
A Novel Pairing-Free Authentication Scheme for
Vehicular Sensor Network



MS Thesis

By

Ashiq Hussain

799-FBAS/MSCS/F14

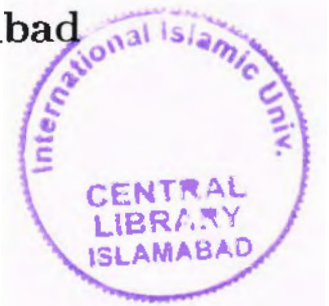
Supervisor

Dr. Shehzad Ashraf Chaudhry
Assistant Professor DCS&SE, FBAS, IIU

Department of Computer Science & Software
Engineering

International Islamic University, Islamabad

2018



MS

625.794

HUA

Sensor

1- vehicular

2- sensor network

*A dissertation submitted to the
Department of Computer Science & Software Engineering,
International Islamic University, Islamabad
as a partial fulfillment of the requirements
for the award of the degree of
Master of Science in Computer Science.*

**Department of Computer Science & Software Engineering
International Islamic University Islamabad**

Date: 18-01-2018

Final Approval

It is certified that we have examined the thesis report submitted by Mr. Ashiq Hussain, Registration No. 799-FBAS/MS(CS)/F14, and it is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University, Islamabad for the Master of Science in Computer Science.

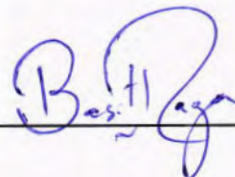
Committee:

External Examiners

Dr. Basit Raza

Assistant Professor

Department of Computer Science & Faculty of Information
Science, COMSATS, Islamabad

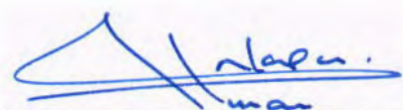


Internal Examiner

Dr. Syed Husnain Abbas Naqvi

Asst. Professor

Department of Computer Science & Software Engineering
International Islamic University Islamabad

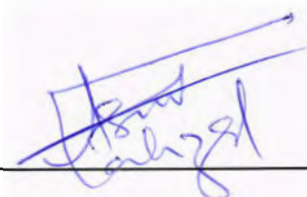


Supervisor

Dr. Shehzad Ashraf Chaudhry

Assistant Professor

Department of Computer Science & Software Engineering
International Islamic University Islamabad



Declaration

I hereby declare that this thesis, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that no portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Ashiq Hussain

Acknowledgments

I am very grateful to *ALLAH* the *ALMIGHTY* for without His grace and blessing this study would not have been possible.

Foremost, I would like to express my sincere gratitude to my supervisor *Dr. Shehzad Ashraf Chaudhry* for the continuous support of my MS study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my MS study.

I would also like to acknowledge my friends, and colleagues. All of them encouraged and provided logistic and technical help during this research.

I would like to admit that I owe all my achievements to my truly, sincere and most loving parents and friends who mean the most to me, and whose prayers have always been a source of determination for me.

Abstract

Increasing number of vehicle in metropolitan cities people are migrating towards cities due to having good health facilities, social security and good job . So Government agencies are taking step in VANET as Intelligent Transportation system (ITS) to maintain and control the traffic system in future. Vehicular adhoc network working process is same as mobile adhoc network but the key difference between them is that in MANET we have to consider the battery problem and space, but in VANET the vehicle are carried huge battery, that is enough for our sensors. The problem in VANET is that communication time is short. Vehicular Adhoc Network (VANET) is introduced to control the traffic system. Existing system has many problem such as road block, time consuming, ambulance can not find the shortest and right route that is not blocked. Drivers has no update about route if somewhere occur incidents. Passengers have internet service . There is no forecast information available for driver of different places. As compare to existing system VANET are very useful for traffic system. Driver can get information about forecast of weather, can guide the extract route that is short and not block. Ambulance can get the easy route. VANET provide alternative routes if some route is block. Police can get information about incident and crime. Vehicle communicate with wireless enabled road side unit (RSU) to share message to other infrastructure. No vehicle can't transfer the wrong message in traffic system because each vehicle and message will be authenticated and signed before sending to others. And also check for any changing occurrence before receive to valid recipient. We have focused on reduction of cost of scheme main in signature generation. Lo and Tsai work has reduced the computation and communication cost as compared to previous work but we can reduce the computation time more. Lo and Tsai has not used pairing operation. Our proposed scheme also not use pairing operation but in signature generation our proposed scheme has reduce 1 pairing operation as compared to Lo and Tsai operation. So our proposed scheme has eliminated repetition of pairing operation in signature generation.

Contents

1	Introduction	1
1.1	Preliminaries	3
1.1.1	Cryptography	3
1.1.2	Elliptic Curve Cryptography(ECC)	5
1.1.3	Attribute-Based Encryption	5
1.1.4	Bilinear Pairing	6
1.1.5	Identity-Based Cryptography	6
1.1.6	Hash Function	7
1.1.7	XOR	8
1.2	Objectives	8
1.3	Thesis outline	8
2	Literature Review	9
2.1	The review of the scheme of Zhang et al	10
2.1.1	Identity Generation	11
2.1.2	Message Signing	11
2.1.3	Batch Verification	12
2.2	Shim et al scheme review	12
2.2.1	System Parameter Setup	12
2.2.2	pesudo identity generation and private key extraction	12
2.2.3	Message Signing	13
2.2.4	Batch Verification	13
2.3	Shurong etc scheme review	14
2.3.1	Road Side Unit Certificate Issuing	14
2.3.2	Vehicle anonymous and private keys generation	14
2.3.3	Mutual authentication and Secure group key distribution	15
2.4	Lo and Tsai scheme review	15

2.4.1	Setup	15
2.4.2	Extract	16
2.4.3	Signing of message	16
2.4.4	Verification	17
2.4.5	Batch Verification	17
2.5	Problem Statement	18
2.6	Chapter Summary	18
3	Proposed Scheme	19
3.1	Setup	19
3.2	Extract	19
3.3	Sign	20
3.4	Verification	20
3.5	Batch Verification	20
3.6	Chapter Summary	21
4	Security Analysis and Computation Cost Analysis	22
4.1	Security Analysis	22
4.1.1	Security Analysis with ProVerif	22
4.1.2	Informal Security Analysis	25
4.1.3	Security Requirements and Comparison	29
4.1.4	Security Requirements	29
4.2	Computation Cost Analysis	29
4.3	Chapter Summary	32
5	Conclusion and Future Work	33

List of Figures

1.1	Structure of Vehicular Sensor Network	3
1.2	Asymmetric Cryptography	4
1.3	Public Key Infrastructure	5
1.4	Attribute Based Encryption	6
1.5	ID-based PKC	7
1.6	Hash Function	7
4.1	Communication cost of proposed scheme	32

List of Tables

2.1	Notation Guide	16
4.1	Security requirements table	30
4.2	Comparison of computation cost and running time	31

Chapter 1

Introduction

Wireless Sensor Network is a distributed autonomous sensors. It is used to check and observe the environmental and physical states like sound, pressure, temperature. They cooperatively share their data to each other and to other location via network. Wireless sensor network is a combination of nodes and they are connected in a network. Every sensor is composed of a radio transceiver, an internal antenna. Internal antenna is connected with external antenna, a micro controller board that interfaces with sensor. Applications of Wireless sensor network are area health care monitoring, monitoring, earth sensing (air pollution sensing and , Land sliding forest, fire detection, water quality monitoring and data center monitoring). Main characteristics of WSN are, power consumption of nodes, resilience, mobility of nodes, heterogeneity of nodes, same properties nodes, large deployment of nodes, withstand in difficult conditions and environment, easy to use. One of the major tasks of WSN is to produce low cost and tiny sensors. There are three topologies used in wireless sensor network. In star topology there is a gateway and each node is connected with gateway. In cluster tree topology, every node is directly connected with one higher node and then connected to gateway and data is transferred from lower node to higher than gateway. In mesh network a node can connect to multiple nodes and data can be sent to a reliable route. Vehicular Adhoc Network (VANET) is based on the principles of mobile adhoc networks, for creation of wireless network for data exchange of data in area of vehicles. Vehicular adhoc network was first introduced in 2001 with car to car communication and network application. VANET is very important and key part of Intelligent Transportation System (ITS). VANETs are referred to as intelligent transportation networks. Examples of VANET are electronic brake lights, Traffic information system, platooning, on-the-road services. Rapid enhancement in Mobile Adhoc Network, (MANET) introduced the Vehicular Adhoc Network in Vehicular Sensor Network (VSN). VANET has been introduced to control the traffic system due to increasing number of vehicles in metropolitan cities

due to having good health facilities, society security and good job opportunities people migrating towards to cities. So Government agencies are taking step in VANET as Intelligent Transportation system (ITS) to maintain and control the traffic system in future[1]. VANET based on MANET but the key difference between them is that in MANET we have to consider the battery problem and space, but in VANET the vehicle are carried huge battery, that is enough for our sensors. The problem in VANET is that there is short communication time. The VANET composed of On-Board-Unit, Road-Side-Unit and Trace Authority (TA). In VANET, all the vehicles have On board unit (OBU). OBU can communicate via Wifi or Wimax, because OBU is pre equipped with communication module, and it can communicate with other vehicle and infrastructure by wireless communication. OBU share the instant messages as the speed of vehicle, temperature, direction to the driver and other infrastructure for safety. The RSUs are fixed on road side of highways and it broadcast instant message for vehicle and TA and also receive the message from the vehicles by wireless communication. RSU can monitor and summarize the the traffic related message just like the direction and position/location of vehicle and send to traffic control center. In VANET there are two types of communication: vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). Both V2V and V2I Communication is controlled via short range wireless communication protocol, called, called the (DSRC) Dedicated Short Range Communication protocol. Every vehicle and road side unit must have to broadcast message in 100-300 milliseconds in DSRC environment as specification are described in DSRC.

Due to wireless communication in VANET adversaries can control the communication channel. Adversaries and attacker can replay, intercept, change, edit and delete the message, which is transmitted in VANET environment. So therefore the vehicle (OBU) and RSU should validate and verify the coming message to avoid from different attacks. Pseudo ids of vehicle should also safe otherwise the adversaries can capture the pseudo ids and can aware about routes of vehicle and that can be used for crimes. VANET network model composed of two layers: The lower layer composed of OBU (inside of vehicles) and RSU with road side. Every vehicle is equipped with GPS (Global Position System). OBU is device for data storage and it has limited computing capability and it is wireless connected with RSU. On board unit is tamper-proof device where we stored the vehicles and RSU's identities and their private keys. The Upper Layer: consist of traffic control center, PKG and TRA. Trace authority (TRA) is responsible for pseudo Id's generation and PKG is responsible for private key creation corresponding to pseudo id. RSU and TRA and PKG is connected via wired link.

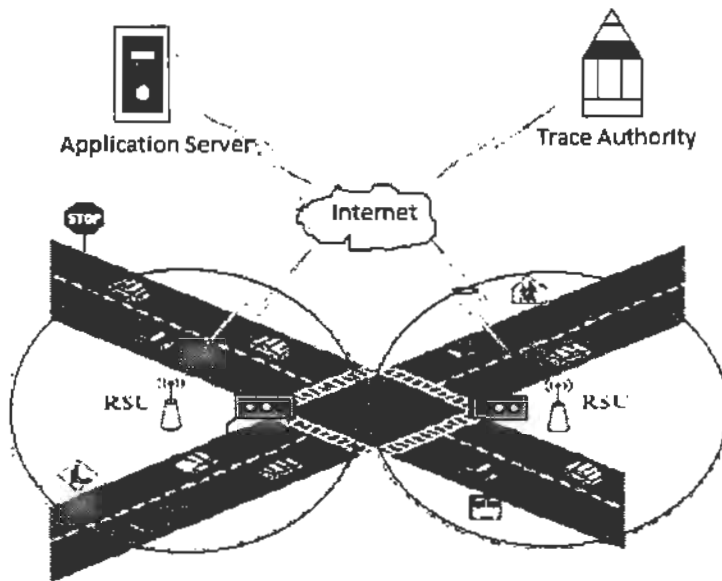


Figure 1.1: Structure of Vehicular Sensor Network

1.1 Preliminaries

This section describes the basic background of hash function and ECC.

1.1.1 Cryptography

Cryptography is also known as cryptology and its study of scheme and technique for secure communication within existing of adversaries. Cryptology also construct and analyze the protocols that prevent third parties from reading private messages. Cryptography used for data confidentiality, integrity fo data, authentication of messages and non repudiation. Application of cryptography are electronic commerce, chip-based payment card, e-banking, VSN, cell phones, ATM cards, e-passport system, routers etc. Cryptography based on mathematical theory and computer practice.

Types of ECC.

- Symmetric Cryptography
- Asymmetric Cryptography

Symmetric Cryptography

Symmetric key algorithm are algorithm used in cryptography where same keys is used for for both encryption of plain-text and and decrypt the cipher-text. Key may be unique and share a secret key between two parties to share the private information link. In symmetric key algorithm both sender and receiver require same secrete key of message. In early cryptographic system , a copy of secrete key is share with other party via a physical scure channel, but now modern techniques has eliminate this physical secure channel to share to secrete key, now instead of physical secure channel , Diffe-Hellman key exchange algorithm and some other public key protocols are used to agree on the new fresh scure key of each message. We can used Symmetric key encryption as 'Stream Cipher and Block Cipher. Stream Cipher encrypts at a time the digits of a message and block cipher picks a a specific number of bits and encrypt the number of bits as single unit.

Asymmetric Cryptography

In Asymmetric Key Cryptography we used two pair of keys, where we encrypt the plain-text by recipient public key and and other side receiver decrypt the cipher-text by its private key. Asymmetric encryption is also known as Public Key Cryptography , and user creates matching pairs where one key is as public and other key keep secret. User can sign the message by encrypting using their private key. Public Key Cryptography is majorly used for public-key-encryption and digital-signature. In public key encryption any user can encrypt the message using public key of receiver and that message can decrypt only bey receiver private key. In digital signature any message can be signed by sender's private key and any one can convert the cipher text into plain text who has sender's public key.

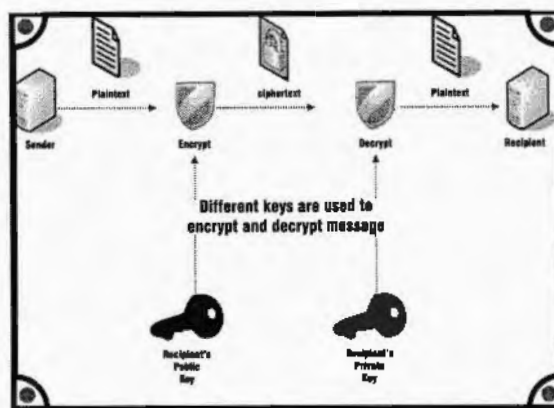


Figure 1.2: Asymmetric Cryptography

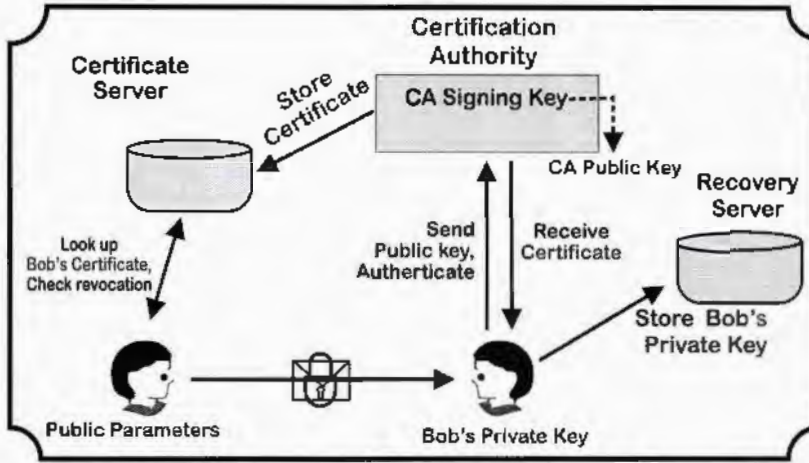


Figure 1.3: Public Key Infrastructure

1.1.2 Elliptic Curve Cryptography(ECC)

Elliptic Curve Cryptography basic on algebraic structure of elliptic curve over finite field. A public-key Cryptography that has small key size but provides equivalent security as compared to non-ECC. $y^2 = x^3 + ax + b \pmod p$ where a, b belong to finite fields and $(4a^3 + 27b^2 \neq 0)$ the ECC allows scalar point addition $P+Q=R$ and equation can be computed as $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$ where $x_r = (\lambda^2 - x_p - x_q)$, $y_r = \lambda(x_p - x_r) - y_p$ and $\lambda = \frac{y_q \cdot y_p}{x_q - x_p}$ and point multiplication is defined as $nP = P + P + \dots + P$ with equation $\lambda = \frac{3x_p^2 + a}{x_q - x_p}$. It can be used with Diffie-Hellman for key key exchange also with DSA, ECIES and etc.

1.1.3 Attribute-Based Encryption

Attribute Base Encryption is a type of public-key encryption. Secret key of user and cipher-text depends on attributes. Attribute can be many and attribute may be in which country he or she live and kind of subscription. The conversion of cipher-text into plain text only possible if he/she has attributes of user matching key and attributes of cipher-text. If a adversary has multiple key than he can access data because he will match at least one of key from bundle of keys. The main challenges of ABE are key coordination, key escrow and key revocation.

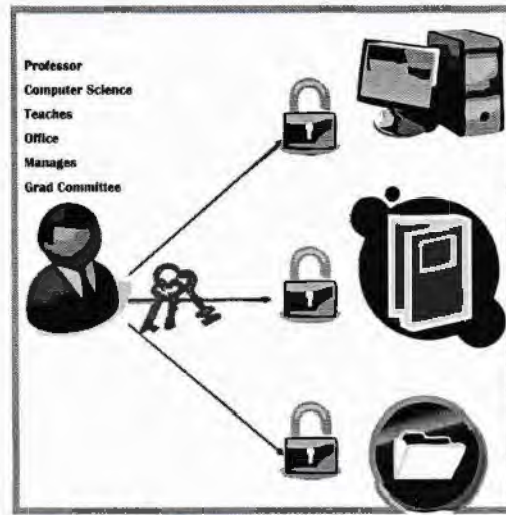


Figure 1.4: Attribute Based Encryption

1.1.4 Bilinear Pairing

Pairing base cryptography is the use of pairing between elements of two group $e : G_1 \times G_2 \rightarrow G_T$. to analyze the cryptographic system. G_1 and G_2 is additive cyclic group and their prime order is q and G_T is another cyclic group and has prime order q . It is advanced and modern cryptography operation but it is time consuming technique and we analyze performance of major protocols and scheme on computation of time. It satisfies two properties.

Bilinearity:

$$\forall \alpha, b \in F_q^*, \forall P \in G_1, Q \in G_2 : e(\alpha P, bQ) = e(P, Q)^{\alpha b}$$

Non-Degeneracy:

$$e \neq 1.$$

1.1.5 Identity-Based Cryptography

It is a type of public-key cryptography (PKC). In ID-base PKC a string is represented as public key. Public key may be email address, IP address, domain name etc. In 1984 Adi Shamir introduced the public key cryptography and it allows users verify digital signature and authenticate the user using public information or public key. ID-based PKC allows users to generate a public key from a known identity which may be ASCII. A trusted third party, private key generator (PKG) generates private key corresponding to public keys. Here must keep secret the master private key of PKG.

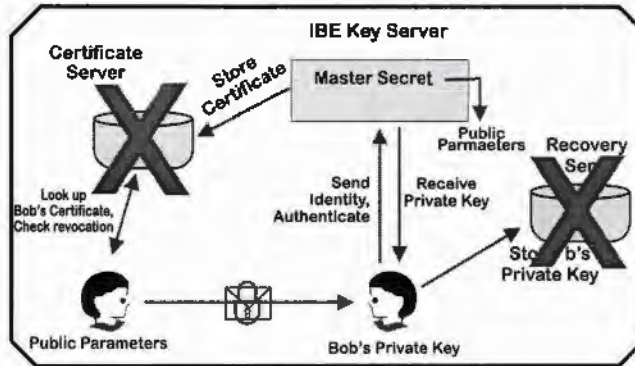


Figure 1.5: ID-based PKC

1.1.6 Hash Function

A function that takes arbitrary sized data as input and converts it to fixed size of data $H : \{0, 1\}^* \in Z_p$. The output value is called hash value. Hash function can be defined in following properties:

- Suppose, on any given input value b , the $H(b)$ can be easily computed.
- According to pre-image resistance property, on a given value $H(b)$ it's not possible and infeasible to compute the exact value of b .

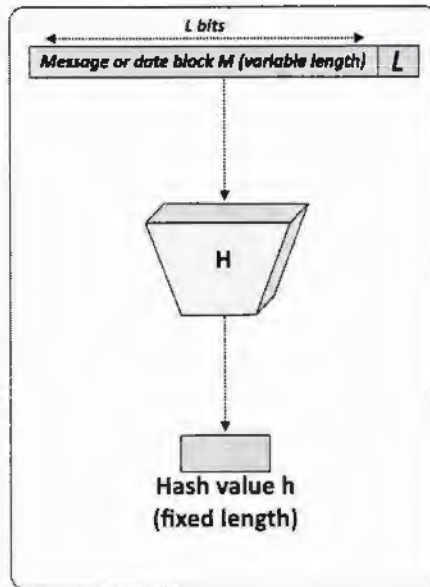


Figure 1.6: Hash Function

1.1.7 XOR

XOR is a additive cipher. it is an encryption algorithm which operate according to principal. $A \oplus 0 = A$, $A \oplus A = 0$, $(A \oplus B) \oplus C = A \oplus (B \oplus C)$, $(B \oplus A) \oplus A = B \oplus 0 = B$, Here \oplus denotes exclusive disjunction operation. Sometime this operation called modulus 2 addition, subtraction and identical. Using Bit wise XOR operator we can encrypt a text to every character by a given key.

1.2 Objectives

Objective of this thesis is to propose an authentication scheme that has ability to detect and resist all possible attacks. Formal security analysis , authenticity and correctness of proposed thesis is analyzed with ProVerif. We also checked the security of our proposed scheme informally, with different attacks. Additionally, the scheme offers:

1. Computational efficiency.
2. Communication efficiency.
3. Low latency an delay.

1.3 Thesis outline

Further detail of thesis is as follow:

- Chapter 2, provides literature survey of previous work, detailed review and cryptanalysis of Lo and Tsai scheme. At the end of chapter 2 we have provided the problem statement of our thesis.
- Chapter 3, provides the proposed solution and their four phases(extract, sign, verification and batch verification).
- Chapter 4, provides the security analysis, this chapter provides the formal analysis with ProVerif (automated tool) and informal analysis against different security requirements. Furthermore this chapter also provides the performance analysis, we have analyzed the computation cost, running time and its comparison with previous work.
- Finally, we made a conclusion in chapter 5.

Chapter 2

Literature Review

To eliminate the privacy and security issues of vehicular adhoc network Raya and Hubax[1], introduce the "Secure vehicular adhoc Network" it used anonymous certificate to design a conditional privacy preserving scheme. It modified the public key cryptography function of integrity and authentication. It does not reveal the vehicle' real identity, it stores public and private key pairs and their certificate in OBU. For each communication it takes a public and private key pairs and certificate and than discarded it. It has following issue: 1) To keep the public and private keys and their certificate , each node should have large storage space. 2) The Trace authority should have enough storage capacity to save all the certificates. 3) It is difficult to get the real identity of adversary when send the fake messages. The authority has to exhaustive search of a single certificate from the bunch of certificate.

To overcome the weakness in Raya , Hubaux's Lu ct scheme [2] introduced CPPA scheme. It obtain the temporary certificate then it pass to road site unit frequently. The disadvantage is that frequent interaction with RSU lose efficiency. Because each vehicle have to request for certificate to RSU. To solve the issue of Lu et al, Frediger et al[3], combined the anonymous certificate and mix zone to design a new condition privacy preserving authentication scheme. But here also large certificate have to store each vehicle. Zhang et al used the technique of hash message authentication code (HMAC) for CPPA where Key for HMAC is developed by key agreement protocol.

To overcome the Key Management problem in PKI base CPPA, Zhang [4] used Identity-based Public key cryptography. the concept of identity base PKC was introduce by shim[], here the third party private key generator (PKG) generates the public and private key pair. There does not need to bind the public key with certificate. Zhang [4, 5] proposed an Identity based Signature (IBV) scheme and used it in ID-based CPPA scheme for VANET. Advantage is that either vehicle nor RSU needs to store a certificate. It has low communication cost

as compared to earlier scheme because it supports the batch authentication and verification. However Zhang identity-based CPPA is attackable to the replay attack and can't stand with non-repudiation pointed by Lee and Lai [6]. Chim[7] also pointed that that Zhang, "ID based CPPA scheme" does not withstand to anti traceability and impersonation attacks. Chim proposed an ID-based CPPA scheme [7] that share two secrets and it could give the privacy requirement in VANET. But Horng et al.[8] pointed that Chim's ID-Based CPPA scheme is attackable to the impersonation attack. 1) a interceptor vehicle can impersonate any another vehicle by broadcasting bogus messages. Shim [9] proposed an identity base scheme but Liu et al.[10] check out and pointed a security attack in proof of shim CPPA scheme. In[11], key is global and hence key update is a major problem and need more communication overhead and computation cost and TA should be online. Huang et al.[12] proposed anonymous batch authentication and key agreement scheme for in VANET. For invalid request, they propose detection algorithm. In 2015, Shunrong et al [13] presented ABAH for VANET using Hash Message Authentication Code (HMAC) and its avoid the overhead and privacy disclosure due to Certificate revocation list (CRL). Its check the efficiency and integrity of batch authentication scheme using HMAC.

2.1 The review of the scheme of Zhang et al

Zhang et al[4] proposed system consist of four phase: Key Generation and pre distribution , Pseudo Identities and Private key generation, Signing of Message and Batch Verification.

2.1.0.1 Key Generation and Pre-distribution

Trusted Authority is responsible for generation and pre-distributing the private secret key of vehicle. TA setup the system parameter for every OBU and RSU as follow:

- G is a additive cyclic group generated by elliptic point P and G_T be a multiplicative cyclic group and both group has same order q .
- TA randomly select two master key s_1, s_2 and computes its public keys $P_{pub1} = s_1P$ and $P_{pub2} = s_2P$. Each tamper proof device of vehicle is pre load with master key of TA. Each RSU and vehicle are pre loaded with public parameter $(G, G_T, q, P, P_{pub1}, P_{pub2})$
- Tamper proof-device is activated by assigning real identity of vehicle R_ID belongs to group G , and pwd is a password. R_ID uniquely identify the vehicles and in authentication process we used pwd .

2.1.1 Identity Generation

The tamper proof device consist of three step: Authentication phase, identity generation phase and private key generation phase.

- **Authentication Phase:** RID vehicle real identity and PWD password are send to authentication phase. PWD may be signature of RID and it is signed by TA. If both RID and PWD successfully pas the authentication than it is given to next phase otherwise rejected.
- **Identity Generation phase:** This phase generate the pseudo identities for real identity of vehicle. Each identity is consist of ID_1 and ID_2 .

$$ID_1 = i.P$$
$$ID_2 = RID \oplus H(iP_{pub})$$

here i is random number and i is each time changed and ensured the distinct of ID_1 and ID_2 . Completion of encryption the ID_1 and ID_2 are transferred to private key generation phase.

- **private key generation phase:** Using pseudo identities ID_1 and ID_2 , tamper-proof device two private keys.

$$Sk_1 = s_i.ID_1$$
$$Sk_2 = s_j.H(ID_1||ID_2)$$

2.1.2 Message Signing

1. First vehicle V_i generate a message M_i .
2. V_i select a anonymous identity $ID^i = (ID_1^i, ID_2^i)$ and their corresponding private key $SK^i = (SK_1^i, SK_2^i)$ from the tamper-proof device.
3. Using private key $SK^i = (SK_1^i, SK_2^i)$, vehicle V_i can generate signature σ_i for message M_i .

$$\sigma_i = SK^i + h(M_i)SK^i.$$

V_i finally send the message (ID^i, M_i, σ_i)

2.1.3 Batch Verification

RSU check the integrity and verify the received signature of message to avoid from the different attacks, When RSU receive the traffic related message from vehicles .

verification :

For n different given messages $(ID^1, M_1, \sigma_1), (ID^2, M_2, \sigma_2), \dots, (ID^n, M_n, \sigma_n)$ send by vehicle V_1, V_2, \dots, V_n and signatures are expressed by $\sigma_1, \sigma_2, \dots, \sigma_n$:

$$e^{\wedge} \left(\sum_{i=1}^n \sigma_i, P \right) = e^{\sum_{i=1}^n ID^{i1} P_{pub1} \cdot e \left(\sum_{i=1}^n h(M_i) H(ID_1^i || ID_2^i), P_{pub2} \right)}$$

2.2 Shim et al scheme review

Shim et al 9 proposed CPPA scheme for VANET and it consist of four phases which are mentioned below:

2.2.1 System Parameter Setup

Trace authority and private key generator generate the system parameters:

1. Giving parameter $k \in Z^+$. Trace authority generate two cyclic group G_1 and G_T , prime number q and three generator point P, Q and Q' in G_1 . The private key generator picks a number which is random $s \in Z_q$ and compute $P_{pub} = s.P$, s is a secret key, which is only know private key generator.
2. The TA picks an integer random number $\alpha \in Z_q$ and calculates $T_{pub} = \alpha.P$, where α is master secret of TRA. It will used for traceability.
3. TRA and PKG chooses two has functions H_1 and H_2 and publish the system parameter $param = (q, G_1, G_2, e, P, T_{pub}, P_{pub}, Q, Q', H_1, H_2)$. All tamper-proof device are preloaded with params.

2.2.2 pseudo identity generation and private key extraction

1. Vehicle computes $PID_i = k_i.P$ and send (RID_i, PID_i) the Trace authority, where the RID_i uniquely identified vehicle V_i .

2. After confirming RID_i , TRA computes the following:

$$PID_{i2} = RID_i \oplus H(\alpha PID_{i,1}, PID_{i,2}, ET_i, T_{pub}).$$

where ET_i show the valid time for this identity. The pseudo-ID is $PID_i = (PID_{i,1}, PID_{i,2}, ET_i)$ is given to private key generator via a secure channel.

3. The pseudo-ID PID_i , the PKG picks a number that is random t_i and compute $T_i = t_i.P, h_i = H_1(PID_i, T_i)$ and $S_i = (s + h_i.t_i).Q$. This is private key $SK_i = (T_i, S_i)$. Here s is master secret key of private key generator.
4. TRA and PKG send the pseudo id and private key (PID_i/SK_i) to the vehicle. Pseudo ids and private key are store in tamper proof device.

2.2.3 Message Signing

For the message integrity and authentication, each message should be signed by the vehicle V_i . Vehicle V_i select a pseudo identity PID_i from its storage and choose current time stamp tt_i , it provide the freshness of signed message. the vehicle V_i sign a message by the private key $SK_i = (T_i, S_i)$.

1. Select r_i and compute $U = r_i.P \in G_1$.
2. Computes $h'_i = H_2(PID_i, M_i, tt_i, T_i, U_i)$ and $V_i = h'_i S_i + r_i.Q'$, then $\Gamma_i = (T_i, U_i, V_i)$ is a signature on $M_i || tt_i$ for PID_i .
3. Vehicle V_i sends the message $(PID_i, M_i, tt_i, \Gamma_i)$ to road side unit.

2.2.4 Batch Verification

Given n different message -signature tuples $(PID_1, M_1, tt_1, \Gamma_1), \dots, (PID_n, M_n, tt_n, \Gamma_n)$, which are signed by n different vehicles V_1, \dots, V_n where $\Gamma_i = (T_i, U_i, V_i)$, if $tt_i (i = 1, \dots, n)$ is a valid, then RSU verify:

1. Compute $h_i = H_1(PID_i, T_i)$ and $h'_i = H_2(PID_i, M_i, tt_i, T_i, U_i)$.

$$e\left(\sum_{i=1}^n V_i.P\right) = e\left(\sum_{i=1}^n h_i.P_{pub} + \sum_{i=1}^n h'_i.h_i.T_i.Q\right) + \sum_{i=1}^n U_i.Q'$$

2.3 Shurong etc scheme review

Shurong proposed scheme composed of following five phases which are described below:

2.3.0.1 System Initialization

Using public parameters (q, G_1, G_T, e, p) TA initialize the below stages:

1. TA selects two random numbers $Q, Q' \in G_1$.
2. TA select a random number sZ_q as private key and calculates the public key $P_{pub} = sP$.
3. TA picks hash functions $H_i : [0, 1]$ where $(i = 1, 2, 3)$. TA selects $H_4 : G_1$. Then TA publish the parameter $(q, G_1, G_T, e, P, P_{pub}, Q, Q', H_1, H_2, H_3, H_4)$. TA divide in different domain its precinct which consist of many RSU.

2.3.1 Road Side Unit Certificate Issuing

For road side unit, R_x which is in domain of D_y , TA issues certificate $Cert_{(TA, Rx)}$.

1. TA selects random number rZ_q as private key of RSU, R_x . Then it calculate public key $PK_{Rx} = rP$.
2. Trace authority generates the signature $\sigma_{TA, Rx} = Sign(s, PK_x \ll D_y)$:
3. Trace authority delivers securely SK_{Rx} and $Cert_{(TA, Rx)}$ to R_x where $Cert_{(TA, Rx)} = (PK_{Rx}, D_y, (\sigma_{TA, Rx}))$.

2.3.2 Vehicle anonymous and private keys generation

Shruong scheme divide the one year in time slot TS_j , it length is δT . We can get C times time-slot. The time-range of TS_j is $j.\delta T(j+1).\delta T$. PID_j is as V_i pseudonym at the time slot TS_j generated by two hash chains.

$$S_{1,j} = H_3^j(SD_{1,j})$$

$$S_{2,c-j+1} = H_3^{c-j+1}(SD_{i,2})$$

$$PID_{i,j} = H_3$$

$(S_{i,j} \oplus S(2, c - j + 1))$

2.3.3 Mutual authentication and Secure group key distribution

Situation 1: Mutual identification between vehicles and RSU should start. R_x in domain D_y and D_y broadcasts its $Certi_{TA,Rx}$ every 5 seconds. V_i receives the message D_y . D_y is a fresh and new domain for V_i , it verify the message using equation.

$$Verify(P_{pub}, PK_{Rx} || D_y, \sigma_{TA,Rx})$$

P_{pub} is the public key of TA, PK_{Rx} is the public key of Rx, and $\sigma_{TA,Rx}$ is the signature of Rx. If certificate $Certi(TA, Rx)$ is valid, then V_i pass the process of authentication in time slot TS_j by following process.

1. V_i select a number which is random $r_{i,j}$ and computes $U_{i,j} = r_{i,j} \cdot P$ and Pair wise key $K_{PID_{i,j}, Rx} = r_{i,j} \cdot PK_{Rx}$.
2. V_i computes $h'_{i,j} = H_2(PID_{i,j}, 4M_i | tt_i, T_{i,j}, U_{i,j}, W_{i,j} = h'_{i,j} \cdot S_{i,j} + r_{i,j} Q')$. $PID_{i,j}, M_i, tt_i, Y_{i,j}$ to R_x).

2.4 Lo and Tsai scheme review

Lo and Tsai [14] scheme composed of five algorithms steps: setup, extract, sign, Verification and Batch Verification.

2.4.1 Setup

In setup algorithm the PKG take a large prime number n, P, q . We takes a fixed size field F_N over n , the size of finite field is n . P is base point which is also called base point of elliptic curve E and q are the prime order of base point P . PKG calculates public-key P_{pub} where $P_{pub} = s \cdot P$ and $s \in Z_q$ is master private key of PKG and keeps the s secretly. PKG select two one-way hash function: $H_1 : [0, 1]^*$ and $H_2 : [0, 1]^*$. PKG publish $(P, P_{pub}, q, H_1, H_2)$.

Table 2.1: Notation Guide

Notations	Description
V_i	ith vehicle
TA	Tracing Authority
PKG	Private Key Generator
s	master private key of PKG
P_{pub}	public key of PKG
$alpha$	secret key of Tracing Authority
H_1, H_2	Two one-way hash function
t_i	Time stamp for pseudo-ID
RID	Vehicle real identity
ID_R	identity of a RSU
G_1	cyclic additive group
$E_k(.) / D_k(.)$	using secret key k symmetric encryption and decryption
q	prime order of G_1
$tt_i, tt_i^R SU$	Current timestamps
$PID_i = PID_{i1}, PID_{i2}, t_i$	Pseudo identity for a vehicle
p, q, n	p and q are prime number and $n=p.q$
\oplus	The XOR operation
\parallel	The concatenation operation

2.4.2 Extract

When a vehicle want to register on private key generator for extraction of private key, the vehicle sent selected identity ID_i to private key generator via a secure and safe channel. When PKG received the ID_i , private key generator calculates

$$R_i = r_i.P$$

$$SID_i = r_i + H_1(ID_i, R_i) \times smodq$$

Here r_i is a random number. Private key generator sends (R_i, SID_i) return to the vehicle via a directly connected channel which is secure.

2.4.3 Signing of message

after extracting private key, when vehicles and RSU broadcast a message, they sign the message. The signer has an identity ID_i .

$$K_i = k_i.P$$

$$V_i = H_2(K_i, R_i, ID_i, M_i) \times k_i + SID_i \text{mod} q$$

where k_i is a random number. (R_i, K_i, V_i) is the digital signature for M_i for identity ID_i .

2.4.4 Verification

To verify and validate the message M_i and its signature (R_i, K_i, V_i) , following equation is checked, if its verify then it is valid signature and authenticate user. If equation does not hold and verify then it reject the signatures.

$$V_i.P = H_2(K_i, R_i, ID_i, M_i)R_i + K_i + H^{-1}(ID_i, R_i)P_{pub}.$$

2.4.5 Batch Verification

If there are n distinct message-signature tuples $(R_1, K_1, V_1), (R_2, K_2, V_2), \dots, (R_n, K_n, V_n)$ signed by n different singers, the verifier can simultaneously verify the validity of signer and sender by verifying the below equation.

$$\left(\sum_{i=1}^n V_i \right) P = \left(\sum_{i=1}^n H_2((R_i, K_i, ID_i, M_i)K_i) + \sum_{i=1}^n R_i + \left(\sum_{i=1}^n H_1(ID_i, R_i)P_{pub} \right) \right)$$

. if above equation holds then n distinct signatures are valid. To avoid from the attacks pointed by Shim, replace the above equation by adding small exponent test where $a_i \in \mathbb{R}^0, 1^l$. where $i = 1, \dots, n$.

$$\left(\sum_{i=1}^n a_i.V_i \right) P = \left(\sum_{i=1}^n a_i.H_2(R_i, K_i, ID_i, M_i)K_i) + \sum_{i=1}^n a_i R_i + \left(\sum_{i=1}^n a_i H_1(ID_i, R_i)P_{pub} \right) \right)$$

2.5 Problem Statement

In past, mostly schemes were used bilinear pairing technique in VANET and it has high computation time. Some scheme used third party for public key certificate and it need huge storage to store the certificates and it also take huge time to search the specific certificate. We have discussed Lo and Tsai scheme that does not use pairing but it has also high computation.

2.6 Chapter Summary

This chapter first section discusses the literature review, second section discusses brief reviews and cryptanalysis of Lo and Tsai scheme last section provides the problem statement of our thesis.

Chapter 3

Proposed Scheme

Proposed scheme composed of four parts: setup,extract,verification and batch verification.

3.1 Setup

In this step, private key generator picks a large prime number n , a base point P which is generator point of elliptic curve E and q is prime order of base point P . It also takes a finite field F_n for large prime number n . PKG computes Public key P_{pub} where $P_{pub} = s.P$ and $s \in Z_q$ is master private key of PKG and keeps the s secretly. PKG select two one-way hash function: $H1 : (0, 1)^*$ and $H2 : (0, 1)^*$. PKG publish $(P, P_{pub}, q, H1, H2)$.

3.2 Extract

To register on private key generator, the vehicle sends its real identity ID_i to (PKG) private key generator by a safe channel. PKG compute following equation when it received the identity ID_i from the vehicle or RSU.

$$\begin{aligned}K_i &= k_i.P \\P_i &= H_1(ID_i) \times (k_i + s) \\Q_i &= H_1(ID_i) \times (k_i + s)P\end{aligned}$$

$$SID_i = H_1(ID_i, Q_i) \times s + k_i$$

k_i is a random number. (K_i, Q_i, P_i, SID_i) is send to vehicle where Q_i is public key and P_i, SID is private key of vehicle .

3.3 Sign

For a traffic related message M_i , a signer which may be vehicle or RSU with an identity ID_i computes

$$V_i = H_1(K_i, ID_i, M_i, T_i) \times P_i + SID_i$$

T_i is timestamps of message M_i . (K_i, Q_i, V_i) is signature on message M_i for (ID_i, T_i) .

3.4 Verification

In proposed scheme the given given message M_i and its corresponding digital signature (K_i, Q_i, V_i) , a verifier can verify and checked the correctness and validity of signature (K_i, Q_i, V_i) with the following equation.

$$V_i.P = H_1(K_i, ID_i, M_i, T_i) \times Q_i + K_i + H_1(ID_i, Q_i)P_{pub}$$

Proof:

$$\begin{aligned} V_i &= H_1(K_i, ID_i, M_i, T_i) \times P_i + SID_i \\ V_i.P &= H_1(K_i, ID_i, M_i, T_i) \times P_i + (H_1(ID_i, Q_i) \times s + k_i).P \\ V_i.P &= H_1(K_i, ID_i, M_i, T_i) \times Q_i + K_i + H_1(ID_i, Q_i)P_{pub} \end{aligned}$$

3.5 Batch Verification

If there are n distinct message-signature tuples $(K_1, Q_1, V_1), (K_2, Q_2, V_2), \dots, (K_n, Q_n, V_n)$ signed by n different singers, the verifier can simultaneously verify the validity of signer

via checking the below equation.

$$\begin{aligned} \left(\sum_{i=1}^m V_i\right) \cdot P &= \sum_{i=1}^n H_1(K_i, ID_i, M_i, T_i) \times Q_i + \sum_{i=1}^n K_i + \sum_{i=1}^n H_1(ID_i, Q_i) P_{pub} \\ &= \sum_{i=1}^n (H_1(K_i, ID_i, M_i, T_i) \times P_i + SID_i) \cdot P \\ &= \sum_{i=1}^n (H_1(K_i, ID_i, M_i, T_i) \times P_i + K_i + H_1(ID_i, Q_i) P_{pub}) \end{aligned}$$

3.6 Chapter Summary

This chapter of our thesis provides the proposed solution and its all steps (extract, sign, verification and Batch verification) in detail.

Chapter 4

Security Analysis and Computation Cost Analysis

This chapter provides security analysis and computation cost analysis of proposed thesis. The detailed analysis is given in following sections:

4.1 Security Analysis

Security analysis of our given protocol is done formally and informally. Formal analysis is done with BAN logic and proVerif, the informal analysis is checked against different attacks. Furthermore this section also shows the security requirement comparison.

4.1.1 Security Analysis with ProVerif

We have verified and checked the correctness of our proposed scheme with ProVerif. ProVerif is automated reasoning software tool and ProVerif can test authentication, anonymity, reachable and all other security requirements[15]. ProVerif can support different cryptographic functions like: Encryption/decryption, MAC, signatures, hash, ecc and many others. [16],[17] In our propose scheme we have run three queries. First query for setup query than we run successfully and end successfully and give result true. It mean our protocol is correct. Second query for server that we cexecute successfully and end with successfully and give output true. Third query we checked the session key k is not attachable and successfully it is giving output true,it means our proposed

scheme is not attachable. The ProVerif code correctness results are shown below. We used two channels one channel "ChSec" which is secure and "ChPub" is insure. We have used some constants P, Pk and s where, P is ECC point, PK is P_{pub} public key and s is secret key of PKG which is defined as private. We have declared h, XOR, Concat, Inverse, ECPA(Point-addition) and ECPME(Point-multiplication) as constructors

```
(* ----- Channels -----*)
free ChSec:channel [private]. (*secure channel Vi and PKG*)
free ChPub:channel [private]. (*RSU to Vehicle and TRA*)
(*----- Constants and Variables -----*)
free IDi :bitstring.
free IDvi :bitstring.
const s : bitstring [private].
const P :bitstring.
(*=====Constructors=====*)

fun1 h(bitstring):bitstring.
fun1 h(bitstring2):bitstring3.
fun1 Inverse(bitstring4):bitstring5.
fun1 Concat(bitstring6,bitstring7):bitstring8.
fun1 XDR (bitstring9,bitstring10): bitstring11.
fun1 Mult (bitstring12,bitstring13):bitstring14.
fun1 Add(bitstring15,bitstring16) :bitstring17.
fun1 enc( bitstring18,bitstring19):bitstring20.
fun1 dec(bitstring21,bitstring22): bitstring23.

(*=====Used Equations=====*)
equation forall a:bitstring4; Inverse(Inverse(a))=a.
equation forall a:bitstring, b:bitstring; XDR(XDR(a,b),b)=a.
equation forall x:bitstring, y: bitstring; dec(enc(x,y),y) = x.
```

In Extract phase the V_i starts with registration phase, the vehicle calculate with real identity R_{ID} , computes $PID_i = di.P$ and forwards (R_{IDi}, PID_i) to TRA via a secure channel. Afterward TRA receives it and check R_{iD} and computes $P_{ID_{i,2}}$ and sends $PID_{i,1}, PID_{i,2}, t_i$ to private key generator. In login phase Mb_u verifies B and after that picks a random integer number a_i and calculates K_i, SID_i, L, Z and V afterward he/she transmits $out(ChPub, (x_SID, xV, IDHA, Z, TSmbu))$ over public-channel. Mbu

receives "in (ChPub,(xV1:bitstring,xC':bitstring,xTSFA:bitstring));" and verifies xV1' in case of true result the Mb_u calculates the session key with his/her K. FA and HA also performs same processes, with different parameters and values as defined below.

```
(*====*Setup and Extract*====*)
let pVi=
(* Setup *)

let pUi=
event start_Ui(IDi);
let Ppub=Mult(s,P) in
new $a_i$:bitstring;
  compute Ki=Mult(ai,P) in
  compute SID= Add(ai,(h(IDi),h(Ki))) in
out(ChSec,(IDi,SID));
event end_Ui(IDi)
else
0.
(*-----Sign and Verification-----*)
let pTA=
event start_TA(IDvi);
in (ChSec,(xIDi:bitstring,SID:bitstring));
new ri:Bitstring;
new Mi:Bitstring;
new ti:Bitstring;
suppose Ri=Mult(ri,P)in
suppose Vi=Add(ri,(SID,IDi,Ri,Mi,ti)) in
event end_TA(IDvi)
else
0.
process ( (!pTA) | (!pUi) )
```

The results are shown below:

```
1-- Query inj-event(end_TA(IDvi[])) ==> inj-event(start_TA(IDvi[]))
Completing...
Starting query inj-event(end_TA(IDvi[])) ==> inj-event(start_TA(IDvi[]))
goal reachable: begin(start_TA(IDvi[]), SID = Add(ai[!i = @sid_407],
```

```
(h(IDi[]),h(Mult(ai[!1 = @sid_407],P))))),xIDi = IDi[], @sid = endsid_408,
  @occ2 = @occ_cst) -> end(endsid_408,end_TA(IDvi[]))
RESULT inj-event(end_TA(IDvi[])) ==> inj-event(start_TA(IDvi[])) is true.
2--Query inj-event(end_Ui(IDi[])) ==> inj-event(start_Ui(IDi[]))
Completing...
Starting query inj-event(end_Ui(IDi[])) ==> inj-event(start_Ui(IDi[]))
goal reachable: begin(start_Ui(IDi[]), @sid_263 = endsid_727,
  @occ11 = @occ_cst) -> end(endsid_727,end_Ui(IDi[]))
RESULT inj-event(end_Ui(IDi[])) ==> inj-event(start_Ui(IDi[])) is true.
3-- Query not attacker(S[])
Completing...
Starting query not attacker(S[])
RESULT not attacker(S[]) is true.
```

Result 1,2 and 3 are showing that all three processes are successfully started and terminated. Whereas, result 4 shows that the adversary cannot find the session key *SK*. Hence proposed scheme preserves the secrecy and authentication.

4.1.2 Informal Security Analysis

Our proposed scheme accomplishes all possible security risks as stated below:

1. Message Authentication.
2. Preserving Identity Preserving.
3. Unlinkability.
4. Backward/Forward secrecy.
5. Replay Attacks.
6. Known-key attacks.
7. Modification Attack.
8. Insider attacks.
9. Stolen- verifier attacks.
10. Mutual authentication.
11. Impersonation attacks(Forgery attacks)

12. Role Separation

4.1.2.1 Message Authentication

Message Authentication Code is also known as tag. It is piece of relevant information used to authenticate and validate the message. Message authentication ensured that the message has come from the claimed user(sender) and has not been yet any changed or alter. Each message and user should authenticate to find that no one adversary can be change or modified the message before communicating to each other, so illegal user could not intercept.Each vehicle and Road Side Unit checks the validity and integrity of message before receiving. For the message M_i and ID_i, T_i is checked by verifying the equation $V_i.P = H_1(K_i, ID_i, M_i, T_i) \times Q_i + K_i + H_1(ID_i, Q_i)P_{pub}$. If it fulfill the given equation then user is authenticated user.

4.1.2.2 preserving identity

The real identity of a vehicle should not be include and transmittted in a message. Therefore real or original identity should be protected, if any user known the real identity then he/she can forge the transmittted message. In proposed scheine each pseudo identity PID_i contained with TRA's master secret key α and d_i secret which is chosen by user. The values of master secret key of TRA's and user chosen secret d_i is known by Trace authority and vehicle. If malicious user or adversary does not know of value of d_i and α , malicious adversary can not compute $\alpha.PID_i$ due to CDH problem.

4.1.2.3 Provision to Traceability

In our scheme we will protect the vehicle real identity RID_i is involved in PID_i which is generated by Trace Authority. $PID_{i,2} = RID_i + H(\alpha PID_{i,1}, PD_i, 1)$ to Private Key Generator. The malicious adversary can not guess the real identity because $PID_i = d_i.P$ and α which is only known by user and TRA. $PID_{i,1} = \alpha.d_i.P$ which is CDH problem. We will also protect the private key s of PKG and α of TRA.

4.1.2.4 User Unlinkability

For a secure protocol user traceability is vulnerable issue because, a legal user traceability may leads to many attacks. Suppose that any malicious user or adversary aim to find that m and m' are transmitted by same user/vehicle but he will not successful because, two different ID_i have been used to sign the two messages and private key is also different. The proposed scheme provides complete unlinkability.

A type of security attack in which a malicious adversary or attacker illicitly inserts Himself/herself in a two parties communication and intercepts their conversation. The Adversary can capture the sensitive data/information, can send or receive data anytime and may impersonate both parties by pretending himself/herself a legal user.

4.1.2.5 Backward/Forward secrecy

Backward secrecy is a type of secrecy in which if an adversary A if aware of new session key he/she would be unable to obtain the the earlier keys. While the forward secrecy means any compromization of old session key should not reveal any future kcys for the adversary A.

Our proposed scheme fulfills all forward-backward secrecy requirements due to random numbers because, with a new session random numbers are chosen newly even if L is compromised at any stage later still, may not compute the SK . Therefore we can say that our proposed-scheme accomplishes backward/forward secrecy.

4.1.2.6 Replay Attacks

A replay attack also known as playback attack is type of network attack. In replay attack valid sended data is maliciously or fraudulently delayed or repeated. This attack can be done by valid sender or an adversary or malicious user who intercepts the transmitted data and re-transmit it. In replay attacks the malicious attacker/adversary repeats or delays the transmission. Replay attack can be eradicated by on-time-password, mac and timestamps techniques. The vehicles and RSU's checked the freshness of T_i in given message M_i, T_i, ID_i and K_i, Q_i, V_i is digital signature of message M_i, T_i , so using timestamps technique our proposed scheme withstand to replay attack.

4.1.2.7 Known-key attacks

Known key attack is cryptographic attack in which an attacker can access the cipher-text. Known-key-attacks are possibly attempted successfully by an attacker/adversary when plain-text is associated with cipher-text and adversary could trace plain-text by just performing backtracking.

In our proposed scheme as stated in section 7.2, 7.3 we used the elliptic-curve points with different random numbers for all sessions when session ends random numbers are freshly generated. Furthermore our session key is created with all three participants at each end independently. If attacker gets the previous session key He/She cannot compute new session key and if he/she gets the new session key still may not compute the previous one because of ECC-points, random numbers and timestamps. Proposed scheme resist the known-key-attacks.

4.1.2.8 Modification Attack

In modification attack, some portion legal message is edited. The message is re-ordered or delayed to produce an authorize affect and sometime it is dangerous. According our proposed scheme ,we know K_i, Q_i, V_i is digital signature for M_i, T_i . Any modification of the message M_i, T_i, ID_i and digital signature K_i, Q_i, V_i , can be verified by equation $V_i.P = H_1(K_i, ID_i, M_i) \times Q_i + K_i + H_1(ID_i, Q_i)P_{pub}$. So proposed scheme not attack able by modification attack.

4.1.2.9 Stolen verifier attack

Our proposed scheme withstand the stolen verifier attacks because the road side unit nor the vehicle maintain the verifier table for message and user authentication. So adversary can not steal any verifier table.

4.1.2.10 Role Separation

In proposed scheme , there are two authorities, Trace Authority and private key generator(PKG). The main tasks of Tracing Authority has to generate pseudo-IDs for vehicles and tracing of real identity of vehicle from its signature. Therefor secrete key of TRA α must be protected. No use can access master secrete key of TRA.

Another trusted authority is private key generator. The main task of private key generator is generation of private keys for each vehicles of the corresponding pseudo-IDs. PKG generate an extract private key using its master secrete key s and its must be protected. PKG can't trace the real identity of vehicles from the pseudo-IDs. Therefor in our technique master keys s and α must be protected, threshold cryptography can be used to protect the maste key of trusted authorities.

4.1.3 Security Requirements and Comparison

The main aim of this section is to get the analysis of security requirements and to find out the computation cost and performance analysis of our proposed scheme. The subsection elaborates security comparison and the cost comparison of proposed scheme with other related work.

4.1.4 Security Requirements

TH19208
This section provides the comparison of security and cost requirements of our proposed scheme with the schemes which are proposed in following articles[18][19] [9] [14]. We compared all 13 security requirements of our proposed scheme with some previous work whereas, R is security requirement so R1 is requirement 1 and . The comparison table that only our proposed scheme provides all 13 security requirements. The detailed comparison is shown in table. The security observation and analysis shows that only our given scheme can fulfill all security requirements.

4.2 Computation Cost Analysis

To measure the computation cost we ignore some lightweight function such as concatenations, XOR due to their limited computation cost. Our main attention is to analyze cryptographic operation that TRA , PKG and RSU need to cxececute. We consider all three participants TRA , PKG and RSU . Detailed description is shown in table.

In performance analysis section we compared our proposed scheme with few previous schemes. To check the computational efficiency and performance of our scheme we compared our scheme with following schemes: [17][9] and [12] these schemes are proposed recently. The total computation cost of scheme [17] is $(T_{mp}) + (T_{mp} + T_H + 3T_p) +$

Requirements	[15]	[20]	[5]	[9]	[14]	Proposed Scheme
SR1	✓	✓	✓	✓	✓	✓
SR2	✓	✓	✓	×	✓	✓
SR3	✓	✓	✓	✓	✓	✓
SR4	✓	✓	✓	✓	✓	✓
SR5	×	✓	×	✓	✓	✓
SR6	✓	×	✓	×	✓	✓
SR7	✓	✓	✓	×	✓	✓
SR8	×	✓	×	✓	✓	✓
SR9	✓	✓	✓	×	✓	✓
SR10	✓	✓	×	✓	✓	✓
R11	✓	✓	✓	✓	✓	✓
R12	×	×	✓	✓	✓	✓

Table 4.1: Security requirements table

- SR1:Message Authentication.
- SR2:preserving identity.
- SR3:Unlinkability.
- SR4:Backward/Forward secrecy.
- SR5:Replay attacks.
- SR6:Known-key attacks.
- SR7:Modification Attack.
- R8:Insider attacks.
- SR9:Stolen-verifier attacks.
- SR10:Mutual authentication.
- SR11:Impersonation attacks(Forgery attacks)
- SR12:Role Separation

✓: Yes provides, ×: Does not provide

Computation Cost	Zhang et al [5]	Shim and Hwang[9]	Lo and Tsai [14]	Proposed Scheme
Signature generation	T_{mp}	$2T_{mp}$	$T_{mp}+T_m+1H$	T_m+1H
Signature Verification	$T_{mp}+T_H+3T_p$	$2T_{mp}+3T_p$	$3T_{mp}+2PA+1H$	$3T_{mp}+2PA+1H$
Batch Verification	$nT_{mp}+nT_H+3T_p$	$(n+1)T_{mp}+3T_p$	$(n+1)T_{mp}+2PA+1H$	$(n+1)T_{mp}+2PA+1H$
Computation Time	21.8 ms	26.3 ms	6.7 ms	4.5 ms

Table 4.2: Comparison of computation cost and running time

$(nT_{mp} + nT_H + 3T_p)$, total computation cost of scheme[9] is $(2T_{mp}) + (2T_{mp} + 3T_p) + ((n + 1)T_{mp} + 3T_p)$, total computation cost of scheme [12] is $(T_m + T_{mp} + 1H) + (3T_{mp} + 2PA + 2H) + (n + 2)T_{mp} + 2PA + 2H$ and total computation cost of our proposed scheme is $(T_m + H) + (3T_{mp} + 2PA + 2H) + (n + 2)T_{mp} + 2PA + 2H$. Our proposed scheme has reduced 1 point multiplication in signature generation as compare to Lo and Tsai scheme. So our proposed scheme is faster 2.2 ms in signature generation as compared to Lo and Tsai scheme. Execution time of cryptographic operation are taken from Kilinc and Yanik paper [21] The detailed description is illustrated in table 4.

- CC:Computation cost
- T_p : CC of pairing operation;
- T_m : CC of scalar multiplication operation;
- T_{mp} : CC of scalar multiplication point operation;
- PA: CC of point addition; TH: CC hash function;

TABLE IV					
FORMAT OF THE SIGNED MESSAGE IN CURRENT IEEE TRAIL-USE STANDARD FOR VANET SECURITY					
Protocol	Type	Message	certificate	Signature	
1 byte	1 byte	67 bytes	125 bytes	56 bytes	

TABLE V					
FORMAT OF THE SIGNED MESSAGE FOR OBU AND RSU IN THE PROPOSED SCHEME					
Type ID	Message ID	Payload (message)	Timestamp	Signature	PseudoID(OBU)/RSU ID
1 byte	1 byte	67 bytes	4 bytes	60 bytes	41 bytes / 10 bytes

Figure 4.1: Communication cost of proposed scheme

To measure the running time of our proposed solution we followed Lo and Tsai experiments. Single T_p takes 5.811 ms, T_{mp} 2.226 ms, T_m 0.03 ms, T_{pa} 0.0288 ms and T_h 0.0023 ms. We mentioned here the total running time of all proposed scheme, whereas [14] takes total 21.8 ms, [9] takes total proximately 26.3 ms and [18] takes total 6.7 ms. our proposed scheme takes total 4.5 ms. As a result, the running time of our proposed scheme is very efficient as compared to previous schemes [9] and [14].

4.3 Chapter Summary

This chapter describes formal security analysis, informal security analysis, comparison of security requirements, computation costs and running time of our proposed scheme in detail.

Chapter 5

Conclusion and Future Work

In our thesis, we provide an efficient ID- based scheme introduced and also introduced new CPPA scheme is developed for VSN. Security analysis has been conducted with proverif and informal security checking against different attacks. Our scheme also supports the batch authentication and both withstand adaptive chosen message attack under. Proposed identity based authentication scheme that support batch verification does not required to use mapto point function and pairing operation. Our scheme has low computation cost as compared to Lo and Tsai scheme. In terms of time consumption our proposed scheme is approximately time faster in signature generation as compared to Lo and Tsai scheme which discussed as base paper. In signature generation stage our proposed scheme has reduced 1 point multiplication as compared to Lo and Tsai scheme. Our proposed scheme supports message integrity, unlinkability, role separation, traceability for trusted third party, anonymous authentication. Proposed scheme supports vehicle -to- vehicle communication and vehicle -to- infrastructure communication. Proposed scheme is very efficient as compared to previous works in terms of security and computation. Our scheme is faster and take less memory in execution. This scheme can be used in any vehicular sensor environment and give a well traffic control. Our scheme is has two authorities, one is private key generator which generate private keys for different identities and and Trace authority which has master key by which it generate identities for vehicles. It can reveal real identity of any vehicle. So our proposed scheme is very efficient in terms of time consumption, space consumption and in terms of time computation. For future study and research, our given scheme can be used in VANET environment where is two party communication and we can used for lightweight authentication.

Bibliography

- [1] Raya M, Hubaux JP. Securing vehicular ad hoc networks. *Journal of Computer Security* 2007; 15(1):39–68.
- [2] Lu R, Lin X, Zhu H, Ho PH, Shen X. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. *INFOCOM 2008. The 27th Conference on Computer Communications.*, IEEE, 2008.
- [3] Freudiger J, Raya M, F3legyh3azi M, Papadimitratos P, *et al.*. Mix-zones for location privacy in vehicular networks 2007; .
- [4] Zhang C, Lu R, Lin X, Ho PH, Shen X. An efficient identity-based batch verification scheme for vehicular sensor networks. *The 27th Conference on Computer Communications.INFOCOM 2008*, IEEE, 2008.
- [5] Zhang C, Ho PH, Tapolcai J. On batch verification with group testing for vehicular communications. *Wireless Networks* 2011; 17(8):1851–1865.
- [6] Lee CC, Lai YM. Toward a secure batch verification with group testing for vanet. *Wireless networks* 2013; 19(6):1441–1449.
- [7] Chim TW, Yiu SM, Hui LC, Li VO. Specs: Secure and privacy enhancing communications schemes for vanets. *Ad Hoc Networks* 2011; 9(2):189–203.
- [8] Horng SJ, Tzeng SF, Pan Y, Fan P, Wang X, Li T, Khan MK. b-specs+: Batch verification for secure pseudonymous authentication in vanet. *IEEE Transactions on,Information Forensics and Security*. 2013; 8(11):1860–1875.
- [9] Shim KA. : An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. *IEEE Transactions on, Vehicular Technology* 2012; 61(4):1874–1883.
- [10] Liu JK, Yuen TH, Au MH, Susilo W. Improvements on an authentication scheme for vehicular sensor networks. *Expert Systems with Applications* 2014; 41(5):2559–2564.

- [11] Huang D, Misra S, Verma M, Xue G. Paap: an efficient pseudonymous authentication-based conditional privacy protocol for vanets. *IEEE Transactions on Intelligent Transportation Systems* 2011; 12(3):736–746.
- [12] Huang JL, Yeh LY, Chien HY. Abaka: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology* 2011; 60(1):248–262.
- [13] Jiang S, Zhu X, Wang L. An efficient anonymous batch authentication scheme based on hmac for vanets ; .
- [14] Lo NW, Tsai JL. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. *IEEE Transactions on Intelligent Transportation Systems* 2016; 17(5):1319–1328.
- [15] Cremers CJ. The scyther tool: Verification, falsification, and analysis of security protocols. *CAV*, vol. 8, Springer, 2008; 414–418.
- [16] Küsters R, Truderung T. Using proverif to analyze protocols with diffie-hellman exponentiation. *22nd IEEE, Computer Security Foundations Symposium, 2009. CSF'09.*, IEEE, 2009; 157–171.
- [17] Blanchet B, Smyth B, Cheval V. Proverif 1.90: Automatic cryptographic protocol verifier, user manual and tutorial. URL: <http://prosecco.gforge.inria.fr/personal/bblanche/proverif/manual.pdf> 2015; .
- [18] Zhang C, Lu R, Lin X, Ho PH, Shen X. An efficient identity-based batch verification scheme for vehicular sensor networks. *INFOCOM 2008. The 27th Conference on Computer Communications.*, IEEE, 2008; 246–250.
- [19] Yoon H, Cheon JH, Kim Y. Batch verifications with id-based signatures. *ICISC*, vol. 3506, Springer, 2004; 233–248.
- [20] Bellare M, Neven G. Multi-signatures in the plain public-key model and a general forking lemma. *Proceedings of the 13th ACM conference on Computer and communications security*, ACM, 2006; 390–399.
- [21] Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security* 2015; 10(9):1953–1966.

