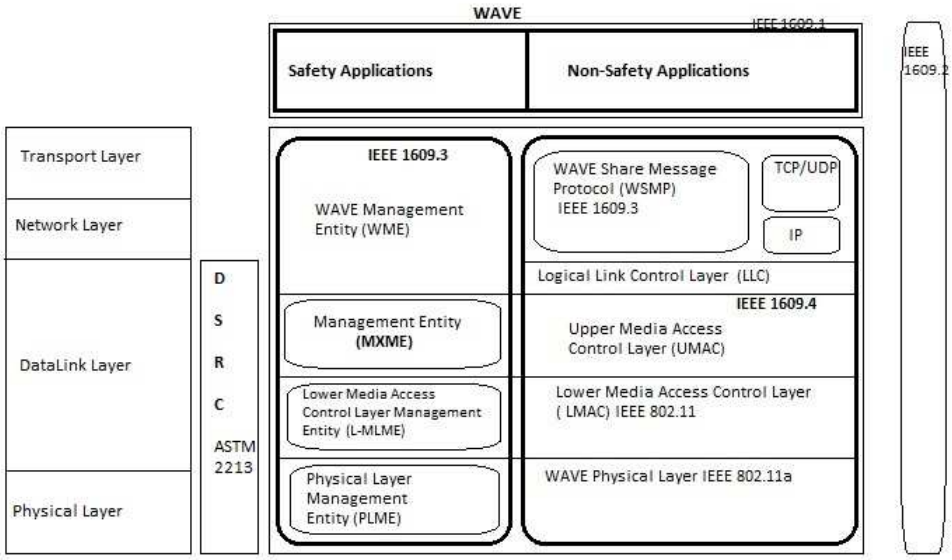

Figure 1.3: WAVE protocol Stack [8]

1.5 Components Needed for VANET Security Architecture

1.5.1 Event Data Recorder (EDR)

Similar to black-box in areoplanes and responsible for storing the vehicles critical data, such as position, speed, time, received messages etc. during emergency events [14], which will help in crash reconstruction and the attribution of liability. It should be tamper-proof.

1.5.2 Trusted Component (TC)

All the cryptographic materials (keys) of a vehicle need proper hardware protection, namely TC. The TC stores all the cryptographic material and performs all the cryptographic operations, [14]. The TC can also include its own clock and battery that is periodically recharged from vehicles electric circuits.

1.5.3 Electronic Licence Plate (ELP)

These are unique ID of vehicles equivalent to the traditional license plates [16]. The advantage of ELPs is that they will automate the paper-based document checkup of vehicles, detection of stolen cars. An alternative approach to ELP is to use Electronic Chasis Number (ECN) [16]

1.5.4 Vehicular Public Key Infrastructure (VPKI)

The large number of vehicles registered in different countries and travelling long distances requires a robust, inter-operable and scalable key management scheme. The involvement of legal authorities in vehicle registration indicates a certain level of centralization. Hence the need for Vehicular Public Key Infrastructure (VPKI) [14], where Trusted Authority (TA) will issue certified public/private key pairs to vehicles. There will be several TAs corresponding to different regions; they should cross certify each other. Vehicle manufactures can also take the role of TAs.

1.5.5 Authentication

In order to prevent in-transit traffic tampering and impersonation attacks, authentication is needed of the origin of data packets. Currently ECC (elliptic curve cryptography), the most compact public key cryptosystem is used due to its less overhead. The overheads can further reduced by signing only critical messages [14].

1.5.6 Privacy

To conceal the vehicles identity, a set of anonymous keys which will change frequently according to different driving conditional are used. These are preloaded into vehicles TC until the next maintenance. Each key is certified by the issuing TA and has a short lifetime. It can be traced back to the real identity of the vehicle in liability issues [14].

1.5.7 Secure Positioning

A vehicle can cheat with its position to escape liability cases. Hence secure position verification is needed. In addition, vehicles or base stations may want to verify the position of other vehicles or base stations on-the-fly to ensure they are communication with the claimed party. Verifiable Multilateration [17] which works by measuring the distances from three points (vehicles) to a claimant (the vehicle whose position is being verified) are verifying that the claimed position is consistent with the measured one.

1.6 Security Threats to VANET

Before we discuss various attacks on VANET, we must classify the capacities of an attacker. So the attackers can be classified into four dimensions [1] which are discussed below.

(1) Insider vs Outsider : The insider is an legitimate member of the network that can communicate with other members. The outsider is considered as an intruder by the network members and hence is limited in the diversity of attacks he can mount.

(2) Malicious vs Rational: A malicious attacker has no personal agenda for the attacks and his only aim is to harm the member or the functionality of the network . Hence, he may employ any means disregarding corresponding costs and consequences. On the other hand, a rational attacker has personal motives and hence is more predictable in terms of attack means and attack target.

(3) Active vs Passive: An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

(4) Local vs ExtendedAn attacker can be limited in scope, even if controls several entities, which makes him local. An extended attacker controls several entities that are scattered across the network, thus extending his scope.

The security of VANET is crucial as sometimes they are related to life threatening situations. Hence No vital information should be inserted or modified by a malicious attacker. The system must able to determine the liability of drivers while still maintaining their privacy.

The security attacks are broadly categorized, depending on the availability, authentication, confidentiality, privacy, non-repudiation and data-trust [9, 10]into the following main groups and discussed as below.

1.6.1 Threats to Availability

The following threats to the availablility of V2V and V2R have been identified.

- DoS Attack:The attacker is $*$.M.A.L category and may want to bring down the entire VANET or even cause an accident by channel jamming or aggressively injecting dummy messages into the network [11].

- Broadcast Tampering : An insider attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.

- Malware : A potential threat which can cause serious disruption to VANET operations. Malwares can be introduced into the networks when the OBUs and RSUs receive software and firmware updates.

- Spamming : The increased presence of spam messages on VANET may increase the latency.

1.6.2 Threats to Authenticity

Whenever any vehicle in VANET needs secure communication its basic requirement is either identification or authentication of nodes under consideration. The different types of attack on authentication are given below:

- Masquerading : By posing as a legitimate vehicle in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false information.
- GPS Spoofing ; The attacker can produce false GPS readings by use of a GPS satellite simulator to generate signals that are stronger than genuine GPS satellites.
- Replay Attack : The attacker re-injects the previously received packets back into the network, poisoning a nodes location table by replaying beacons.
- Message Tampering : An attacker may modify messages exchanged in V2V and V2I communication in order to falsify transaction application requests or to forge messages.
- Sybil Attack : It is the creation of multiple fake nodes broadcasting false information [12].In this attack, a vehicle installed with an OBU sends multiple copies of messages to other vehicles and each message contains a different fabricated identity. The problem arises when malicious vehicle is able to pretend as multiple vehicles and reinforce false data [13].
- ID Disclosure : This is a big brother scenario, where a global observer can monitor the mobility pattern, trajectory of targeted vehicles and use this location information for his benefits. To monitor, the global observer can leverage on the fixed infrastructure or the vehicles around its target.

1.6.3 Threats to Confidentiality

Despite the fact that the messages transmitted in VANET doesn't hold any delicate information which ought to be kept a secret, still the secrecy of messages

exchanged between the nodes of a vehicular system are especially vulnerable to eavesdropping for collecting messages and gathering of location information available through the transmission of broadcast messages [11].

1.6.4 Threat to Privacy

Location privacy and anonymity are important issues for vehicle users. Location privacy involves protecting users by obscuring the users exact location in space and time. By concealing a users request so that it is indistinguishable from other users request, a degree of anonymity can be achieved [11].

1.7 Challenges towards security of VANET

The provision of robust security for vehicular networks must overcome a set of technical, economic, and social challenges discussed as follows:

- Network scale and Dynamics : If realised, VANET will be the largest real-life instance of self-organized ad hoc network, consisting of millions of nodes which are distributed under different authorities and services providers. Problems of scalability and seamless interoperability should be solved in a way transparent to the driver, especially that most operations are performed on the fly while the vehicle are moving at high speeds. Hence the vehicles will not be able to participate in long term security protocols because of the highly dynamic nature of the network. [4,6]

- Liability vs Privacy: One of the major concerns of VANET is accountability, and eventually liability, of the vehicles and their drives is required. Vehicular communication is envisioned as an excellent opportunity to obtain data that can assist legal investigations This implies that unambiguous identification of the vehicles should be possible, as sources of messages. But such prerequisites raise even stronger privacy concerns [13, 14].

- Real Time Communication : The safety applications pose strict deadlines for message delivery. This means the security protocols should impose low processing and messaging overhead and be robust to clogging denial of service attacks [14].

- Trust: Due to the extensive number of independent nodes and the presence of human factor, it is highly probable that misbehavior will happen. Additionally the drivers are increasingly concerned about their privacy. Due to lack of privacy and related potential of tracking may result in high financial charges on the drivers (e.g. due to occasional over speeding). Hence, the level of trust in vehicles as well as service provider base stations will be low.

- Cost : The introduction of new communication standards, such as DSRC, for vehicular communications will require the manufactures to install new hardware modules on all vehicles, thus increasing the unit cost for consumers [15].

- Gradual Deployment: IVC deployment gaining considerable market penetration will take much time may be a decade. Hence only a small proportion of vehicles will contain the enhanced features of IVC over the next decade. But the functionalities should be supported despite the low penetration rate. The vehicles should be able to carry out most of the security functions autonomously [15].

1.8 VANET Projects Across the World

With the advent of wireless technology and underlying VANET architecture, there are several Intelligent Transportation System [18] projects, which have been undertaken in various countries mostly in USA, European Union and Japan. Some of them are sponsored by automobile industries and others by government.

Early developments in VANET focused on underlying VANET architecture such as communication standards, wireless protocol infrastructure, standardization of 802.11p, WAVE [8] and DSRC [8] . Those are considered as phase 1 development in VANET. But now various projects in VANET are mostly concerned with real life implementation by field trials, called phase 2 where the verification of protocols developed during phase 1 is also conducted. A brief summary of various research projects is given below.

1.8.1 In European Union

- Car-to-Car Communications Consortium (C2C-CC)(2001) [19] : The Car2Car Consortium, a non-profit organization, sponsored by various European automobile manufacturers that is open for research organisations, equipment providers and other partners. Aim was to improve driving assistance, active safety applications deployment.
- SEVECOM [20]: Secure Vehicle Communications is an EU-funded project that focuses on providing a full definition and implementation of security requirements for vehicular communications.
- FleetNet (2000-03) [21] : An early European Union sponsored trial, aimed at identifying problems inherent in V2V communications.
- Network on Wheels (2004-10) [21] : An initiative by major European manufacturers and supported by Federal Ministry of Education and Research, Germany. Aim was to solve key technical issue of communication protocols and security of V2V communications.
- PReVENT (2004-08) : PReVENT [21], an EU project regarding safety applications using sensors, maps and communication system.

1.8.2 In USA

- Wireless Access in Vehicular Environments (WAVE)(2004) [10] : It is a set of standards released in 2004 and again revised in 2006 [ref] , which enabled the practical trials for V2V and V2I communications and became foundation for other projects.
- Vehicle Safety Communications (VSC) (2002-04) (VSC-2) (2006-09) [10] : Goal was to improve critical safety situations with the help of positioning systems and DSRC, Evaluate the minimum safety requirement and various performance parameters.
- Vehicle Infrastructure Integration (VII) (2004-09) : Aim was to provide co-ordination between different automobile manufacturers.
- Clarion [10] : Clarion A consortium of hi-tech automobile companies from both Japan and USA.

1.8.3 In Japan

- ASV 2 (1996-2000) [10] : stands for Advanced Safety Vehicle. It is extended to ASV-3 in 2001 and ASV-4 in 2005 by providing automatic collision avoidance system and navigation system. It is supported by Honda, Mitsubishi, Suzuki and Toyota.
- DEMO started in 2000 for providing cooperative driver support system. It uses band of 5.8 GHz and CSMA protocols for communication.
- JARI [22] stands for Japan Automobile Research Institute which conducts many trials for the projects and it evaluated the USA projects and European Union Projects. It mainly focuses on security and safety.

The following figure 1.4 shows the various project undertaken in different countries.

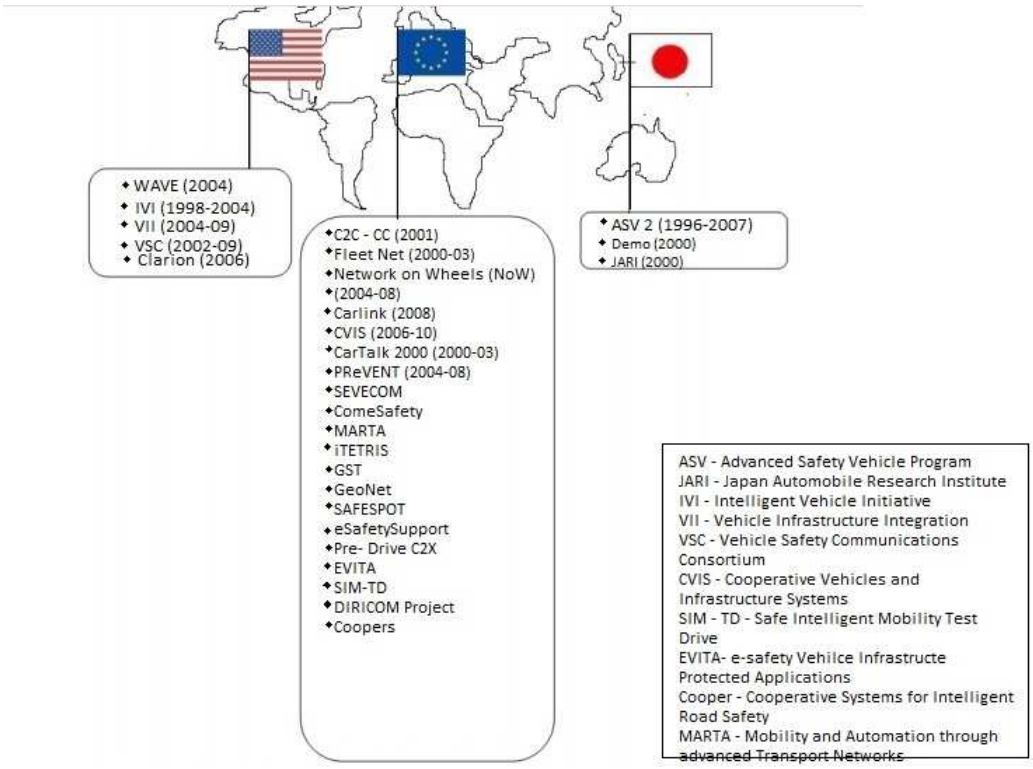

Figure 1.4: Recent Projects in European Union, USA and Japan.

1.9 Motivation

There are so many existing research areas in VANET such as secure routing, security, Quality of Service etc. Also researchers are working on some other important areas like communication protocol design, cost-effective hardware design. But out of all of these above areas, security is one of the major areas of concern as VANETs very existence relates to life threatening conditions. Hence it is very important that the information exchanged in VANET communication should be authentic and cannot be inserted by a malicious attacker. While performing the authentication, the whole system should protect the privacy of the sender and disclose the identity of the sender only in liability issues. Now authentication in VANET can be done with the help of Digital signatures, PKI but it requires omnipresent fixed infrastructure (RSU) which may not be possible due to high cost of deployment. Hence our aim is to provide authentication with limited help of fixed infrastructure.

1.10 Objective

The main objectives of this research work is to

- Authentication for V2V Communication :Design of an Authentication scheme for V2V communication in VANET which can operate with limited existance of fixed infrastructure.
- Privacy :while preserving privacy, it should also be able to track the malicious vehicle, in liability cases.
- Reduction of Communication Overhead : Group formation is done, so that the vehicle within a group will communicate with the Group leader, then Group Leader(GL) will aggregate and send the messages with one-hop broadcast, also GL communicates with infrastructure, when in contact for reporting vehicles for revocation purposes.

1.11 Organization of Thesis

The rest of the thesis is organized as follows :

1. Chapter 1 : In this chapter we have already discussed the Introduction to VANET, Overview, Security architecture, Motivation and Objective of our research.

2. Chapter 2 : In this chapter, Various existing schemes for authentication in VANET such as RSU Based, Pseudonym Based, Group Based authentication is presented along with their brief overview, features and limitations.

3. Chapter 3 : In this chapter, we present our proposed OBU based Authentication Scheme for V2V Communication in VANET.

4. Chapter 4 : In this chapter, we evaluate the performance of our proposed scheme.

5. Chapter 5 : Finally we conclude our research in this chapter.

Chapter 2

Literature Review

2.1 Literature Review

There are various authentication mechanisms present in VANET, but mostly they are based on VPKI which is inefficient. Lately some group based authentication schemes are proposed but still they couldn't avoid the absolute necessity of RSUs. Here we are going to discuss some of them which can be classified into the following.

2.1.1 RSU Based Authentication

The authentication of messages exchanged in VANET with the help of Digital Signatures is efficient, but simultaneously puts the privacy of drivers/vehicles at risk. Most RSU based authentication mechanisms use certification services and heavily reliant on fixed continuous infrastructure. Lu, Rongxing, *et al.* [6] proposed a conditional privacy preservation protocol consisting of 3 layers of privacy. First, an RSU issues temporary anonymous certificates to vehicles, hence it can map the vehicle with the anonymous certificate. Second, in the V2V communication, the vehicles are anonymous to each other due to anonymous certificates. Third, Trusted Authority (TA) can find out the identity of malicious vehicle in disputes. The anonymous certificates have an expiration date, hence certificate revocation can be done after the validity period. But this mechanism may not be scalable as it depends on fixed continuous infrastructure. Due to cost constraints, it will not be possible to provide proper infrastructure for VANET in near future.

RAISE [7] by Zhang, Chenxi, *et al.* also employs RSUs to assist vehicles in

authenticating messages. In this mechanism, the messages exchanged between vehicles are stored in temporary buffers of the receiving vehicles. They wait for the RSU to broadcast an aggregated message compiled from all the exchanged messages, and then compare that RSU broadcasted messages with stored messages and use it, if they find it reliable. Although it reduced communication overhead, still the vehicles have to wait for RSU to broadcast a aggregated message, which may not be suitable in emergency safety messages (ESM).

2.1.2 Pseudonym Based Authentication

Message authentication and anonymity of vehicles are always two major challenges faced by VANET. To achieve both Message authentication and privacy, Raya, *et al*. [1] proposed to preload each vehicle with a large number of anonymous public/private key pairs together with their PKI certificates. Here, for achieving privacy, each public/private key pair has a very short life span, and a pseudo ID is used in each public key certificate. This mechanism suffers from the limitations of storage requirement and also dependent on PKI based architecture. It also increases the overhead at the TA as TA has to maintain a large no of certificates for all vehicles. The Above limitation are dealt by the mechanisms proposed by Calandriello *et al*. [2] and Lin *et al*. [3] where group signatures [4] are used to permit vehicles to generate self-certified public keys.

2.1.3 Group Based Authentication

Group Based protocols are mainly used for privacy preservation. The key is to hid the vehicles identity in a group. Group signature [4] allows a group member to sign messages anonymously on behalf of a group. The identity of a signer can only be revealed by group manager in case of disputes. Lin *et al* [4] proposed a group signature based scheme to sign the messages. Here, the recipients can verify the messages authenticity using the group public key. If authenticated, then then the vehicle confirms that the message has originated from a legitimate vehicle of the network, not some malicious vehicle. But the recipient vehicle cannot determine the source vehicles identity due to group signature. Hence it helped in authentication, privacy preservation, reduced storage and also low bandwidth consumption. Lin et al. also proposed a geographic based group formation. Calandriello *et al* . [2] proposed a scheme where a vehicle can generate

public/private key pairs by itself using a group key. It achieved a tradeoff between traditional PKI based Schemes and group-signature-based schemes. Though, group signature is a stronger property than pseudonym authentication, it still has many complexities as Group formation in VANET is highly volatile and frequently changes.

Verma, *et al.* [5] proposed SeGCom which is a combination of both RSU based and Group based authentication. Here group refers to the vehicles under the coverage area of same RSUs. SeGCom provides 2 types of authentication mechanisms. First, successive authentication mechanisms for V2I communication, where the vehicle is authenticated by RSUs. Second, group formation and group Key distribution for V2V communication which is done with the help of corresponding RSU, Here no group leader is present. The RSU distributes a split key to vehicles for V2V communication upon the entrance of the vehicle to its coverage area. Then the vehicle can self-compute different split keys inside the coverage area of RSU, until it leaves the current group.

2.2 Summary

In this chapter, we discussed briefly about various authentication schemes in VANET which are primarily dependent on fixed infrastructure and TA. But due to high cost of deployment and communication overhead issues, they are not always efficient. Our proposed On Board Unit Based authentication scheme which primarily focuses on V2V communication can operate with lack of infrastructure due to its self-sustaining nature. Hence it drastically reduces cost of deployment. Also Group communication between members and Group leader reduces network overhead.

Chapter 3

On Board Unit Based Authentication for V2V Communication in VANET

3.1 Network Model

In our proposed scheme, we only consider V2V communication for mostly for safety related information as traffic optimization messages are mostly broadcasted by RSUs via V2I communication. The vehicle form dynamic non-overlapping groups depending upon their driving pattern and closeness. Each vehicle is equipped with Global positioning Systems (GPS) , Trusted Component(TC) and OBUs which are capable of short lived anonymous public/private key pairs. The newly generated key pairs are self-certified, hence doesn't depend on any fixed infrastructures for key certification. The keys can be authenticated by the receiver (group leader in this case) and can be revoked later.

3.2 Assumptions

The proposed scheme is based on following assumptions

- A straight road scenario such as Highways, Hence group formation would be easier by their mobility pattern as most of the vehicles travel in same direction and there is little chance of changing direction.
- The Group leader can be elected as the vehicle at the center of the vehicle cluster.
- Each vehicle is equipped with GPS, TC etc.
- Whenever the OBU sends a message, it automatically attaches a tracking hint which is provided by TA. It will later help in identifying malicious vehicles.
- Key revocation can be done by the TA using the existing Revocation of Trusted Component (RTC) protocol [16] by mapping the tracking hint with the vehicle unique ID registered.

3.3 Notation

The Notations used in this scheme are given in Table below and we have adopted some of the notations from [23]

- G = (G,*). A Finite Cyclic group of order q , $g \epsilon G$ is a generator of G, assuming it is impossible to compute discrete logarithms in G with respect to g. G might be a large multiplicative subgroup of Z_p^* for some large prime p, where q is a large prime dividing $p-1$.
- h Cryptographic one way hash function mapping arbitrary length binary string to fixed length strings of length l (typical value of l is 512 for SHA-512)
- f Another Cryptographic one way hash function mapping the set $\{0, 1, ..q-1\}$ onto itself.
- $m \geq 1$, Positive integer determining number of key pairs that a vehicle can generate.

Table 3.1: Notations

Notation	*Description*
sk_{TA}	TA's master secret Key
PK_{TA}	TA's public keys
V_{ID}	The vehicle
OBU_V	The OBU equipped on the vehicle V
TC_V	The Trusted Component on the vehicle V
σ	Tracking Hint
cv	Check Value
PK_i	Public key at time T_i
SK_i	Corresponding Private Key at time T_i
H_i	Corresponding Helper Value for PK_i
G_{jreq}	Group Joining Req
Pu/Pvt	Short lived public/pvivate key pair of vehicle V
$cert_{OBU}$	OBU certification on Pu and H_i

3.4 Generation of Check Value

1. TA chooses $sk_{TA} \epsilon Z_p^*$ [The Master Secret]

2. Generated corresponding public key

$$PK_{TA} = g^{sk_{TA}} \tag{3.1}$$

3. OBU_V submits its V_{ID} to TA during registration. TA chooses another random number $S\epsilon(G, *)$ for the OBU_V and generates a +ve integer P such that

$$P = \pi_{j=0}^{m} f^j\,(S) \tag{3.2}$$

4. Check Value cv is calculated as

$$cv = h(g^P) \tag{3.3}$$

5. Tracking hint

$$\sigma = Encr_{PK_{TA}}(V_{ID}) \tag{3.4}$$

3.5 Generation of Anonymous public/private Key pairs

- TA gives the following to TC_V

$$\{cert_{TA}(cv)\ ,\ \sigma\ ,S\ ,\ T_{span}\}$$

- T_{span} is life time for the check value cv until the next maintenance, where as T_i is a short time interval, within which the vehicle should not be able to generate enough different keys to make a false information reliable for the receiving vehicle.

- In each time interval T_i, TC_v generates anonymous public/private key pair as follows

  – Private Key

$$SK_i = \pi_{j=0}^{m-i-1} f^j\,(S) \tag{3.5}$$

– Public Key

$$PK_i = g^{SK_i} \tag{3.6}$$

– Helper value for public key pk_i

$$H_i = \pi_{j=m-i}^{m} f^j(S) \tag{3.7}$$

- if V wants to join a group, the OBU_v generates a key pair pu/pvt (preferable by RSA) and corresponding certificate $cert_{OBU}$ is signed using SK_i, generated in equation 3.5. The $cert_{OBU}$ also contains cv and pu and valid for only time period T_i.
- OBU_V sends the following parameters to Group Leader (G_L)along with G_{jreq} message.

$$\{cert_{OBU},\, PK_i,\, H_i,\, \sigma\ \}$$

3.6 Authentication

- The G_L calculates

$$cv^* = PK_i^{H_i}$$

- if $cv == h(cv^*)$
  then vehicle V (OBU_V) is authenticated and G_L stores the corresponding pu and cv
- G_L sends to OBU_V his group public key for further communication. $Encr_{pu}(PK_{gl}||\{PK_{gl}\}_{sig_{PK_{gl}}})$

3.7 Summary

In this chapter, an authentication scheme which can operate with limited support of fixed infrastructure was presented. Here, the vehicles generate self-certified anonymous public/private key pairs based on a check value given by TA, hence it eliminates the necessity of TA to store all the key pairs as well as frequent communication with TA for authentication purpose. While the proposed scheme preserves the privacy of vehicles, it can also track a vehicle using tis tracking hint. But other vehicles can't track a vehicle even if they have the tracking hint as they don't have the master secret of TA. Group formation is done only to reduce the network overhead by reducing no of broadcasts by all the members.

Chapter 4

Experiment and Results

4.1 Authentication by Group Leader

- The Group Leader G_L calculates cv^* as

$$cv^* = PK_i^{H_i}$$

by equation 3.6

$$cv^* = g^{SK_i H_i}$$

by equation 3.5 and 3.7

$$cv^* = g^{\pi_{j=0}^{m-i-1} f^j(S) \pi_{j=m-i}^{m} f^j(S)}$$

which reduces to

$$cv^* = g^{\pi_{j=0}^{m} f^j(S)}$$

Hence by equation 3.2

$$cv^* = g^P$$

But from equation 3.3

$$cv = h(g^P)$$

$$cv = h(cv^*)$$

Hence the vehicle is authenticated by group leader.

4.2 Privacy

In Our Proposed authentication scheme, the TA gives a common check value cv to all the registered vehicles. And the authentication is also achieved using the check value. So if an adversary or a member of group itself tries to track a specific vehicle using its check value cv, it will not succeed in its attempt as all the vehicles are having same check value cv. '

But in liability cases, the Group Leader can submit the tracking hint σ of the sender vehicle to TA, when comes in contact with fixed infrastructure, from equation 3.4

$$\sigma = Encr_{PK_{TA}}(V_{ID})$$

Hence it can only be decrypted by TA using his master secret sk_{TA}. No other vehicle can decode the tracking hint. Then TA may revoke the certificate of the vehicle using any of the existing Certificate revocation protocols [ref] such as RTC.

4.3 Group joining and leaving

As already discussed, a vehicle can become member of a group (having same mobility pattern) by sending G_{jreq} and subsequent authentication by Group Leader. If a vehicle leaves the group, the Group Leader doesn't have to change anything in its key, but if the Group Leader itself leaves the group, in which case the remaining members must elect a new group leader (usually the vehicle at the center of the cluster). By group formation the communication overhead is reduced significantly which can be shown by the following scenario..

Consider a scenario when there are 10 vehicles in a group. All vehicles will send messages to each other (mesh topology), which will result in 45 messages transmissions within group. But if there is group leader and the vehicles (in this case 9) only send their messages to Group Leader and then the group leader aggregate and send one aggregated message, the same information sharing can be achieved using 10 message transmissions. (9 unicast+ 1 broadcast)

Hence group formation definitely helps in reducing network overhead. (Although group formation in VANET is not yet very clear)

4.4 Summary

In this Chapter, the authentication procedure by Group leader is shown. Then how our proposed scheme protects the privacy of vehicles, is explained. Lastly a comparison table of various existing authentication schemes is given. Although the performance of our proposed scheme may not be very effective, but the major advantage is the drastically reduced cost. It can operated with limited support of fixed infrastructure, hence can readily deployed, while other schemes may have to wait until omnipresent fixed infrastructure is deployed. The following table 4.1 shows a comparison of various schemes which summarizes everything.

Table 4.1: Summary of Characteristics of Various schemes discussed in literature and our proposed scheme

Features	Raya et al. [1]	Calandriello et al. [2]	SegCom [5]	Our Solution
Additional Hardware Needed	yes	yes	yes	yes
Provide Authenticity of messages	yes	yes	yes	yes
Anonymity of msg origin	no	yes	no	yes
Cost of infrastructure	High	High	High	Low
RSU needed	must	must	must	can operate with limited support
provide distinguishable emitters	no	no	yes	yes
no of key pairs to be stored	All that must be used	1	All	NONE
no of key pairs to be managed by TA	ALL	1	All	NONE

Chapter 5

Conclusion and Future Work

In our work, we proposed an On Board Unit Based Authentication for V2V Communication in VANET which can operate effectively with limited support of fixed infrastructure when there is a lack of it. Our proposed Scheme also forms groups between vehicle based on their mobility pattern to share traffic related information. The group leader receives and authenticates the messages from the vehicles and then sends the aggregated information into the network which reduces network overheads. By this scheme, the privacy of vehicles is also protected. But most importantly, it drastically reduces the overhead on TA as neither the TA have to store all the key pairs for revocation purpose nor the TA have to authenticate each vehicle. Also less dependency on fixed infrastructure results in reduced cost, as the infrastructure needed for VANET will take a lot of time in coming days to be fully implemented, till then our scheme can be an effective way to authenticate vehicles.

Scope for Further Research

Although our work only deals with Authentication of message, there is considerable concern regarding reliability of messages and subsequent evaluation for revocation. So this work can be further extended for checking reliability of messages as well as design of parameters for an efficient certificate revocation procedure.

Bibliography

[1] Raya, Maxim, and Jean-Pierre Hubaux. "Securing vehicular ad hoc networks."Journal of Computer Security15.1 (2007): 39-68.

[2] Calandriello, Giorgio, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. "Efficient and robust pseudonymous authentication in VANET." InProceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19-28. ACM, 2007.

[3] Lin, Xiaodong, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. "GSIS: a secure and privacy-preserving protocol for vehicular communications."Vehicular Technology, IEEE Transactions on56, no. 6 (2007): 3442-3456.

[4] Chaum, David, and Eugne Van Heyst. "Group signatures." InAdvances in Cryptology EUROCRYPT 91, pp. 257-265. Springer Berlin Heidelberg, 1991.

[5] Verma, Mayank, and Dijiang Huang. "SeGCom: secure group communication in VANETs." InConsumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, pp. 1-5. IEEE, 2009.

[6] Lu, Rongxing, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications." InINFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.

[7] Zhang, Chenxi, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, and Xuemin Shen. "An efficient message authentication scheme for vehicular communications."Vehicular Technology, IEEE Transactions on57, no. 6 (2008): 3357-3368.

[8] Std, A. S. T. M. "E2213-03,?Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems?5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications?.

[9] Fuentes, Jos Mara de, Ana Isabel Gonzlez-Tablas, and Arturo Ribagorda. "Overview of security issues in Vehicular Ad-hoc Networks." (2010).

[10] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular ad hoc networks (VANETS): status, results, and challenges."Telecommunication Systems50, no. 4 (2012): 217-241.

[11] LUO, JUN. "The security and privacy of smart vehicles." IEEE Security and Privacy (2004).

[12] Douceur, John R. "The sybil attack." In Peer-to-peer Systems, pp. 251-260. Springer Berlin Heidelberg, 2002.

[13] Parno, Bryan, and Adrian Perrig. "Challenges in securing vehicular networks." InWorkshop on hot topics in networks (HotNets-IV), pp. 1-6. 2005.

[14] Raya, Maxim, Panos Papadimitratos, and Jean-Pierre Hubaux. "Securing vehicular communications." IEEE Wireless Communications 13, no. 5 (2006): 8-15

[15] Raya, Maxim, and Jean-Pierre Hubaux. "Security aspects of inter-vehicle communications." In 5th Swiss Transport Research Conference (STRC), no. LCA-CONF-2005-012. 2005.

[16] Raya, Maxim, Daniel Jungels, Panos Papadimitratos, Imad Aad, and Jean-Pierre Hubaux. "Certificate revocation in vehicular networks." Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland (2006)

[17] Leinmuller, Tim, Elmar Schoch, and Frank Kargl. "Position verification approaches for vehicular ad hoc networks." Wireless Communications, IEEE 13, no. 5 (2006): 16-21.

[18] Dimitrakopoulos, George, and Panagiotis Demestichas. "Intelligent transportation systems." Vehicular Technology Magazine, IEEE 5, no. 1 (2010): 77-84.

[19] http://www.car-to-car.org/. Accessed : August, 2013

[20] http://www.sevecom.org/. Accessed : August, 2013

[21] http://www.cvisproject.org/en/links/. Accessed: August, 2013

[22] http://www.jari.or.jp/tabid/200/Default.aspx?language=en-US. Accessed : August, 2013

[23] Kounga, Gina, C. J. Mitchell, and Thomas Walter. "Generating certification authority authenticated public keys in ad hoc networks."Security and Communication Networks5, no. 1 (2012): 87-106.