AN ENHANCED SECURE PKI AUTHENTICATION SCHEME FOR VEHICULAR AD-HOC NETWORKS

Thesis submitted in partial fulfilment of the requirements for the award of degree of

Master of Engineering
in
Information Security

Submitted By
Navkiran Kaur Mann
801333014

Under the supervision of:
Dr. Neeraj Kumar
Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

JULY 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*AN ENHANCED SECURE PKI AUTHENTICATION SCHEME FOR VEHICULAR AD-HOC NETWORKS*" in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Neeraj Kumar* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Navkiran

(Navkiran Kaur Mann)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

13/7/15

(Dr. Neeraj Kumar)
Associate Professor,
Computer Science and Engineering Department

Countersigned by

Deepak Garg

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

Acknowledgment

No volume of words is enough to express my gratitude towards my guide, **Dr. Neeraj Kumar**, Associate Professor, Computer Science and Engineering Department, Thapar University, who have been very concerned and have supervised the work presented in this thesis report. He has helped me to explore this vast field in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to **Dr. Deepak Garg**, Head of Department, CSED and **Ms. Jhilik Bhattacharya**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my **parents**, **friends** and the **Almighty** for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Navkiran Kaur Mann

(801333014)

Abstract

For the past few years, Vehicular Ad Hoc Networks (VANETs) have been attracting researchers across the globe due to their usage in wide areas of networks. VANETs bring a revolutionary change to the current on road experience of drivers. This network deals with communication of nodes which are dynamic nature. Due to this reason, issues exist in both efficiency and security of this system.

Security is one of the most important components which needs to be investigated further in VANETs as bogus information may mislead the users. In past, numerous schemes have been proposed to prevent different kinds of attacks for increasing the efficiency of various applications in VANETs. In this dissertation, a new scheme is proposed which identifies the pitfalls in the existing Wang *et al.* [20] scheme. The proposed scheme is evaluated in comparison to the existing scheme by using various evaluation metrics and attacks in VANETs, where its performance was found better than the above said scheme. Various types of attacks are identified and their performance in comparison to the proposed scheme is evaluated.

Table of Contents

List of Figures

List of Tables

List of Algorithms

Abbreviations

CA	Certificate Authority
CRL	Certificate Revocation List
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSRC	Dedicated Short Range Communication
ECDSA	Elliptical Curve Digital Signature Algorithm
ECPP	Efficient Conditional Privacy Preservation
EDR	Event Data Recorder
ELESPP	Enhanced Lightweight and Efficiency Strong Privacy Preservation Authentication.
FANETs	Flying Ad-hoc Networks
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IOT	Internet of Things
KDC	Key Distribution Centre
LESPP	Lightweight and Efficient Strong Privacy Preserving
MAC	Message Authentication Code
MANETs	Mobile Ad-hoc Networks
OBU	On Board Unit
ONE	Opportunistic Network Environment
PKI	Public Key Infrastructure
R2S	Road-to-server
RSU	Roadside Unit
SDH	Strong Diffie-Hellman
TESLA	TeV-Energy Superconducting Linear Accelerator
TPD	Temper Proof Device
VAST	VANET Authentication using Signatures and TESLA++
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
VANETs	Vehicular Ad-hoc Networks
WLAN	Wireless Local Area Network

Chapter 1

Introduction

1.1 Background

Wireless technology is one such miracle of science that has changed the way we live. The proof of this statement are the numerous services that encircle our lives today. Be it the mobile phones, TV remotes, Wi-Fi connections etc. wireless technology has its grip everywhere. The deployment of wireless systems in laptops and palmtops only emphasize the importance of wireless technology. Wireless technologies are in a huge demand in today's world. Wireless Local Area Networks (WLAN) can be seen deployed in the office buildings, college campuses, public areas etc.

Wireless technology as the word suggests is a way to receive or send data without having a direct connection between the communicating systems, i.e., wirelessly. Wireless Standards and specifications come under the family of IEEE 802[1]. This family ranges from Ethernet to wireless. The common specifications being 802.11 (WLAN), 802.15 (Bluetooth/ZigBee) etc. the first ever wireless technique was developed by Guglielmo Marconi, who developed the first ever wireless telegraph system back in 1896 [2]. Since then a lot of inventions and discoveries have been made in this field to enhance its efficiency.

The whole world is moving very fast from wired to wireless. The emergence of new technologies in the wireless arena ascertain demand for it in every aspect of today's modern life. This technology has enabled wireless remote classrooms, telemedicine, video conferencing, smart homes, smart cities and many such fields.

An interesting and new emerging wireless technology is 'Ad-hoc Wireless Communications'. Ad-hoc refers to *temporary connection*. This type of network does not depend on pre-existing infrastructure. Thus, the communication where the nodes or end devices are not stationary is known as ad-hoc wireless network. For example, the wireless routers of a wired network, the sensor nodes of a wireless sensor network there are many applications of this type of network, one such is Mobile Ad-hoc Networks (MANETs) which has been discussed in the next pages.

1.2 MANETs

MANETs are type of ad-hoc network. With a huge demand in mobile devices, the MANETs technology is building up. MANETs are nothing but mobile devices that communicate with each other through no physical infrastructure between them.

A very prominent feature of MANETs is that it supports a dynamic topology. All devices or nodes in the network are mobile and free to communicate with each other. This feature though increases the ease of communication but also has its challenges. The beauty of this network is that every node acts as an independent router. It's a short range communication. Every node in the network takes independent routing decisions and thus there is no central authority that governs this action in the process of communication.

Being an infrastructure less network, MANETs are a cost effective network. It is a decentralised network. Being so, it is also a very flexible mode of communication. MANETs are efficient enough to function in isolation as well as in presence of another centralised or decentralised network. The Figure 1.1 shows a schematic diagram of MANETs.

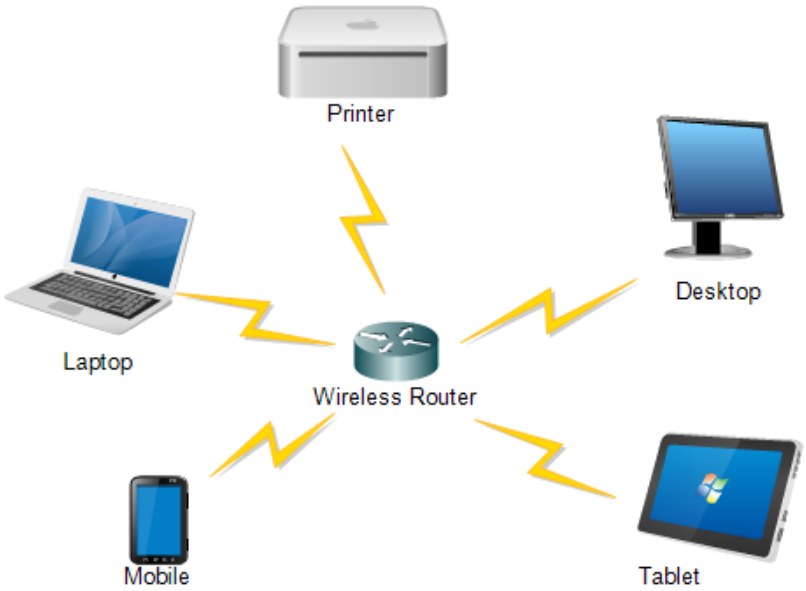

Figure 1.1 Schematic diagram of MANETs

There are many type of MANETs, like Flying ad-hoc networks (FANETs), Vehicular ad-hoc networks (VANETs) etc. The most interesting of these is VANETs as they are an emerging technology and will be implemented on very soon. Many big

companies like Car2Car and General Motors have already tried the prototype models and are working on them to increase efficiency so as to introduce VANETs in the world.

1.3 VANETs

VANETs are one domain of MANETs on which a lot of research has been done recently. With the man's urge to induce technology everywhere, VANETs is one such field where a lot of work has been done. VANETs are nothing but a wireless system that provides a communication between the vehicles. VANETs have changed the whole transportation experience by equipping the vehicles with technology to communicate with each other. As VANETs are a wireless facility and that too on ad-hoc basis, a very frequent change of nodes occur. Due to this it is crucial that the protocols implemented for data transfer match the speed of nodes and also ensure an efficient and secure data transfer.

VANETs have two basic types of communications viz. vehicle to vehicle (V2V) communication and vehicle to infrastructure (V2I) communication. In V2V communication, a vehicle communicates important information with another vehicle like it's speed, the traffic density around it, casualty details (if any) etc. This type of communication helps the other vehicle to drive more cautiously and thus safely. This communication is very vital, as it may also give away information regarding the health of the passengers in the vehicle (if paired to pulse monitor or any other such devices) and may help in recuing lives.

In V2I or Road Side Unit (RSU) communication, vehicles are authenticated, i.e., the vehicle is a legitimate vehicle and not that of any imposter. For the purpose of security, VANETs implies Public Key Infrastructure (PKI) system. The RSU act like a Certificate Authority (CA) in PKI infrastructure. They are responsible for collecting the public key certificates as well as Certificate Revocation Lists (CRL) from a trusted third party and give authentication clearance based on these to the vehicles in its range. RSUs also communicate amongst each other as to provide vital information.

Advantages of using VANETs are that it provides with a co-operative driving experience that can help to reduce the chances of stressed and accident prone driving. VANETs also provide value added services like GPS navigation system, internet access etc.

1.4 Security in VANETs

VANETs being a wireless communication system is prone to a number of attacks. These attacks pose a threat to three main areas viz.

- Threat to availability.
- Threat to authentication.
- Threat to driver's confidentiality.

A vehicle's availability of services can be blocked by attacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack. These saturate the server with a huge number of connection requests (say) because of which the server cannot cater to the needs of crucial information of authentic vehicles. Other attacks such as Black Hole attack, Spamming, Broadcast tampering can also lead too blocked channel.

A vehicle's identity can be imposed by another if proper security techniques have not been used. Such type of attacks tend to tamper with the authenticity of a legitimate vehicle. Other type of such attacks that are a peril to authenticity include Masquerading, Replay Attack, Global Positioning System (GPS) spoofing, Sybil Attack etc.

The next and the last category involves those attacks that present a danger to the driver's confidentiality. These attacks include Eavesdropping. This is one of the most prominent attack. In this the attacker can listen to any information being exchanged by the legitimate vehicle. Keeping all the attacks in mind, the best security scheme used for protecting VANETs is inducing a PKI (Public Key Infrastructure) system.

1.5 PKI

PKI infrastructure is a security proficiency in which a proper hierarchical schema is followed. The Root CA generates Public and Private key certificates which are then distributed by Policy CA after they have been proved by the registration CA.

In a PKI a user may freely make his public key available to all others. PKI system is based on asymmetric cryptography technique. So, if A wants to send data to B, he should possess B’s public key. A uses the public key of B to encrypt the message. This message then travels through the unsecure network (Internet, say) and is received by B. B decrypts the message using his private key. In this way, B is able

to receive the message securely and no one else can open the message except B, due to the presence of private key which only B possesses. Figure 1.2 shows the hierarchical structure of PKI.

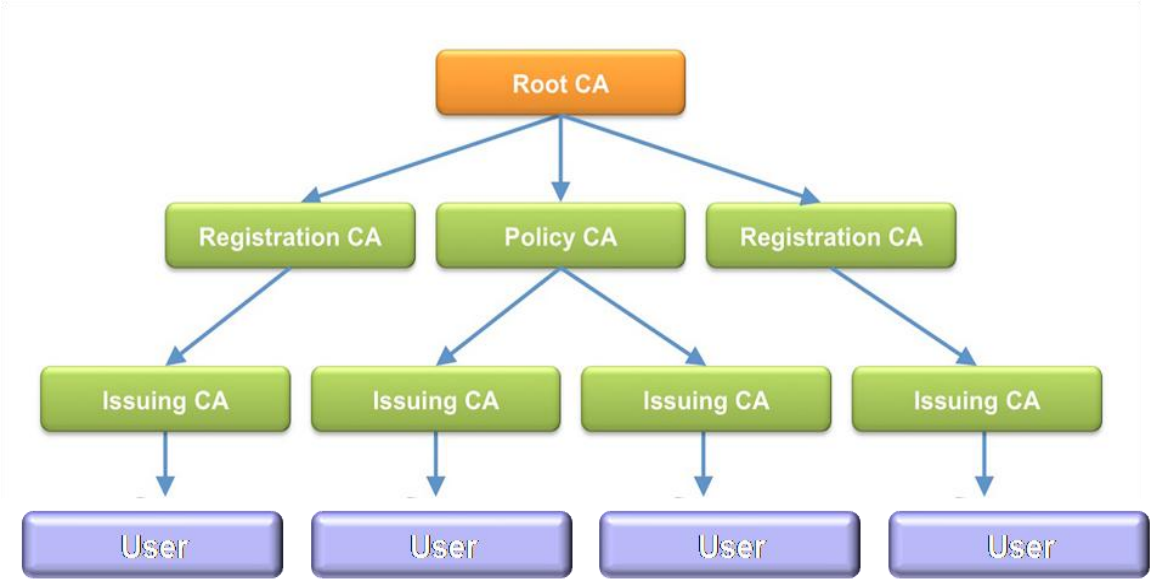

Figure 1.2 Hierarchy in PKI [3]

In PKI, the private and public keys are referred to as digital certificates that are issued by PKI to its users. A digital certificate is nothing but a certificate that ensures that the user in possession of the certificate is an authentic user. A digital signature is a type of user's signature that affirms the fact that he is a legitimate user. This certificate is used to tackle the problem of non – repudiation.

Consider a user A, who places an order of goods to user B. When B has produced and delivered the required amount of goods to A, he refuses to have placed an order of goods. This state is known as non – repudiation, when a person refuses to have sent a message. To solve this kind of problem a concept of digital signature is used.

Whenever a user wants to communicate he signs the message (to be sent) with his digital signature thereby proving his identity. A digital signature is usually added as a plain text to the message that has been encrypted with the private key of the sender. This message plus the digital signature is then again encrypted using public key of the receiver.

These certificates then reach the issuing CA which then provides the users with these certificates. There are two types of keys used in this, one is private key and the other is public key.

A public key is the unique key of a user that is distributed to everyone on the network. Whenever anybody wants to sent a message to a user, that message must be encrypted by the user's public key. A private key is the secret key that stays with the user alone. This is the key with which the user decrypts the data sent to it.

Both these keys are mathematically inverse of each other, therefore data encrypted by one can only and only be decrypted by the other key and none other than that. CA has the most significant role to play in a PKI. A Certification Authority is responsible to deliver the certificates to its clients. The format of the certificate followed is known as X.509. A CA is directly attached to its clients and is responsible for the safe delivery of the certificate. Along with the user specific certificate, CA also regulates among its clients a CRL, which will be briefed in the next section.

A certification authority mainly comprises of two basic units. One being the registration authority (RA) and the other being certificate repository. The registration authority is responsible for issuing of certificates to new users. It also keeps a check on what information goes into a digital certificate and whether or not the information is correct.

The certificate repository on the other hand includes a public key database and certificate revocation list. A public key database includes the public keys of all the users that CA has certified and the certificate is up to date. This database provides the users all the public keys of other users. Hence, a user may easily send the data to his fellow users using their public key for encryption.

CA is the node in which the end users put their trust. Thus, it’s very important that a CA maintains its trust and does not let his authenticity be compromised due to any reason.

PKI infrastructure also has a concept of CRL.

1.5.1 CRL

A CRL is a list that contains all the signatures of those whose certificates have been revoked by the CA. These may be revoked either due to the fact that they have been expired or that some malicious activity was reported against that particular signature. A revocation list is a crucial part of security. It’s due to this that a user can know if the

sender sending the data is an authentic user or not. Figure 1.3 shows a sample CRL. These lists needs to be constantly managed and updated so as to keep the security of the system intact.

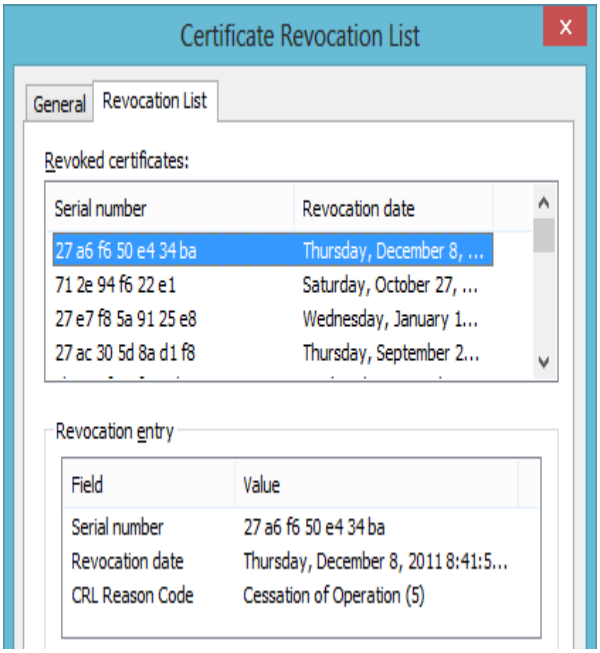

Figure 1.3 Certificate revocation list [4]

1.6 Challenges in VANETs

VANETs being a dynamic structure is faced with many a threats and structural limitations. The work done in this field is mainly to restrict any malicious activity in the network and to increase the efficiency regarding the working of the system. Following are the possible challenges of the network.

- **DoS:**

  DoS is said to occur when a huge number of requests arrive at a single point and the system is not able to take any of them. This condition forms a bottleneck in the network. DoS can be a limitation of the network or the work of an adversary to crash the particular node. Either way it's dangerous as critical information regarding further traffic density, hardware malfunction etc. cannot be circulated once the system of a node crashes.

- **Privacy preservation:**

Privacy preservation refers to the act of securing one's original information in the network. This is done to protect each node from malicious user. An intruder may access the original information of a node by eavesdropping on any conversation. This may further result in impersonation by an adversary and thus prove harmful for the network.

- **Authentication:**

  Every message received first must be verified if it is from an authentic node or not. It becomes immensely important to ensure this otherwise an adversary may broadcast a bogus message.

- **Unlinkability:**

  VANETs while ensuring security uses a PKI model to implement security. As this system involves the generation and regeneration of keys from time to time, there must be a mechanism to ensure that if ever a nod is compromised, the adversary does not get any information of the previous communications or keys.

- **Eavesdropping:**

  Eavesdropping is a technique of illegally listening to a communication. An adversary may record some messages conversed between two nodes and can easily retrieve the private or public keys from it. This can prove fatal if the messages are not encrypted.

1.7 Motivation

VANETs are upcoming technology. It involves critical data transfer amongst its nodes, i.e., Road side units (RSU) or On Board Units (OBU). Road conditions, traffic conditions, hardware malfunction, personal message etc. can all be communicated in this network. Thus, it becomes all the more important to provide adequate security this network.

As mentioned above, PKI forms the backbone of this network. PKI is a flexible system, it can incorporate any technology within itself. Since its inception in the network, there have been numerous ways to implement PKI in VANETs. One such way has been discussed in this dissertation.

1.8 Outline of Thesis

- Chapter 2 discusses the literature review involved in making the proposed scheme.
- Chapter 3 depicts the proposed scheme.
- Chapter 4 contains the implementation of the scheme.
- Chapter 5 discusses the results.
- Chapter 6 envelops conclusion and future prospects.

Chapter 2

Literature Review

2.1 Related Work

Various researchers have suggested a number of methods to mitigate the actions of an adversary with an aim to provide security in VANETs.

Raya *et al.* [5] divided the application provided on a vehicle into two major parts - that responsible for proving safety solutions like avoiding collision, giving data in presence of traffic congestion to prevent malfunctioning of vehicle and the other division being the one that provided services to the vehicle like toll tax payment, closest fuel tank indication, internet access etc. In their work they have mainly concentrated on the safety aspect of the application. They based their model on trust management and to achieve it made use of digital certificates.

In their scheme anonymous secret keys and their respective certificates were distributed prior to any kind of communication. These certificated were loaded even before the vehicle is brought on road and to avoid scarcity of certificates these had to be loaded again from time to time (yearly or so). The messages sent by a vehicle/entity could be signed using any of the provided secret key certificate, but this scheme demanded a lot of memory space on the vehicle. Moreover, while key revocation, all the certificates need to be revoked that are linked to the vehicle. This made the job tedious and CRL very heavy.

Raya *et al.* [6] *has* given importance to the physical as well as virtual safety aspect. They introduced Event Data Recorder (EDR) and a Tamper Proof Device (TPD) to tackle the security concerns related to the physical security. The EDR provides a secure storage (physically) and the TPD has all cryptographic data. All verification and trust management processes were to be done by TPD. This scheme too like the previous scheme had many keys pre-loaded into a vehicle. It also stated that the keys will change with the changing speed of the vehicle, and every key can only be used once. These keys came with a specific pre-decided life time that was managed by the CA. Now, if a vehicle had to be revoked the CA had to revoke all the keys related to the vehicle. This scheme also needed a huge memory space to implement itself and also the size of the CRL also increased. This increased the traversing time required o check if a key is revoked or not.

Sun *et al.* [7] came up with a new technique which used the concept of hashing and bilinear pairing to cater to the solutions regarding problems of efficiency and security. For this technique to function the vehicle is loaded with pseudonym certificates by the manufacturer or at a later stage. These certificates though being available cannot be used directly. The vehicle has to get an RSU's consent by the scheme of proxy re-signature to use them. This RSU only signs for its domain and not beyond it. RSU only signs a certain number of certificates at a time for a user. When revocation is done in this scheme the Tertiary Authority (TA) revokes the compromised RSU and all pseudonym certificates issued by it are revoked automatically.

Lu *et al.* [8] gave a scheme as Efficient Conditional Privacy Preservation (ECPP). This scheme was built around the idea that security and efficiency. It worked to provide efficient calculation of authenticity of safety messages and also provide anonymity to the vehicle so as to preserve privacy. It also provided an efficient mechanism to trace back the path of a bogus message by providing a three level authentication mechanism.

This technique used bilinear pairing to ensure safety of the keys produced so forth. The storage overhead produced in the OBU (On Board Unit) was much less as the keys generated were produced using bilinear pairing and elliptical curve technique. It generated short term anonymous keys to the vehicles in a particular vicinity. The computational overhead of the OBU was also much less than that proposed by other schemes of the time. Thus, this scheme made the process of message authentication much efficient and fast. The issue with this scheme was that it demanded the vehicles to stay always in the vicinity of the RSU.

Zhang *et al.* [9] came up with a new kind of verification known as batch verification. The protocol used in this scenario was Dedicated Short Range Communication (DSRC). Every vehicle would sign its messages and send the same to the RSU in the vicinity which on receiving the message would authenticate its information. This scheme makes use of Bilinear Maps to develop keys which are given to the vehicles. This scheme as they ensure, is resilient to bogus messages as it uses one time identity based signature also due to the use of pseudo ids related to a vehicle, the privacy of the vehicle is also preserved only the TA (having master keys) can trace the true identity of the vehicle. All the cryptographic information was

preserved in TPD. This scheme though used batch verification scheme which is quite efficient, but is not as efficient as a symmetric key verification scheme.

Lin *et al.* [10] have targeted the security and conditional privacy preservation in VANETs. To materialize this aim the scheme used is Group Signature [11], [12] and Identity Based Signature [13]. It uses the concept of Bilinear Pairing to produce keys. The quality of group signatures is that a certificate can be signed by any member of the group without revealing itself. Only a third party can reveal the identity of the message sender. Whenever a revocation is to occur, the revoked vehicle is intelligently removed from the network without affecting the signing capability of other participants.

This technique was functional in reducing the overhead of managing enormous number of keys at OBU and RSU. This scheme was further taken to next level in works of Boneh *et al.* [12]They used the concept of Bilinear Groups in their mechanism to produce keys. The technique being worked upon in this paper is that of Zero Knowledge Proof [14] in which the one who proves can prove the verifier that the element under verification is true without dissipating any other knowledge. This is used in coherence with Strong Diffie-Hellman (SDH) scheme. This scheme though stands undefeated on many fronts of security but comes with a large computation cost which makes it a little unviable for practical usage.

Zhang *et al.* [15] proposed a scheme that used signcryption and concept of group signatures to retrieve keys from the respective RSU. Signcryption has the advantage of both data encryption and that of digital signature. Thus, this scheme lets a user attach a signature as well as encrypt the same for maximum security. This technique gives an upper-hand in two aspects of message exchange. One being that of message secrecy and other of non-repudiation.

This scheme, as a typical group signature scheme, allows its members to send anonymous group certificates amongst themselves under the respective vicinity of an RSU. Everyone in the group has means to verify the authenticity of the group key yet identity of the signer can only be identified by its RSU. Moreover, it's nearly impossible to affirm if two massages were given by the same vehicle or not. This technique uses the mechanism of Bilinear Maps for implementation of their protocol. The scheme reduced the entire dependence of privacy on the TPD as the keys generated during communication are time variant and also space variant as every time a vehicle enters a different region of a different RSU, the group key changes. This

protocol claims to remove large computation overheads and bottlenecks in their calculation and also claims to perform well in times of dense traffic.

Sampigethaya *et al.* [16] proposed an algorithm AMOEBA to address to a major problem faced by VANETs which is of location tracking. If the location of a vehicle is tracked it gives access to its past locations as well. This being breach of privacy should thus be checked as to not give adversary any upper hand over the system. This scheme makes use of the anonymity based approach. This scheme deals with anonymity in terms of unlinkability, i.e., the two successive locations of a vehicle will not be visible to the adversary. To achieve this algorithm makes use of group concept, as mentioned earlier this concept helps keeps the privacy of the vehicle intact by issuing group certificates in a particular range of an RSU.

The main idea behind the stated algorithm is that there exist group members and a group leader. Group leader is chosen randomly and has some powers vested in it. These being that of communication between vehicles and infrastructure. The group members can exchange messages amongst themselves using a group key but to send any information to the infrastructure, i.e., RSU they need group leader. Due to this, a lot of energy including its computational resources is used up and may also result in bottleneck at the group leaders end.

A breakaway from the traditional, well defined techniques is the use of hybrid constructed algorithms. These can have various combinations of the existing techniques which involve digital signatures, pseudonymous key generations, symmetric keys, group signatures etc. The variance may also be in the bandwidth consumption on an algorithm or the delay in verification of authenticity of a node. As there are three or four basic functionalities involved in construction of a VANETs and then to provide a secure and efficient VANETs experience to its users, thus a lot of hybridism even in the process of CRL generation and its dissipation to the vehicle through the infrastructure can be indulged. Calandriello *et al.*[17] purported an algorithm using the technique of hybrid structure that combines the properties of both pseudonym signatures. A group signing key and a group public key are associated with each vehicle. Every node in the architecture generates its own pseudonym key which is then signed using the group signing key. The algorithm base used in this scheme is that of Elliptical Curve Digital Signature Algorithm (ECDSA) as algorithm to produce digital signatures. The discussed technique, though makes use self-certifying certificates which undoubtedly reduces some overhead on the key

generation technique, but as it employs group signatures and so the problems related to the much expensive checking of a huge CRL generated still persist.

Studder [18] gave a scheme called VAST using ECDSA and TESLA++. They used a modified version of TESLA [19] which they named TESLA++. TESLA++ also like TESLA used symmetrical cryptography with an added delay in key disclosure to improve security. The advantage of TESLA++ over TESLA is that the former is resilient to DoS attacks that could easily be attempted against TESLA.

The delay in authenticating a message sent by a vehicle or an RSU is very important as if the delay is too much the driver may not have ample time to react to a critical situation. This verification delay has been taken care of in VAST. The delay depends on the time when the transmitter transmits Message Authentication Code (MAC) and when the original message, key, signature etc. are sent. The verification of a message must be done using TESLA++ as it prevents a self inflicted computational DoS in the network. Also, in TESLA++ if one out of the two packets is lost, the data would not be received. To counter this VAST has a mechanism. The flaw in this whole scheme was that the proposed scheme was fast but did not provide anonymity to the system and also does not provide conditional traceability.

Wang *et al.* [20] proposed a scheme called LESPP for lightweight and efficient strong privacy preserving authentication. This scheme as claimed can be deployed in large scale implementation of VANETs. It also assures an efficient privacy preserving technique with conditional privacy preserving authenticating function. To achieve the above said features it uses symmetric key cryptography and MAC. The use of digital signature is also there but only to authenticate things at the TPD level. It was a five phase algorithm.

The first being that of system setup. In this phase, Key Distribution Centre (KDC) verifies and provides the requesting vehicle with pseudo identity and an access token though a secure channel. The vehicle first gets itself registered with the KDC by providing all its credentials like engine number, registration number etc. This information is processed and stored by the KDC. After this, the KDC generated a pseudo identity for the vehicle and appends an access code with it which is then delivered to the vehicle.

The second phase illustrates the message signing phase. The message that needs to be sent needs the sender to be authenticated first and then on being verified as true, the sender then signs the message with the pseudo identity code provided to it during

registration and sends the message with MAC appended to it. The reason as to why MAC is appended is so that the receiver can authenticate and verify the message.

Next comes the message verification phase. In this, when the receiver receives the message send by any other vehicle, it first verifies its own identity by giving a self check using the access token given to it during registration phase. After the verification is done, it then checks the integrity of the message it received by checking its MAC. If it verifies to be true then the message is accepted and acted on otherwise it is discarded. Apart from these phases there are two other phases that are a part of LESPP scheme. They are key generation and updation and vehicle revocation phase. Both these algorithms are exercised only when required.

The key generation and updation phase is the one in which the system keys need to be updated and dissipated amongst its clients. The system key is stored in the TPD of OBU of a vehicle. This TPD is such that, an adversary cannot take advantage of it even if the vehicle is stolen. This TPD has all cryptographic data related to the authentication, i.e., system key and access code. A KDC after a fixed time (say, an year) or until compromised changes its system keys to maintain the security of the network. The key after it has been generated is then sent to RSU which after updating their system broadcast the new system key. This process has the highest computational cost in the whole scheme but as it's not done on a frequent basis, it can be ignored.

The last in the list of five algorithms is the vehicle revocation algorithm. There is no particular algorithm specified for the revocation, the message containing the credentials of a revoked vehicle are broadcasted through the network. Every vehicle verifies the broadcast message containing the id of revoked vehicle and verifies with its own information. If the information matches, the TPD of the vehicle revokes itself and thereby deletes all the important data present in its TPD. If the information doesn't match, the message is ignored. This scheme uses message authentication code to preserve the integrity of the message and symmetric encryption to provide data security.

This scheme though being quite efficient does has some shortcomings. LESPP does not provide an efficient algorithm for CRL distribution. Also there is no time stamp appended with the CRL when dissipated. This poses a threat to backward secrecy. Also when the CRL is distributed within the network, a hierarchical approach is used. This results in delay in receiving the CRL and any adversary may take

advantage of this. Therefore a more efficient technique is required. This scheme has not specified as to what technique is used to check if the vehicle requesting a signature is present in the CRL or not. A comparative study of all schemes is given in Table 2.1.

Table 2.1 Comparative study of existing schemes

Name	Technique	Key Management	Vulnerabilities
Raya *et al.* [5][6]	hashing	Pseudonym keys	Memory constraints and heavy CRL
Sun *et al.* [7]	Hashing and bilinear pairing	Pseudonym certificates	Heavy CRL
Liu *et al.* [8]	ECC and bilinear pairing	Anonymous keys	Required vehicles to stay in the vicinity of an RSU
Zhang *et al.* [9]	DSRC and bilinear maps	Identity-based Batch verification	Vulnerable to DoS attack, Heavy CRL
Lin *et al.* [10]	Bilinear pairing	Group signature and identity based signature	Large computation cost
Zhang *et al.* [15]	Bilinear maps	Signcryption	Required vehicles to stay in the vicinity of an RSU
Sampigethaya *et al.* [16]	Hashing	Group Keys	Not energy efficient
Calandriello *et al.* [17]	ECDSA	Group Keys and Pseudonym signature	Heavy CRL
Studder *et al.*[18]	ECDSA and TESLA++[13]	Symmetric Key	No privacy preservation
Wang *et al.*[20]	Hashing	Symmetric Key	Weak backward secrecy

2.2 Problem Statement

VANETs being a network of high dynamicity has challenges of security and efficiency. For a complete implementation of it in the real world all the possible threats need to be taken care of.

The schemes discussed so far have though brought the goals of complete security and efficiency a little closer, they do have some shortcomings. The schemes given discuss many technologies, some involving pure structures and some working on hybrid structures to bridge the needs required for smooth functioning of the network. However, there exists some gaps like, if the security is increased the computational cost also increases. These problems have gained much attention of researchers. Thus, a system is required that while managing the huge overheads produced also provides an immaculate security.

2.3 Objective

An effort has been done, to resolve the issues mentioned above and to make it more efficient and secure while maintaining feature of light weight computations so as to apply it the proposed scheme to a larger network.

Chapter 3

Proposed Scheme

This section explores the proposed scheme in detail as follows.

3.1 Network model

Figure 3.1 shows the network model used in the proposed scheme. As mentioned above, in VANETs there are two types of communication viz. V2V, and V2I. To manage these communications, three types of network units are used namely as KDC, RSU, and Vehicles containing TPD in OBUs.

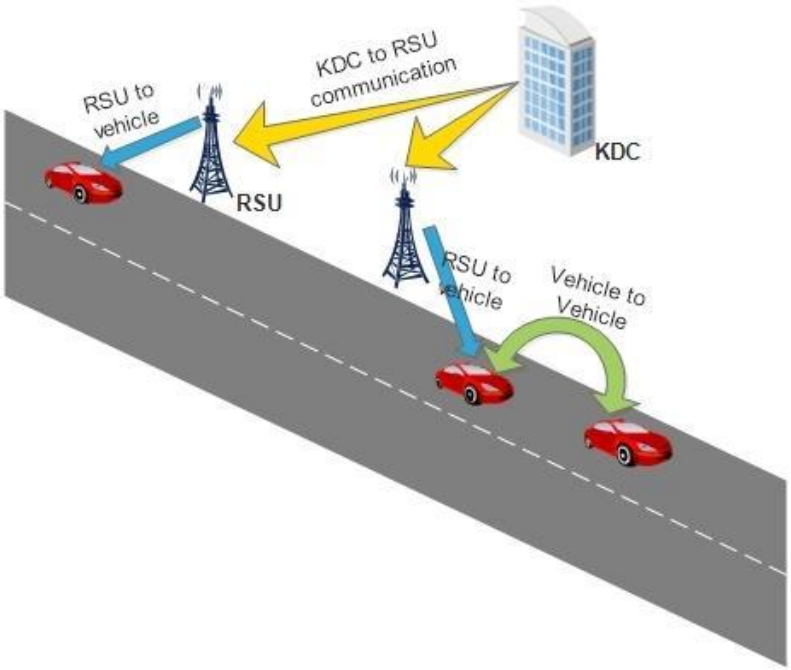

Figure 3.1 Network model

KDC is the main unit on which the whole authentication system stands. It is trusted by all other units. KDC provides the authentication of RSU, and do the **vehicle registrations. [20]. RSU are the mediating bridge between vehicles and KDC.** Any kind of information that KDC needs to sent to vehicles is broadcasted by RSU. RSU is used to distribute the System keys generated by the KDC and most importantly it also broadcasts the certificate revocation information to the vehicles. Vehicles are the basic unit of the network model and the most vulnerable ones.

Vehicles contain OBUs having TPD, used to contain all crucial information (cryptographic information) in it. This information is the authentication information provided to the vehicle by KDC. This tamper proof device is fully secure from any kind of adversary action [20].

3.2 Type of communication

There are two types of communications required in the scheme *viz.*V2V and V2I. They are as under:

- **V2V:**

  This is a short range communication and is functional between two or more vehicle. These include technologies like Bluetooth, ZigBee, Radio Frequency Identification (RFID), Infrared Communication etc.

  V2I:

  This is a long range communication. This is the type of communication that exists between RSU and Vehicles or KDC and RSU. This includes technologies like WIFI, WIMAX etc.

3.3 Design goals

In the given scheme, an effort has been made to achieve the following properties related to VANETs that provide an efficient and secure functioning of the network.

- **Dos resilient**

  An algorithm design in VANETs must be such that it can resist bottleneck like situation. VANETs being a network of many nodes who are very dynamic in nature, it becomes necessary that any kind of computation involved in the scheme should be fast enough to handle huge bombastic nature or requests with ease.

- **Authenticity**

  In VANETs, it becomes crucial to authenticate a sender so that the information received is not bogus. This network also houses critical traffic messages of congestion, accident or such. So, it becomes important to verify that the message received is from an authentic source.

- **Privacy preservation**

  As much as the authenticity of a sender matters, its privacy should also be maintained. This rules out the possibility of impersonation or any kind of data theft. If only the concept of digital signature is used, the privacy can be endangered resulting due to broadcast nature of the network.

- **Conditional traceability**

  Anonymity being an important aspect, there also has to be a mechanism to trace the original identity of a vehicle. RSU and vehicles can practice anonymity but KDC should have all access to the actual information of each node.

- **Backward secrecy**

  If ever there exists a condition in which a node is compromised, the adversary should not have access to any kind or old keys that must have been used by the node.

3.4 Attack model

It is assumed that an adversary is capable of capturing and monitoring the data transfer in the environment. this adversary is equipped enough to listen to the convocation between vehicles or infrastructure, may also deliver bogus information to them, can impersonate any node in the network, capable of discarding any message exploit the network for its leisure and personal interest.

3.5 Proposed scheme

Following are the algorithms that are used in the scheme for authenticating the existence of a verified vehicle and not an adversary. There are five algorithms in total for five different phases. They being, the system setup phase, the message signing phase, the message verification phase, the key generation and updation phase, the vehicle revocation phase.

3.5.1 System setup

This is the first phase in the proposed scheme. In this scheme, a vehicle firstly sends its information to the KDC through a secure channel and then waits for the KDC to authenticate it. The KDC after creating a pseudo identity of the vehicle by using its

original information sends the pseudo identity and other such parameters along with the access code, which is crucial for any kind of communication to be carried out in the future through a secure channel. All this cryptographic information is stored in the TPD present in the OBU of the vehicle.

Table 3.1 Notations and symbols

Symbols	Meanings
$\|\|$	Contention operation
KDC	Key Distribution Centre
$\mathbf{Sys_{pu}}$	System Public Key
$\mathbf{Sys_{pr}}$	Private key of KDC
$\mathbf{veh_i}$	i^{th} vehicle
$\mathbf{TPD_i}$	Tamper Proof Device of i^{th} vehicle
Y	A cyclic additive group
C	A cyclic multiplicative group
$\mathbf{k_m}$	System Key
Ts	Time stamp
Msg	Message
$\mathbf{Identity_i}$	The real identity of i_{th} vehicle
$\mathbf{Identity_{KDC}}$	Identity of KDC
$\mathbf{PI_i}$	Pseudo identity of vehicle i
$\mathbf{Info_i}$	Information of i_{th} vehicle
h(.)	hash function, $h : (0,1)^* \times C \rightarrow Z_q$
$\mathbf{h_k^1(.)}$	hash function $h_k : 0,1 \rightarrow 0,1^n$
H(.)	hash function $H : 0,1 \rightarrow 0,1^n$
$\mathbf{e_k}$	Encryption function using k as key
$\mathbf{M_k(.)}$	MAC computation function using k as key
$\mathbf{m_{msg}}$**, ts**	message authentication code of message msg at time ts
$\mathbf{S_k(.)}$	Identity based msg signing

Algorithm1: Vehicle Registration

Input: $Identity_i$, PI_i, $Info_i$, Sys_{Pu}, Sys_{Pr}, ts, k_m

Output: Vehicle Registration

Assumptions: The KDC is already initialized and has a Sys_{Pu} and Sys_{Pr}

$Vehicle_i$ sends $Identity_i$, $Info_i$ to KDC.

if ($Identity_i$ = valid and $Info_i$ = valid) **then**

KDC generates a random pseudo Identity PI_i

KDC generates $r_i = Sign_{S(identity)KDC}$ ($Identity_{i)}$.

KDC saves vehicle information.

KDC loads Sys_{Pu}, $Identity_{KDC}$, $Identity_i$, γ_i, ts, k_m, PI_i On TPD

KDC sends $Identity_i$, γ_i as access token to the owner

else

Exit

end if

3.5.2 Message signing

In this phase, the sender node (vehicle) signs the message it wants to send. This signing of the message is done only after the vehicle has authenticated itself by matching its access code with present in the TPD. This drill is done so as to remove any doubt of presence of an adversary thereby checking the impersonation attack. After the self verification has been done, it also appends MAC with the message so that the receiver can check the integrity of the message received.

The detailed algorithm for the same is as follows:

Algorithm 2 : Message Signing

Input: $Identity_i$, γ_i,msg,

Output: Message signed

$Vehicle_i$ compares its access token with its own TPD

if (($Identity_i$, γ_i) = invalid) **then**

Exit

else

If access token returns valid

Generate current pseudo identity,

$ePI = e^1_{km}$ ($PI_{i,ts}$)

Compute $m_{msg,ts}$, M_k(msg)

Exit

end if

3.5.3 Message authentication

In this phase, the receiving node (vehicle) is to check the authenticity of the message received and then receive the message. Firstly, the receiver authenticates itself with the help of a verification check using access code access token given to it by the KDC and comparing it with the one present in TPD. After the verification is done the receiver node checks the integrity of the message by calculating the hash of the message and then comparing it with MAC appended with the message.

The algorithm is as follows:

Algorithm 3: Message Authentication

Input: $Identity_j$, γ_j, msg, $m_{msg;ts}$, $ePI_{i,ts}$

Output: Message verified

Access token verification

if (Access token = invalid) **then**

Exit

else

Compute $m^0_{msg;ts} = M^0_{kts}$ (m)

Check $m^0_{msg;ts}$?= $m_{msg;ts}$

if true then $vehicle_j$ accepts the msg.

end if

3.5.4 Key generation and updation

The KDC for the purpose of security, keeps updating its keys. The system key generated by the KDC is appended with the time stamp, so as to know exactly when the system key was changed and to avoid any malicious intruder from getting into the network with an outdated system key. After generation the key with the digital signature or the KDC is broadcasted to the RSU which after making changes in their database broadcast the same in their respected vicinity.

The detailed algorithm for this phase is described as follows:

Algorithm 4: Key generation and updation

On KDC

KDC generates a new k_m and associated to it.

$f = e^{1}_{km}$ (ts || $Identity_{(KDC)}$ || k_m^*)

$r = Sign_{S(identity)KDC}(f)$

(f,r) are broad-casted

On vehicles

(ts || $Identity_{KDC}$ || k^o_m) = $d_{km}(f)$

if (ts ts) **then**

Exit

else if (($identity_{KDC}$) != $Identity_{KDC}$) **then**

Exit

else if (1 != $verify_{identityKMC}$ (f, γ)) **then**

Exit

else

$k_m = k^o_m$, $ts = ts^o$

end if

3.5.5 Vehicle revocation

In this phase, the information of the revoked vehicle is sent to other nodes. In their paper, Wang *et al.* [20] used only vehicle to RSU communication to sent the revocation information.

To speed up the process, the usage of an epidemic approach is proposed, as shown in Figure 3.2, in sending the revocation information. By epidemic approach, the information is meant to be send by using both RSU V2I as well as V2V communication. Moreover, Wang *et al.* [20] have not specified any data structure to store the CRL on RSU. Hence, the usage of Bloom filter as data structure to store the CRL is proposed.

Bloom filter [16] is a space efficient probabilistic data structure used to test if an element is part of the set or not. There is a possibility of false positive but never a false negative, i.e., if the set is that of certificate revocation lists, a vehicle revoked will definitely be a part of the list. It has a constant computation cost of O(1) for insertion as well as search operations. Also, an additional parameter, time stamp (t_s), has been included to ensure full backward secrecy.

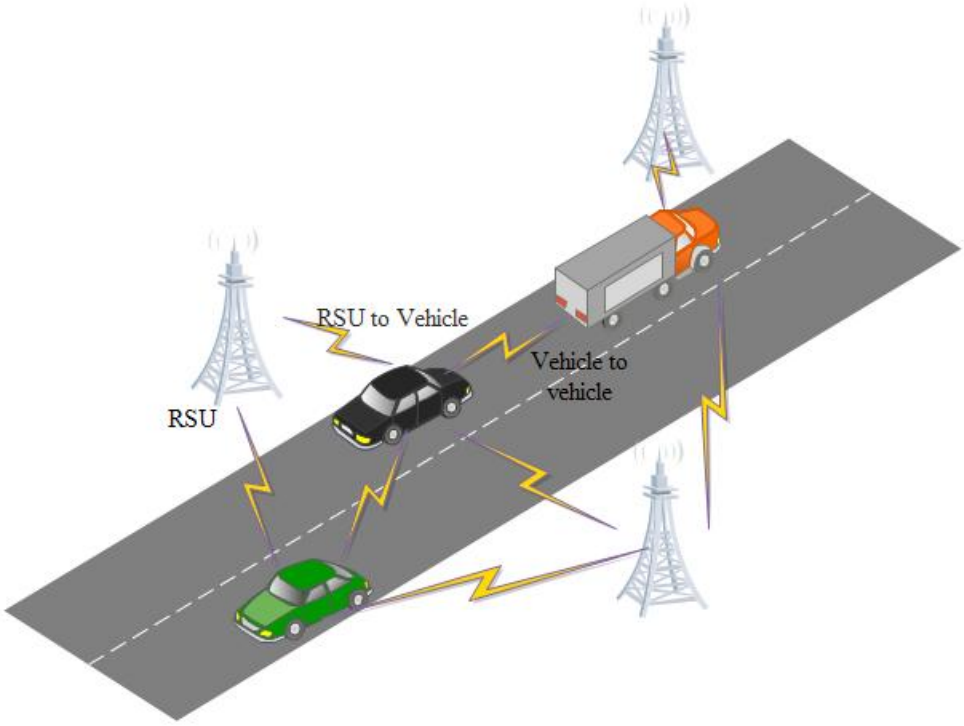

Figure 3.2 Schematic diagram of epidemic approach of data dissipation

The detailed description of the same is provided in the following algorithm:

Algorithm 5: Vehicle Revocation

Input: ts, γ_i, PI_i

Output: Vehicle revoked

KMC broad-casts (PI_i, γ_i, ts)

if ((PI_i, γ_i) = (PI_i^o, γ_i^o)) **then**

    $Vehicle_i$ deletes all data from TPD

else

    Exit

end if

Chapter 4

Implementation

In this chapter, the proposed scheme is implemented using Opportunistic Network Environment (ONE) [21].

ONE is a sophisticated simulation environment which is capable of providing a space to virtually implement VANETs. This involves simulation of nodal movement in the network. It also enables a user to enforce different routing protocols. This simulation application also lets a user see the communication between nodes.

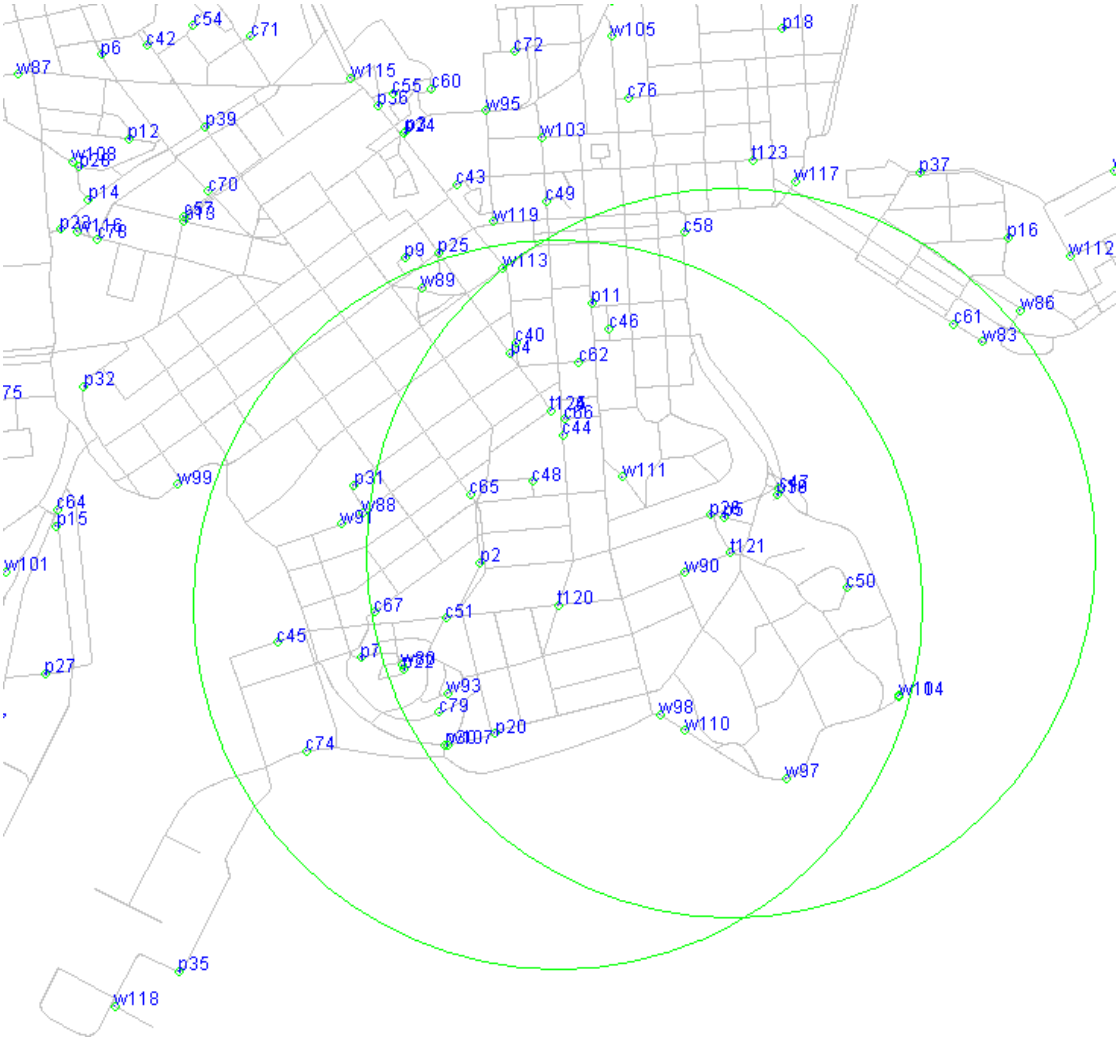

Figure 4.1 City Map with nodes on ONE

It's a java supported application available for free of cost, which can be downloaded in appropriate format (Linux and Windows) from the following website:

http://www.netlab.tkk.fi/tutkimus/dtn/theone/

This URL (Uniform Resource Locator) also contains some tutorials for setting up the environment in the system. This simulator supports two modes: Graphic User Interface (GUI) and Batch Mode. For convenience, GUI has been used in the implementation.

To infer the execution of the proposed scheme, an actual city map is considered in ONE. The default map given in ONE is used here. The specifications for simulation have been given in a table below.

Table 4.1 Simulation specification

Types	Parameters
Scenario	City streets
Communication range	300m
Time	200s
Channel Type	Wireless Channel
Bandwidth	2Mbps
Traffic Type	TCP
Wait time	0-5s

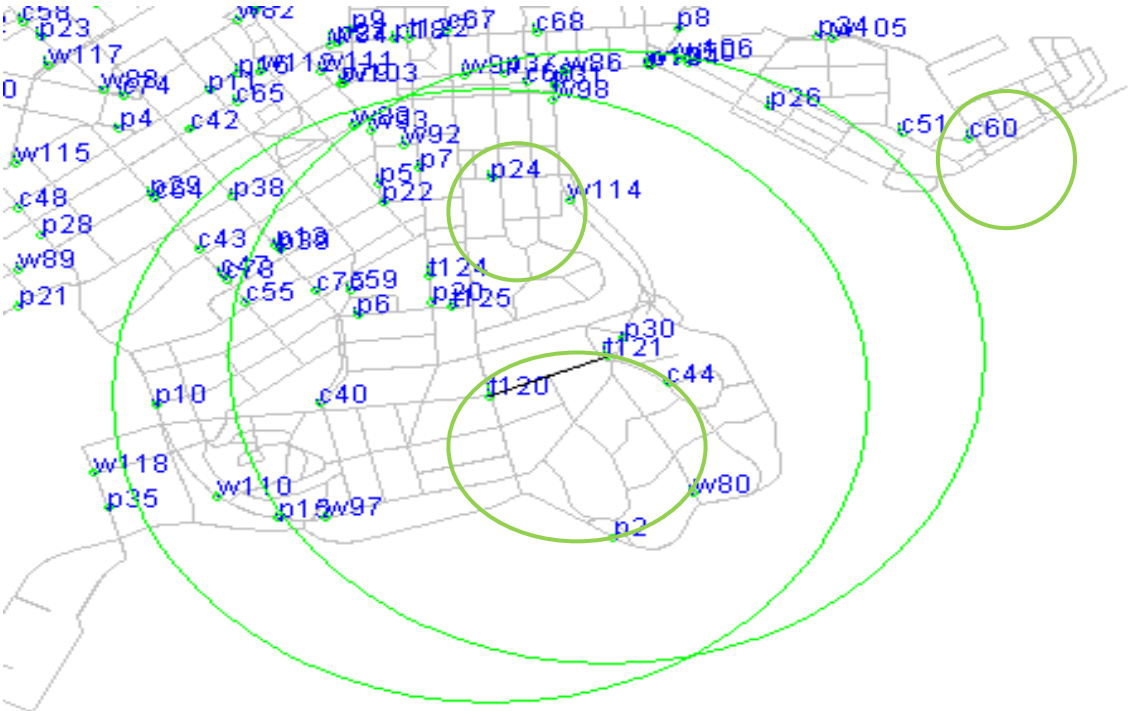

Figure 4.2 Movement of nodes

Next, each node (vehicle) will be equipped with an algorithm based on Dijkstra algorithm to find the SPF (shortest path first). Each vehicle is placed randomly on the map. On the execution of the whole scenario, each of this node will move towards a random decided point at a speed pre-decided. After the completion of first target the nodes will identify the next target and move towards it. This drill continues until the simulation is in process. The functions under observation will be average message delay, average message loss and percentage signature verification.

Chapter 5

Results and Discussions

5.1 Performance analysis

Performance evaluation is done based on the simulation carried out on ONE. The performance of the algorithm is measured with respect to some other algorithms such as VAST, LESPP and the new proposed scheme hereby called as Efficient Lightweight and Efficient Strong Privacy Preserving Authentication (ELESPP) for comparison purposes. By calculating the data received in simulation, the graph comparing the four schemes mentioned earlier is as follows:

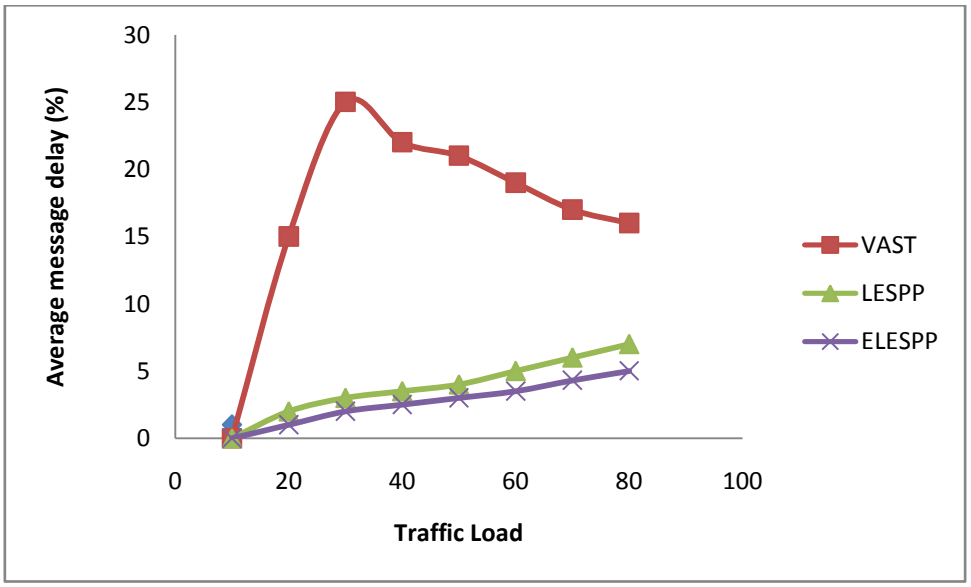

Figure 5.1 Average message delay versus Traffic load

Figure 5.1, depicts a graph of the average message delay with increase in traffic density. Now, more the message loss ratio less will be the efficiency of the scheme. VAST, shows a very huge deflection and then later on it stables. This is due to the fact that VAST using heavy calculations is prone to DoS attack. LESPP on the other hand shows very little deflection as it uses a hierarchical approach to send CRL. ELESPP shows the least deflection amongst the three as the scheme uses an epidemic approach to send CRL.

Next parameter to be evaluated was average message loss ratio with respect to traffic load. The graph in Figure 5.2 compares the above said parameter amongst the three schemes.

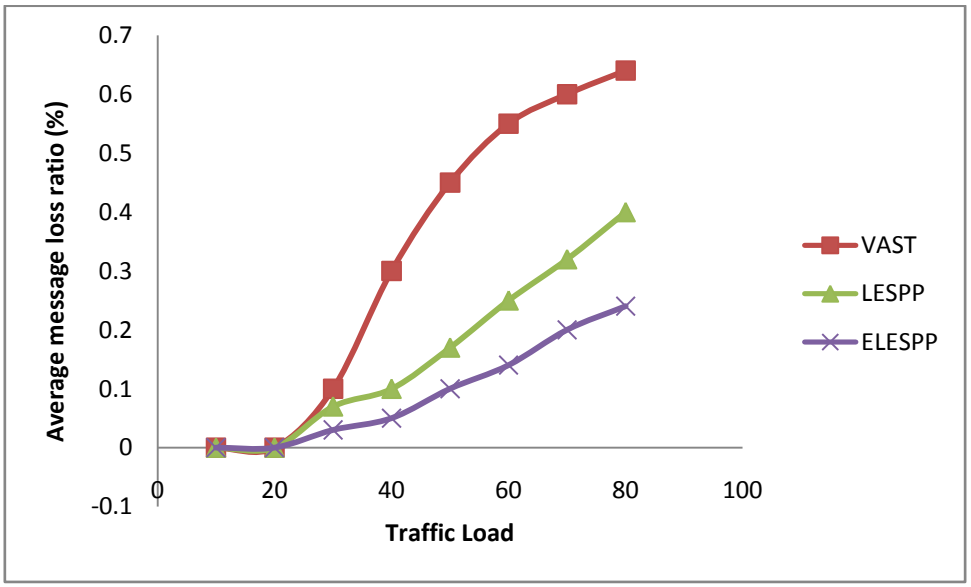

Figure 5.2 Average message loss versus Traffic load

In the graph, VAST shows some consistency in maintaining a loss less communication in the beginning but as the traffic increases the average message loss ration also increases. LESPP though is more efficient than VAST but still has some issues regarding message loss during communication. ELESPP with the use of epidemic approach in delivering the message show less message loss rate.

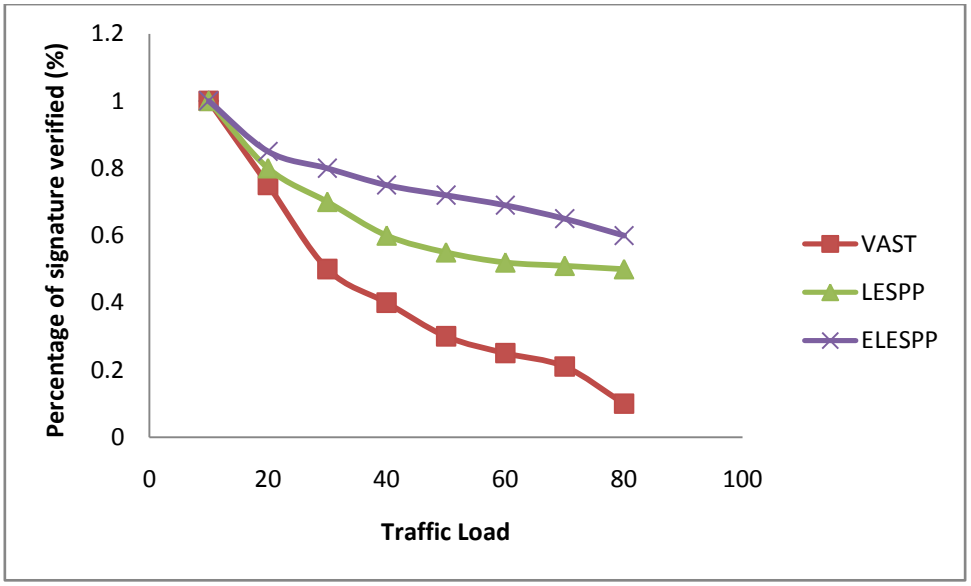

Figure 5.3 Impact of traffic load on message delay

Figure 5.3 shows the graph of percentage of signature verified. VAST starts with 50% in the beginning but declines gradually as the load increases. LESPP scheme is very efficient as it uses a light weight mechanism to test the authenticity of the node. Thus, it can verify more signatures in comparison to VAST. There is not much a gap between LESPP and ELESPP, but as ELESPP uses Bloom filters and epidemic approach along with the light weight algorithm of LESPP, it shows to be more efficient than LESPP. Some changes that were made in proposed scheme that are different from the existing scheme of LESPP are mentioned below:

- **Appending time stamp to revocation list:**
  This ensures that no message of the revoked vehicle is either accepted after the revocation or rejected before the event of revocation occurred.
- **Using Bloom Filters:**
  In proposed scheme, Bloom filters are used as the data structure to store the certificate revocation list at RSU. Bloom filters use hashing to check the existence of an element. Moreover, insertion and search computation cost is O(1), making it the best suited data structure to store, and maintain the CRL.
- **Epidemic approach:**
  In the previous scheme, the CRL is broadcast by RSU to the Vehicles. To enhance the speed of the process I suggest that epidemic approach should be used, i.e., CRL should be send using both Vehicle to RSU as well as V2V communication.

Table 5.1 Performance analysis

Attack Types	VAST[18]	LESPP [20]	Proposed Scheme
Communication Overhead(byte)	145	43	43
Key updation overhead	63	88	88
Vehicle revocation communication overhead	126	63	71

5.2 Security analysis

This section provides an analysis of the proposed scheme with respect to various types of attacks in the network.

- **DoS Resilient:**

  The algorithm uses MAC to check and guarantee the integrity of the message sent. This message authentication code is calculated using a lightweight symmetric encryption hashing algorithm. In the due course of the whole scheme the techniques used are MAC, symmetric key cryptography and hashing. All of these are very lightweight technologies as compared to the asymmetrical key management structure. Due to this, no matter how many requests are generated, the traffic can always be managed. Thus, this technique can be safely said to e DoS resilient.

- **Masquerade attack:**

  The proposed algorithm uses the concept of pseudo identity for each vehicle which is encrypted with system key k_m. This system key k_m is stored on the tamper proof OBU, i.e., even if the vehicle is stolen, the adversary cannot breach the security of the vehicle. Moreover, the original details of the vehicle are stored in the KDC and not openly on the vehicle. Since I have assumed that KDC is the entity trusted by all parties so, an adversary cannot take advantage of the KDC. Thus, masquerade or spoofing attacks are not possible on the proposed scheme.

- **Level 3 privacy:**

  The proposed algorithm provides level three privacy. It takes care of authentication, anonymity, and unlink ability. This is taken care by the fact that pseudo identity given to the units is time variant and knowing any pseudo identity cannot reveal any potential information to the adversary.

- **Strong privacy preservation:**

  In the described algorithm, every vehicle is provided a pseudo identity by the KDC via a secure channel. Even RSU do not have any knowledge of a vehicle's real identity, thereby preserving the vehicle's privacy. In addition to this, every message sent has a message authentication code linked to it. Thus, any kind of modification is not possible by the adversary.

- **Backward secrecy**:

  The proposed algorithm ensures backward secrecy as every time a CRL is sent, the revoked vehicle deletes all its data from the OBU, so that the adversary cannot take advantage of the information related to KDC, or real identity of the vehicle. Moreover, I have appended a time stamp with every revocation information sent by the KDC by RSU, thereby making it more efficient in preserving the privacy. Table 2 provides the analysis of the proposed scheme with respect to various performance evaluation metrics.

Table 5.1 Security Analysis with referred Scheme

Attack Types	**LESPP Scheme [20]**	**Proposed scheme**
Dos resilient	Yes	Yes
Masquerade Attack	No	No
Level 3 Security	Yes	Yes
Strong Privacy Preservation	Yes	Yes
Backward Secrecy	No	Yes

Chapter 6

Conclusion and Future Scope

6.1 Conclusion

With the Internet and related technology, there has been an emergence of the one of the most popular networks called as VANETs. Due to high velocity, and varying densities, security always remains as one of the biggest challenges in the environment. So, there is requirement of an efficient solution to provide security for various applications in this environment. In this dissertation, an enhanced security scheme for VANETs is proposed by modifying the already existing algorithm by Wang *et al.*[20]. The algorithm proposed by them had minor flaws which could put the integrity of the system at stake. Those pitfalls have been covered and new changes are suggested in the existing solution. The results obtained confirm that the designed scheme outperforms the existing solutions with respect to various types of attacks in the network.

6.2 Future scope

A new technology is shaping called the internet of things (IOT). This technology aims at bringing the objects around us in compliance with internetwork. This encompasses smart homes, smart cities, smart cars, smart health etc. I would like to take the proposed scheme in this dissertation one step further and try and implement it in IOT. With IOT smart cars can be built that do not just give a more secure communication network but also can give an automated drive experience. Therefore, this scheme can help enhance the efficiency of the overall system.

References

[1] D. Jiang, L. Delgrossi, “IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments,” In Vehicular Technology Conference, 2008, pp. 2036-2040.

[2] "Wireless History Timeline" [online] Available: http://www.wirelesshistoryfoundation.org/wireless-history-project/wireless-history-timeline [Accessed on June 1, 2015].

[3] Rouse M., “Asymmetric Cryptography (public-key cryptography)”, Rouse M., June, 2008, [online]. Available: http://searchsecurity.techtarget.com/definition/asymmetric cryptography [Accessed: MAY 2014].

[4] Jeff Schertz, “Certificate Revocation in Lync 2013", [online] 28 February 2013, Available: http://blog.schertz.name/2013/02/certificate-revocation-lync-2013/ [Accessed: December 2014].

[5] M. Raya, J. Hubaux, “The security of vehicular ad-hoc networks,” Proceedings of the 3rd ACM workshop on security of ad-hoc and sensor networks, Switzerland, pp 11-21, 2005.

[6] M. Raya, P. Papadimitratos, JP. Hubaux, “Securing Vehicular Communications,” IEEE Wirel Commun, vol: 13(1), pp 8-15, 2006.

[7] Y. Sun, R. Lu, X. Lin, XS. Shen, “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communication,” IEEE Trans Veh Technol, vol: 59(1), pp 3589-3603, 2010.

[8] R. Lu, X. Lin, H Zhu, P Ho, XS Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications", Proceedings of INFOCOM, pp 1229–1237, 2008.

[9] C. Zhang, R. Lu, X. Lin, P. Ho, X.S. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," Proceedings of Infocom, Ontario, pp 246-250, 2008.

[10] X. Lin, X. Sun, P. Ho, X.S. Shen "GSIS: a secure and privacy preserving protocol for vehicular communications". IEEE Trans Veh. Technol. Vol: 56(1):3442–3456 (2007)

[11] D. Cham, E. Heyst, "Group Signatures," Proceedings of 1991 advances in cryptology-EURO-CRYPT, Brighton, pp 257-265, 1991.

[12] D. Boneh, X. Boyan, H. Shacham, "Short group signatures," Proceedings of 2004 CRYPTO, California, pp 257-265, 2004.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," Proceedings of 1984 advances in CryptologyCrypto, Springer, New York, 47-53, 1984.

[14] S. Goldwasser, S. Micali and C. Rackoff, "The knowledge complexity of interactive proof-systems," Proceedings of 17th Symposium on the Theory of Computation, Providence, Rhode Island. 1985.

[15] L. Zhang, Q. Wu, A. solanas, F.J. Domingo, "A scalable robust authentication protocol for secure vehicular communication," IEEE Trans Veh Technol, vol: 59(1), pp 1606-1617, 2010.

[16] K. Sampigethaya, M. Li, L. Huang, R. Poovendran, "AMOEBA:robust location privacy scheme for VANET," IEEE J Sel Areas Commun, vol : 25(1), pp 1569-1589, 2007.

[17] G. Calandriello, P. Papadimitratos, J. Hibaux, A. Lioy, "Efficient and robust pseudonymous authentication in VANET," Proceedings of 2007 the fourth

ACM international workshop on Vehicular, ad hoc networks, New York, 19-28, 2007.

[18] A. Studer, F. Bai, B. Bellur, A. Perrig, "Flexible, extensible and efficient VANET authentication," J Commun Netw, vol: 11(6), 2008.

[19] A. Perrig, R. Canetti, J.D. Tygar, D. Song, "The TESLA broadcast authentication protocol," Proceedings of RSA CryptoBytes, 2002

[20] M. Wang, L. Dan, L. Zhu, Y. Xu, F. Wang, "LESPP: lightweight and efficient stromg privacy preserving authentication scheme for secure VANET communication," Springer-Verlag Wien, 2014.

[21] A. Keranen, J. Ott, T. Karkkainen, "The ONE simulator for DTN protocol evaluation," Proceedings of the 2nd international conference on simulation tools and techniques, 2009.

[22] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol: 13(7):422-426, 1970.

Publication

1. Navkiran Kaur Mann, Neeraj Kumar, "An Enhanced Secure PKI Authentication Scheme For Vehicular Ad-Hoc Networks", Springer International Conference on Emerging Research in Computing, Information, Communication and Applications (ERCICA-15), Nitte Meenakshi Institute of Technology, Yelahanka, Banglore, India, 2015. **[Accepted and yet to Presented]**

Video Link

https://youtu.be/2LTpXsbWn3E

Plagiarism Report

Turnitin Originality Report

hanced Secure PKI Authentication Scheme for Vehicular Ad-Hoc Networks by Navkiran Mann

From Thesis (ME 2013-2015 Batch)

Processed on 11-Jul-2015 02:16 IST
ID: 555038095
Word Count: 10186

Similarity Index	Similarity by Source	
8%	Internet Sources:	7%
	Publications:	3%
	Student Papers:	0%