A Framework for Secure Vehicular Communication Systems

*A **Thesis***

submitted in partial fulfillment of the requirements for the award of degree of

Doctor of Philosophy

by

Avleen Kaur Malhi

(901203001)

under the guidance of

Dr. Shalini Batra

Assistant Professor, Computer Science and Engineering Department,

Thapar University, Patiala-147004, INDIA

Computer Science and Engineering Department

Thapar University, Patiala -147004, INDIA

April 2016

Contents

List of Figures

List of Tables

List of Algorithms

Certificate

I hereby certify that the work which is being presented in this thesis entitled "**A Framework for Secure Vehicular Communication Systems**", in partial fulfillment of the requirement for the award of degree of "Doctor of Philosophy" 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. Shalini Batra and refers other research works which are duly listed in the reference section.

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

(**Avleen Kaur Malhi**)

Regn. No. 901203001

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

(**Dr. Shalini Batra**)

Assistant Professor

Computer Science & Engineering Department

Thapar University

Patiala, 147004

Punjab, INDIA.

Acknowledgements

I would like to express my sincere appreciation to my supervisor, **Dr. Shalini Batra**, for being a pillar of support and encouragement throughout my research work. Her experience, strength, tenderness and willfulness, has taught me valuable lessons of life, which are going to be of immense help to me in taking decisions in going forward.

My sincere thanks are due to **Dr. Deepak Garg**, Associate Professor and Head, Computer Science and Engineering Department (CSED), Thapar University, Patiala for providing me the necessary administrative assistance in completion of the work. I am thankful to my Ph.D. committee members, **Dr. Neeraj Kumar**, Associate Professor, Computer Science and Engineering Department, **Dr. V P Singh**, Assistant Professor, Computer Science and Engineering Department, and **Dr. Mandeep Singh**, Associate Professor, Electrical and Instrumentation Engineering, Thapar University, Patiala for their constructive comments and regularly ensuring the progress of my research work. I am thankful to all the **faculty** and **staff** members of CSED for their support.

I offer my deepest gratitude to my loving father, **Dr. Sukhwinder Singh Malhi** whose love and affectionate blessings have been a constant source of inspiration in making my vision a reality. I am also thankful to my mother **Mrs. Berinder Kaur** and my brother **Dr. Anmol Malhi** for their love, encouragement, motivation and their confidence in me.

I also acknowledge the cooperation and encouragement extended to me by my friends at Thapar University, especially **Mr. Vishal Sharma** and **Ms. Divya Pandove**.

The chain of gratitude would be definitely incomplete without thanking the **Almighty**,

the prime mover, for inspiring and guiding me (a humble being) to complete this task successfully.

Patiala

April, 2016

(Avleen Kaur Malhi)

Abstract

Vehicular ad-hoc networks have attracted comprehensive consideration in last few years for their assurance in enhancing driving safety and revolutionizing the transportation systems. Fundamentally, VANET security design should assure the security primitives of authentication, privacy, non-repudiation, integrity, availability, and in some peculiar application scenarios, confidentiality, to defend the network against intruders. Authentication ensures that a message is trustable by correctly identifying the sender of the message. The trust between vehicles is vital to efficiently transmit the data amongst vehicles. The new and attractive paradigm which eliminates the use of certificates in public key cryptography and solves the key escrow problem in identity based cryptography is certificateless cryptography.

A new certificateless aggregate signature scheme is proposed for VANETs with constant pairing computations. Assuming the hardness of computational diffie-hellman problem, the scheme is proved to be existentially unforgeable in the random oracle model against adaptive chosen-message attacks. A secure privacy preserving authentication framework is proposed which employs certificateless cryptography for authentication, pseudonyms for anonymous communication and multiple authorities are involved in revealing the identity of the vehicle in case of revocation. The signature verification scheme is improved by the use of bloom filters and the results achieved by the proposed scheme have been implemented on a simulated environment.

A fuzzy based trust prediction model is proposed to effectively compute the trust of other vehicles for the secure path formation in Vehicular Ad Hoc Networks (VANETs). The results and analysis of the proposed model over the standard protocols is presented using simulations.

A new misbehaviour detection scheme is proposed for the dissemination of correct information. The proposed countermeasures are proven to be efficient in detecting and blocking

the internal attackers from sharing the false warning messages. A new ubiquitous patient monitoring service called V-Health System is proposed to ensure the reliability of end to end communication between patients and healthcare services irrespective of time and location dependencies.

Chapter 1

Introduction

With the advances in wireless communication technologies and pervasive deployment of information, Vehicular Ad Hoc Networks (VANETs) have emerged as a promising solution aimed at providing the real time information to the vehicles by which the driver safety can be enhanced. Vehicular ad hoc networks, a major part of Intelligent Transportation Systems (ITS), is a self organized, service oriented wireless communication network aimed at accessing the real time information to disseminate the safety related information and traffic conditions to the driver prior to any traffic mishap which may occur. Vehicular communications are becoming increasingly popular, due to the car manufacturers investments, public transport authorities propelled by navigation safety requirements. VANETs are considered as vehicular sensor networks as they enhance the driver's safety through the exchange of traffic information by establishing inter-vehicle communication or communication with roadside infrastructure for ensuring the efficient traffic control system on the roads. The future vehicles need to be equipped with the communication capabilities to communicate with each other, roadside infrastructure and other concerned trusted authorities.

1.1 Background

Intelligent transportation systems are focusing on "smart vehicles"- vehicles equipped with significant computing, communicating and sensing. One of the important goals of VANETs is to provide safer and efficient traffic conditions by providing real time information to drivers and concerned authorities. A vehicular ad-hoc network is a form of Mobile Ad-Hoc Network (MANET) and inherits the key properties of MANETs. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbours and other vehicles in the network. VANET include all types of ad hoc networks formed by the use of short-range radios installed in private (personal consumer) and public (public transport and law enforcement authorities) vehicles. The first requirement of VANETs is to have each vehicle equipped with short-range radios for communication. The other components of a VANET node include those for providing detailed position information, Road Side Units (RSUs), and central authorities responsible for identity management and registration.

Communication in these networks involve both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications (Figure 1.1). V2V communications require the foremost attention and V2I communications comprise the infrastructure to support the completely connected network. Each vehicle in vehicular networks is equipped with devices like Event Data Recorders (EDRs) and sensors that support communication facility in VANETs. Vehicles communicate with one another and with road-side infrastructure when they are within their transmission ranges. VANETs possess features of high mobility, rapidly changing multi-hop topologies over wireless communication links.

Vehicular Ad-Hoc Networks serve as the primitive technology needed to actualize the multitudinous applications relevant to vehicular communications: traffic accidents, vehicle traffic conditions, safety, *etc.* VANETs are characterized by:

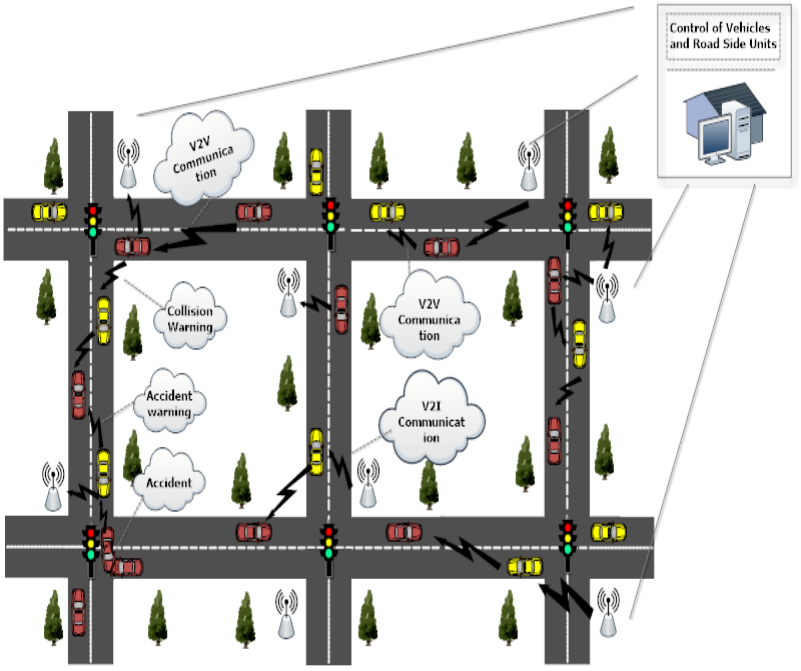

Figure 1.1: The general communication scenario in VANETs

- High velocity of the vehicles
- Determined mobility patterns that depend on source to destination path and on traffic conditions
- Intermittent communications (isolated networks of cars due to the fragmentation of the network)
- High congestion channels (e.g. due to high density of nodes)
- Environment factors: obstacles, tunnels, traffic jams, *etc*.

1.1.1 VANET Architecture

The basic VANET architecture (Figure 1.2) consists of one centrally Trusted Authority (TA) at the root followed by the State Trusted Authorities (STA) thereunder, which in turn is followed by City Trusted Authorities (CTA) in hierarchy. Under each CTA, there are number

of Road Side Units (RSUs) located along the road and each RSU controls the group of vehicles that are moving on the road.

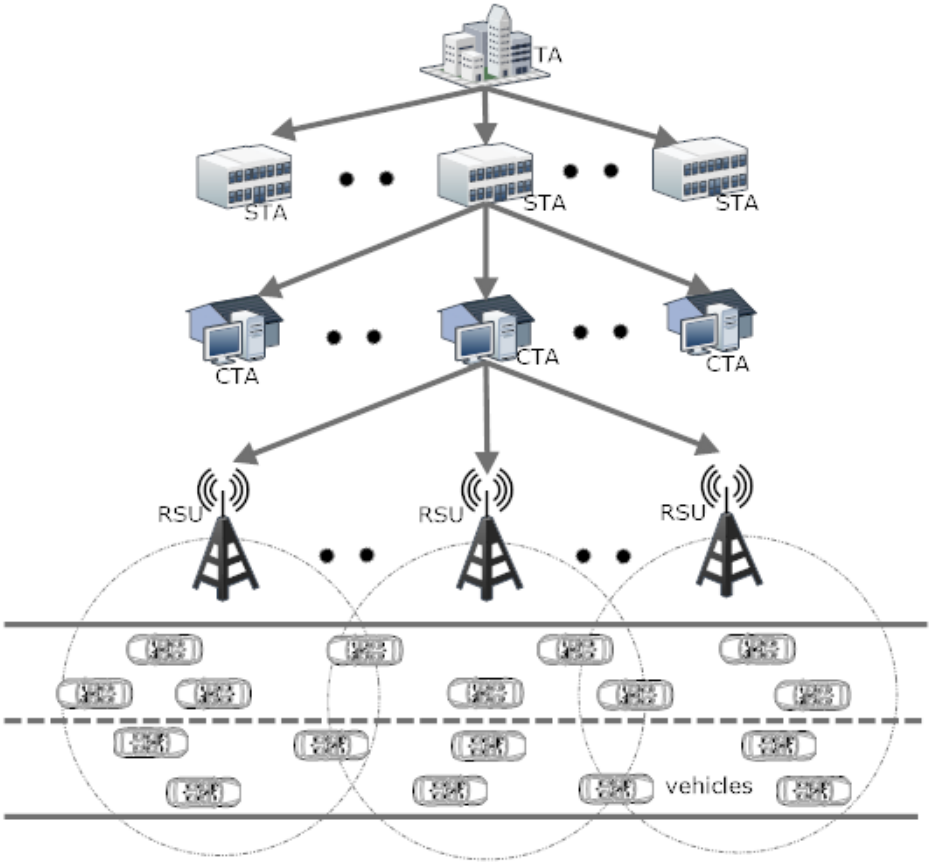

Figure 1.2: VANET general architecture

Each Onboard Unit (OBU) located on the vehicle has the ability to communicate with the other OBUs on the vehicles and RSUs located along the road. Each vehicle also consists of Tamper Proof Hardware (TPH) in order to store the keys and certificates. The function of TA is to control and manage the keys and certificates of STAs under it. Similarly, STA manages the keys and certificates of CTAs. CTA manages the key distribution and certificate management of the RSUs located under it and of the group of vehicles under each RSU. A vehicle will receive the keys and certificates from CTA via the corresponding RSUs under that particular CTA at the time of authentication for inter-vehicle communication. So, hierarchical architecture is maintained which is suitable in view of the scalable nature of VANETs.

1.2 Security of VANETs

The short-range radios are installed in vehicles, road side infrastructures and law enforcement authorities to make them capable of communicating with each other that constitute VANETs. There are various other components of a VANET that include providing accurate detailed position coordinates, road conditions, *etc*.

Dedicated Short Range Communication (DSRC) is one or two way short to medium range wireless communication channel specifically designed for automotive use. The Federal Communication Commission (FCC) allocated 75 MHz for DSRC in USA. Each vehicle can communicate with other vehicles and RSUs using DSRC radio signal being allocated for the vehicular technology in the range of 5.9 GHz band (5.850 GHz-5.925 GHz). The European Telecommunication Standards Institute (ETSI) allocated 30 MHz for DSRC in Europe. An amendment has been developed to the 802.11 standard in 2004 by the IEEE Task Group p, currently known as IEEE 802.11p [1] to include vehicular environments. IEEE 1609 is a higher layer standard based on IEEE 802.11p. The IEEE working group 1609 started specifying the further additional layers of the protocol suite. These standards are: IEEE 1609.1-resource manager [2], IEEE 1609.2-security [3], IEEE 1609.3-networking [4], IEEE 1609.4-multichannel operation [5]. The IEEE 1609.2 [3] standard describes the security services for applications and management messages. It defines the formats for secure messages, their processing, the circumstances where secure message exchanges can be used and how those message exchanges should be processed. The combination of the IEEE 1609 protocol suite and IEEE 802.11p standard is denoted as Wireless Access in Vehicular Environments (WAVE). The appropriate integration of on-board units, GPS receivers, computing platforms and communication capabilities not only opens astounding opportunities, but also increases research considerations. The major research challenge raised is security of VANETs. Without security, a vehicular network is wide open to a number of attacks such as generation of

false warnings by suppressing the actual warnings, suppressing the accident warnings, thus breaching the security of network and causing accidents. Therefore security is a major factor for attention in building Vehicular Ad-Hoc Networks.

The two contradictory facts while securing vehicular networks are to provide anonymity but at the same time allowing the law enforcement authorities to trace the misbehaving vehicle. The malicious vehicle in vehicular networks may cheat other vehicles by sending out bogus information which may be done purposely to throw another vehicle out of its way by dissemination of false traffic reports and clear up one's own way. There might be a scenario where false information may be sent to other vehicles by terrorists to block the police cars. Access to information on speed, status, trajectories and locations of the vehicles within the range of vehicles can be exploited by intruders to draw conclusions about a driver's identity, places of visit and social relationships. This kind of information may be exploited to expose the vehicles and drivers to harass, blackmail and other dangers [6].

The *Important Security Aspects* to be considered in VANET are [7]:

(a) Position verification techniques to thwart position spoofing attacks.

(b) Traceability by trusted network authorities (e.g., network administrator) for privilege revocation once misbehavior is detected.

(c) Identity and location privacy preserving mechanisms against unlawful tracing and user profiling.

(d) Non-frameability of an honest user who cannot be falsely accused of misbehaviour.

(e) Detecting the malicious data and correcting it to ensure data consistency.

(f) The system must have light overheads in terms of computational costs and high efficiency.

(g) Preventing impersonation attacks, that is, no one can impersonate another authorized member to cause service abuse problems and damage the security of VANETs.

(h) Preventing eavesdropping, i.e. an intruder cannot discover some valuable information from communications between members in VANETs.

1.2.1 Challenges

Since VANETs are the highly dynamic ad hoc networks, there are many security challenges which need major consideration in this area.

- **Dependence on Infrastructure:** The vehicle nodes need to authenticate themselves to the trusted authorities before they become the part of vehicular communications. As the vehicles need to authenticate via digital certificates in public key cryptography, obtain the private key from Key Generation Centre (in ID based cryptography), and the partial private key from trusted authority in certificateless cryptography, there is always need of authentication as it is mandatory for revocation and non-repudiation. Moreover, the vehicular communication signal gradually diminishes which needs to be amplified by the infrastructure. So, the vehicles need to depend on infrastructure for securing vehicular communications.

- **Communication range of RSUs:** The communication range of RSUs poses a constraint on vehicular networks. The communication range of a RSU is about 500 m in radius, i.e. Road Side Infrastructure is to be built at a distance of 1 km which is not feasible in view of the high network of roads in the developed countries.

- **Mobile nature of vehicles:** The high mobility of vehicles restrict the usage of the already implemented security solutions for other types of networks. The communica-

tion time and computation time needs to be greatly reduced without compromising the security of such ephemeral network.

- **Difficulty in trust management:** Due to high scale of the network, there is quite low probability that the two vehicles which maintained the trust relationships among them will meet in the future again. Moreover, it is very difficult to manage such large data in the onboard unit of vehicle as the vehicle will meet thousands of vehicles each day leading to the millions of vehicles per month. So it is difficult to manage trust in such large network.

- **Huge data:** Large amount of data is produced each day in vicinity of the large number of vehicles and high number of roads in the country. It is difficult to manage such huge data by the central authority, therefore decentralized approach is more acceptable for such networks. But at the same time, decentralized approach may hinder the revocation and non-repudiation of vehicles.

- **Scalability:** The highly scalable nature of the vehicles prevent the actual deployment of such networks as the security schemes need to be defined for whole network but the actual scale of the network is unpredictable at the first stage of deployment.

- **High cost:** The limited communication range of road side infrastructures leads to the deployment of large number of RSUs on the roads at the distance of 1 km which renders the high cost of such networks. Moreover, the high computational and computing platform of RSU also increases the cost of RSUs. Further, all the vehicles need to be equipped with communication facility, computing platform and storage capacity which incurs high costs for vehicle manufacturers and in turn, renders increase in the cost of vehicles.

1.2.2 Adversaries and their Attacks

A general classification of attacks substantiated by a list of attacks is:

Classes of Adversaries

The following broad classes of adversaries are identified in a vehicular environment.

I **Insider vs. Outsider.** The insider is an authenticated member of the network which can abuse the capabilities of the network. The outsider is an intruder in the network and hence is limited in the diversity of attacks he can mount and usually misuse the network-specific protocols.

II **Malicious vs. Rational.** A malicious attacker aims to harm the members of the network or disrupt the functionality of the network with no personal benefit. Hence, an attacker can adopt any means to harm the capabilities of the network. Whereas, a rational attacker tries to seek personal benefit in the network by predicting the attack means and attack target.

III **Active vs. Passive.** An active attacker fabricates packets or signals in the network, whereas a passive attacker eavesdrops on the wireless channel to gain the personal information of the network members.

IV **Local vs. Extended.** An attacker who is limited in scope and controls several network members (vehicles or base stations) is the local attacker. An extended attacker extends his scope by controlling several network members scattered across the network.

V **Independent vs. Colluding.** Attackers can act independently to exchange information or in collusion by cooperating with each other to make attacks more effective. For example, colluding vehicles can launch DDoS attacks by colluding with each other.

Attacks in VANETs

The deployment of VANETs expose it to multiple attack scenarios which hinders its deployment at the initial stage. The major attacks which are possible in VANETs are:

Greedy Drivers

Greedy drivers try to attack for their own benefit as a greedy driver might try to convince his neighbours that there is congestion ahead, and if his neighbours choose other routes, that greedy driver will get a terrific driving condition. Greedy drivers usually launch the attacks such as message falsification where the message is altered and message delay where the critical messages are not transmitted to its neighbours leading to fatal consequences.

Impersonation Attack

Eavesdropper tries to gain the personal information about the network entities by launching impersonation attack where an attacker may take on someone else's identity to gain the advantages in the network. Snoops can also launch privacy violation attack by associating the vehicles' identity with the sent messages. These are the threats to confidentiality of the network.

Illusion Attack

Attackers use this attack to alter their perceived direction, speed, position, *etc.* in order to escape from law enforcement authorities, notably in the case of an accident. The adversary tampers and misleads the sensors of the vehicle which broadcasts the misleading traffic warning signals. Thus, the incorrect traffic information broadcasted may lead to car accidents, traffic jams, bad road condition warnings and performance of VANETs deteriorates.

Wormhole Attack

In this type of attack, the packets received by one node at one location are tunnelled to another node at some other location in the network and are retransmitted again in the network. The wormhole attack is a serious threat in vehicular ad hoc networks which takes place even after employing all types of authentication and confidentiality checks in the network. Thus, the malicious nodes in the wormhole attacks disrupt the normal operations in the network.

Sinkhole Attack

In sinkhole attack, the compromised node lures all the traffic from its neighboring area creating a sinkhole in the center. The attacker or compromised node tries to attract all the data from its neighbors. The attacker tries to present itself as the most attractive relay in the neighbourhood.

Blackhole Attack

Blackhole is an area where no nodes are present or the present nodes refuse to participate in the communication leading to the loss of data packets. The nodes in the blackhole refuse to transmit the messages received from the legitimate nodes. Solutions to blackhole attack include that the designed routing protocols should have more than one routes to the destination to select the most optimal one.

Grayhole Attack

In Grayhole attack, the attacker misleads the network entities by agreeing to forward the data packets in the network but it starts dropping the packets as it receives the packets. Initially, the attacker behaves normally by replying to all the messages and as it receives the packets, the packets are dropped. It is different from the Blackhole attack that the packets are dropped

by the attacker while forwarding them in the grayhole attack.

Pranksters

Pranksters are the bored teenagers who try to attempt things for fun. For example, a prankster may convince one vehicle to slow down and the other to speed up. A prankster could also launch Denial of Service (DoS) attack or Message Alteration attack to disable applications by preventing critical information from reaching another vehicle or by altering the warning messages to no-warning messages, respectively.

Industrial Insiders

Industrial insiders, stay inside the car manufacturing company and can load the malicious firmware in the vehicle. The insider at one manufacturer could create keys that would be accepted by all other vehicles. Industrial insiders usually tamper with the security hardware of a vehicle by stealing identities and extracting cryptographic keys. Therefore, tamper proof hardware needs to be implemented in the vehicles.

Sybil Attacks

In this type of attack, the attacker fabricates and transmits multiple messages and each message uses different source identity to transmit the message. Thus, the receiver gets the illusion that the messages are received from different identities. Malicious attackers deliberately attempt to cause harm as these have specific targets, and are more professional. For example, the deceleration warning system may be manipulated by the terrorists to create gridlock before detonating a bomb. Sybil attacker floods the network with wrong information and the neighbours also believe the received messages as the messages are fabricated with different identities.

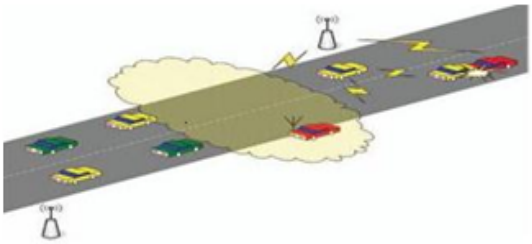

Figure 1.3: Jamming of signals

Denial of Service

The jammer deliberately generates interfering transmissions to prevent communication within their reception range (Figure 1.3). An attacker can partition the vehicular network easily with limited transmission power and without compromising cryptographic techniques. Sometimes, the attackers may try to transmit plenty of messages to jam the network channel and reducing the efficiency and performance of the network. The DoS attack may be launched by the outsider attacker where it transmits invalid messages in the network and exhausts the messages from the legitimate nodes. Thus, the messages from the legitimate nodes are prevented from processing by the invalid messages from the attacker. The Distributed DoS (DDoS) is more severe attack than the DoS in which a number of malicious nodes attack on a single legitimate node in distributed manner in different timeslots and locations.

Position Attacks

The location table is maintained by the GPS satellite maintaining location information with the vehicle's identity. The reading in the GPS system may be manipulated by the attacker to deceive the vehicle about its location.

Forgery

The correctness and timely receipt of the contents of the message is a major vulnerability. Forgery is caused by a single attacker which transmits false hazard warning messages (e.g., bad road conditions) leading to rapid contamination of large portions of the vehicular network with false information. The various dimensions and roadside behaviour of an attacker in VANETs are discussed by Leinmuller *et al.* [8].

In-transit Traffic Tampering

Any node acting as a relay can drop, corrupt, meaningfully modify or replay messages; disrupting communication. In this way, the reception of critical traffic notifications or safety messages can be manipulated. In fact, tampering with in-transit messages may be more powerful yet simpler than forgery attacks.
The classification of attacks and the adversaries are given in Table 1.1.

1.2.3 VANET Security Requirements

Security requirements are the measures that are put in place to secure the vehicular communication system from the effects of possible attacks identified in the section 1.2.2. The security requirements are basically derived from primary security goals of confidentiality, integrity and availability. From a review of existing literature [9][10][11][12][13], the general security requirements of a vehicular communication system are:

I. **Authentication:** Authentication ensures that the receiver correctly identifies the sender of the received message [9]. When the receiver verifies the unique identity of the sender, it is termed as ID authentication. Property authentication is a security requirement which verifies that the sender is a car, RSU, *etc*. The location authentication verifies

Table 1.1: Comparison of security attacks in VANETs

Name of Attack	Class of Adversary	Security Requirement hindered
Message Falsification Attack	Insider, Rational, Active	Data Integrity
Message Delay Attack	Insider, Rational	Data Integrity
Impersonation Attack	Outsider, Malicious, Passive	Authentication, Confidentiality
Illusion Attack	Insider, Malicious	Authentication
Wormhole Attack	Insider, Extended, Passive, Colluding	Authentication, Confidentiality
Sinkhole Attack	Insider, Independent, Local	Confidentiality
Blackhole Attack	Passive, Outsider	Availability
Grayhole Attack	Passive, Insider, Malicious	Availability, Data Integrity
Message Alteration Attack	Insider, Malicious	Data Integrity
Industrial Insider Attack	Outsider, Malicious	Data Integrity
Sybil Attack	Insider, Active, Local	Authentication, Availability
Denial of Service Attack	Outsider, Active, Local, Independent	Availability
Distributed Denial of Service Attack	Insider, Active, Colluding	Availability
Position Attacks	Outsider	Authentication
Forgery	Insider, Independent, Extended	Data Integrity
In-Transit Traffic Tampering	Insider, Active	Data Integrity, Confidentiality

the claimed location of the sender.

II. **Integrity:** Integrity requirements demand that the message should not be altered or dropped while it is communicated from the sender to receiver.

III. **Entity Authentication:** Entity authentication ensures that the recently received message is fresh and live. It prevents the message replay attack among the vehicles. It is ascertained that a message was sent as well as received in a reasonably small time

frame [11].

IV. **Confidentiality:** Confidentiality prevents the eavesdropping of the information sent between sender and receiver. The information transmitted should be accessed by only the sender and receiver of the message.

V. **Privacy:** Privacy is an important factor for the public acceptance and successful deployment of VANETs [14]. The collection of vehicle-specific information may lead to violation of the privacy of the drivers' personal data. A primary concern for vehicular networks is to provide location privacy for the vehicle, which prevents others from learning the location behaviour of the vehicle. Location privacy can be provided by adopting anonymity for vehicular communications. ID privacy [9] specifies upto what extent identity of the sender should be concealed so that the law enforcement authorities should be able to track the vehicles in case of any mishappening.

VI. **Availability:** The wireless channel should be available at all times so that the vehicles can receive the warning messages. If the radio channel goes out (e.g. jamming by an attacker, DoS or DDoS attacks), then the messages will not be broadcasted and VANETs become useless. Hence, it is critical for the vehicular communication systems to have high availability.

VII. **Access Control:** Access control is necessary to distinguish between different access levels of node or infrastructure which specifies what each type of node is allowed to do in the network [9]. The malicious vehicles are excluded from communicating in the network by the law enforcement authorities by the certificate revocation method or by calculating reputation score, *etc*.

VIII. **Auditability:** Auditability or the non-repudiation, is the mechanism by which the communicating vehicles can not deny that messages have been received or sent by them.

This requirement is of utmost importance in case of accident scenarios in identifying the actual cause of the accident.

IX. **Physical Security:** It prevents the unauthorised access of vehicle which includes compromising the security of the vehicle or tampering of cryptographic credentials. This can be prevented by adopting the tamper proof hardware in the onboard units of the vehicle.

1.3 VANET Security Mechanisms

The main difficulty today in developing secure systems based on public key cryptography is not the problem of choosing secure algorithms or implementing those algorithms. Rather, it is the deployment and management of infrastructures to support the authenticity of cryptographic keys. There is a need to provide an assurance to the user about the relationship between a public key and the identity (or authority) of the holder of the corresponding private key. In a traditional Public Key Infrastructure (PKI), an infrastructure based on public key cryptosystem leads to the creation of digital certificates by Certification Authority (CA) upon authentication of vehicles and distribution of certificates to vehicles for secure communication among them. A central repository is used by CA to store the digital certificates which are revoked in case of malicious activity by some entity. The digital certificates so created actually maps the public keys with the vehicular entities. In fact, digital certificates are used to verify that a particular public key is associated to a specific node in network. Therefore, PKI finds use in message authentication with the help of digital certificates and in key distribution. Public key infrastructure is not a viable solution in VANETs in view of the high vehicle mobility and real time guaranties. The overhead of certificate management and the keys sizes put a restraint on use of PKI in VANETs due to limited bandwidth. Further,

if there is an identity dispute, large effort is needed to resolve the same. The most primitive type of cryptosystems used for securing information is Symmetric Key Cryptosystem where the session key is being shared and agreed upon by the nodes that are used to process communication messages. In such approach, a common shared key is established between two nodes which is used to exchange all the messages between these two nodes for the current session. Such type of cryptographic mechanisms are in fact, time and space efficient. But, the pair wise shared keys are being prohibited from preloading in VANETs due to the huge scale of VANETs. Hence, there should be dynamic key establishment. Firstly, initial public key and certificate exchange is completed and then, 'ISO/IEC 11770-3 Key Transport Mechanism 3' [15] is used for key establishment which is considered the most efficient way. The symmetric keys are not so accurate solution for securing the VANETs as session key cannot be established between each pair of vehicles in the network hence, it is not feasible solution for highly scalable VANETs and soon exceeds in terms of overhead. The congestion-less wireless channel prevents the session key establishment for efficiency purposes in vicinity of only few vehicles. Further, symmetric key establishment prevents from achieving non-repudiation, which is foremost requirement for VANETs.

1.3.1 Identity Based Cryptography

The concept of Identity Based Cryptography (IBC) was propounded in 1984 by Adi Shamir [16]. This type of cryptosystem allows the arbitrary strings to act as public keys, i.e. public keys can be derived from public identity information of the network entity such as name, email address, IP addresses *etc*, which in turn can be used for encryption or signature verification purposes. There is no need of any digital certificates for public key verification as it was employed in conventional PKI. Thus, identity based cryptography curtails the complexity of the system significantly and the cost incurred in establishing and managing digital

certificates in traditional PKI is reduced drastically. An identity based signature scheme was constructed by Shamir [16] using the existing RSA function [17] but he could not formulate the Identity Based Encryption (IBE) scheme, which remained a long-lasting open problem till 2001 when this problem of Shamir was solved independently by Boneh and Franklin [18] and Cocks [19]. Since then, identity based cryptography has flourished in the research community due to their successful realization of identity based encryption. Bilinear pairing was used by Boneh and Franklin [18] and the variant of integer factorization problem was used by Cocks [19] to construct their identity based encryption schemes in 2001. The fundamental and functional encryption scheme on bilinear pairing based on elliptic curves using identity based cryptography was introduced by Boneh and Franklin [18]. IBE based on bilinear pairings are more widely in practice in VANETs. Identity based cryptography schemes are mainly employed for encryption, authentication, liability and tracing in vehicular ad-hoc networks. IBC infrastructure is more efficient as identity of user can act as public key thus preventing the exchange of public keys and certificates for public key verification. Thereby improving the communication and computational efficiency.

The field of identity based cryptography relies on the number theory field and related mathematical concepts [20] [21] [22]. Mathematical concepts used in IBE are:

- Roots of unity: When the complex numbers are raised to a given power of n, all of them yield the value of 1. These are also referred to as de Moivre numbers [23] which are the numbers that can be easily represented on the unit circle of the complex plane. Mathematically, the n^{th} root of unity can be defined as a complex number which satisfies: $\mathbb{Z}_n = 1$; n = 1,2,3.....

- Cyclic Groups: A cyclic group is a group in which all the elements are generated from a single element. In the cyclic group, there exists a generator 'g' which is used to generate the rest of the elements of the group which can be represented as the powers

of 'g' in multiplicative group and multiples of 'g' in additive group [24]. It is defined as: $\mathbb{G} = < g > = \{g^n$— n: integer$\}$

For eg. Suppose that G = g^0, g^1, g^2, g^3, g^4 is a cyclic, then the next elements can be represented as $g^5 = g^0$, $g^6 = g^1$ and so on.

- Group Generator: If each element of the group can be expressed as product of finite number of elements in any particular subgroup, then that subgroup S of a group is known as generating set of group [25]. If $\mathbb{G} = < S >$ then $\mathbb{G}$ is generated by S and the elements of S are used to generate the elements of $\mathbb{G}$. S is known as the *Group Generator* of $\mathbb{G}$.

- Group Order: The group order comprises the total count of the elements in a particular group [25]. Eg: if $\mathbb{G}$ = 1,2,4,7; then the order of group $\mathbb{G}$ is represented by: $|\mathbb{G}| = 4$ or ord $(\mathbb{G}) = 4$

- Bilinear Maps: The mathematical functions used for mapping the product of 2 linear elements to a third element within the same group are called bilinear maps [26]. Eg: suppose A and B are the linear elements of group $\mathbb{G}$, the bilinear map can be defined as: F : A * B $\longrightarrow$ C ; C is a third element in $\mathbb{G}$. Another example is multiplication of elements in the integer group N. For instance 2, 3 $\in$ N and 2, 3 = 6 $\in$ N. Hence, integer multiplication is bilinear map.

1.3.2 Certificateless Cryptography

Al-Shamir and Paterson [27] invented the concept of Certificateless Public Key Cryptography (CL-PKC) which is a variant of identity based cryptography and in practice nowadays due to its enticing characteristics. It alleviates problem of the overhead of certificates faced in PKI and escrowing an identity in ID based cryptography. CL-PKC is considered to be

well suited for VANETs in perspective of limited bandwidth and the dynamic nature of such networks. CL-PKC uses a third party called Key Generation Center (KGC) to generate the partial private key for an entity which is then combined with the secret key chosen by entity for the generation of full private key. Then, the user uses the public parameters of KGC and the secret key to compute the public key. The concept of partial private keys was introduced in CL-PKC because if the full private key is generated by the KGC as in IBC [28], then KGC will have the full access on the private key of users and may abuse the capabilities of the network. The notion of partial private key was given in CL-PKC to ensure high security of the network.

Preliminaries

The bilinear pairing is denoted by e and can be defined over groups $\mathbb{G}_1$ and $\mathbb{G}_2$, both of which are having the prime-order q. The operation in $\mathbb{G}_1$ is denoted by an additive notation while an operation in $\mathbb{G}_2$ is denoted by multiplicative notation. The hardness of the scheme lies on Discrete logarithm problem (DLP) and it is assumed that DLP is intractable in both groups $\mathbb{G}_1$ and $\mathbb{G}_2$. Practically, the group $\mathbb{G}_1$ is implemented by a group of points on an elliptic curve, having a small MOV exponent [20] and group $\mathbb{G}_2$ is implemented by a subgroup of the multiplicative group of a finite field. Let P denote a random generator of $\mathbb{G}_1$. The justifiable bilinear map $e : \mathbb{G}_1 \ \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ is constructed with following properties:

I Bilinear: e(aP, bP) = e(abP, P) = e(P, abP) = $e(P,P)^{ab}$, for every P, Q $\in \mathbb{G}_1$ and for every a,b $\in {}_R\mathbb{Z}_q^*$

II Nondegenerate: e(P,Q) = 1, $\exists$ [P,Q] $\in \mathbb{G}_1$

III Computable: e(P,Q) can always be computed with the help of an effective algorithm such that, for every P,Q $\in \mathbb{G}_1$.

The bilinear pairings are constructed by Tate pairings or Weil pairings [18]. The certificateless cryptography's security depends on the hardness of the following computational problems:

Computational Diffie-Hellman (CDH) problem: Let cyclic group $\mathbb{G}_1$ with order q has a generator P, and given two points, aP and bP for unknown a, b $\in \mathbb{Z}_q^*$, then to compute abP is computationally infeasible.

Decisional Diffie-Hellman (DDH) problem: Let cyclic group $\mathbb{G}_1$ with order q has a generator P, and given the points, P, aP,bP and $g \in \mathbb{G}_1$ for unknown a, b $\in \mathbb{Z}_q^*$, to decide whether $g = abP$ is computationally infeasible.

Bilinear Diffie-Hellman (BDH) problem: Let $< P; aP; bP; cP >$ with unknown random choices of a, b, c $\in \mathbb{Z}_q^*$ be given, then to compute $e(P,P)^{abc} \in \mathbb{G}_2$ is computationally infeasible.

1.4 Applications of VANETs

Some of the major applications of VANET include providing safety information, traffic management, toll services, location based services, infotainment *etc*. The various VANET applications based on deliberations between government agencies and private industry have been identified, which are traffic signal violation warnings, curve speed warnings, emergency electronic brake lights, pre-crash warnings, cooperative forward collision warnings, left-turn assistance, lane change warning, and stop-sign movement assistance. One of the major applications is providing safety related information to avoid collisions, reducing pile up of vehicles after an accident and offering warnings related to state of roads and intersections. Affixed with the safety related information are the liability related messages, which would determine which vehicles are present at the site of the accident and later help in fixing cause

for the accident. However, without securing these networks, they would lend themselves to blatant abuse, leading to major problems and immense damage to life and property.

1.5 Thesis Organization

The organization of the thesis is as follows:-

Chapter 1: Introduction: This chapter provides introduces vehicular ad hoc networks, its security, security challenges, requirements and applications. Further, it provides the overview of the identity based and certificateless cryptography.

Chapter 2: Literature Review: This chapter provides the comprehensive survey of work done in the area of security of vehicular ad hoc networks and highlights the various frameworks proposed. A comparative study and analysis of the existing security frameworks for VANETs has also been provided in this chapter.

Chapter 3: Proposed Certificateless Signature Scheme: The proposed 'Certificateless Aggregate Signature Scheme' for vehicular ad hoc networks is presented in detail. The proposed signature scheme is proven existentially unforgeable in the random oracle model against chosen message attacks, assuming the hardness of computational diffie-hellman problem.

Chapter 4: Privacy Preserving Authentication Framework: In this chapter, a privacy preserving pseudonym based security framework is proposed which employs the use of bloom filters in message verification process. A new designed aggregate certificateless digital signature scheme is employed for inter-vehicular communication allowing the vehicles to anonymously communicate with each other. The bloom filters are used to enhance the aggregate message verification process and the security analysis of the proposed security scheme is also presented.

Chapter 5: Experiments and Implementation Details: This chapter provides the implementation details of the proposed framework where authentication of the efficiency of the proposed framework has been done thoroughly. Various evaluation parameters used for measuring its performance have also been discussed. The security library MIRACL and the network simulator NS-2 have been used.

Chapter 6: Effective Vehicular Communications: This chapter proposes the fuzzy based trust prediction model for vehicular communication systems for effective transmission of messages. It also discusses the two XML based modules of the secure vehicular ad hoc networks by the design of the decision inference system for the vehicle misbehaviour detection and the V-Health system for the faster dissemination of medical aid.

Chapter 7: Conclusion and Future Scope: Thesis concludes with this chapter by providing a brief overview of the proposed framework and providing a insight into the future scope of the work.

Chapter 2

Literature Review

With the intent to enhance the traffic safety and driving conditions, VANETs enables the vehicles to communicate with each other and exchange traffic related information. The data on traffic conditions is of prime importance due to which the Intelligent Transportation Systems (ITS) have developed various techniques that allow them to characterize the traffic flow conditions on the road and make intelligent decisions accordingly. VANETs are nowadays getting increased attention from the academia and industry due to its potential and tremendous applications. VANETs deployment can be considered as a next generation network which will be very useful in traffic analysis and management. The brief summary of the recent literature related to the security and privacy in VANETs is presented revealing the different authentication, verification strategies, intrusion and misbehaviour detection schemes.

2.1 Certificateless Signature Schemes

The idea of Certificateless Public Key Cryptography (CL-PKC) was given by Al-Shamir and Paterson [27] where the concept of partial private keys was introduced in CL-PKC. CL-PKC is considered to be well suited for VANETs in perspective of limited bandwidth and the

dynamic nature of such networks. The certificateless signature scheme presented by Riyami *et al.* [27] can not be used in VANETs as it employs more computational cost in signature generation and verification processes but the high mobility of vehicles in the network puts an urgent need to reduce the computational time as much as possible to support the reliable message delivery in the highly dynamic vehicular ad-hoc networks.

The first certificateless encryption scheme was given by A. Shamir [29] along with the formal proof for his scheme. Boneh *et al.* [30] firstly introduced the concept of aggregate signatures. After that, many aggregate signature schemes have been proposed [31] [32] [33], since Boneh *et al.*'s scheme is proposed. The concept of aggregate signatures can be much efficiently used with ID-based signatures and certificateless signatures as certificateless cryptography does not pose a constraint of certificate overhead. The security model of CL signature schemes was given by Huang *et al.* [34], but the ability of adversaries was not fully covered in CL-PKC by this model as the certificateless scheme which was secure in this model might be insecure in actual practice. The more generic way to construct CL signature schemes was put forward by Yum and Lee [35] which was proved insecure by Hu *et al.* [36] and they presented the security model of CLS schemes. A new CLS scheme was propounded by Liu *et al.* [37] which was proven secure in standard model. Huang *et al.* [38] presented the two new constructions of the security models of certificateless signature schemes. Choi *et al.* [39] presented two new efficient constructions of certificateless signature schemes but Boneh *et al.* [30] proved their security in weak adversary model. Du and Wen [40] had given a very efficient short CLS scheme with few mistakes in their security proof. A very efficient CLAS scheme was presented by Zhang *et al.* [41] which was secure in the random oracle model. Certificateless signcryption scheme was proposed by Miao *et al.* [42] but signcryption has high computational overhead in highly dynamic networks such as VANETs. The certificateless threshold signature scheme was given by Xiong *et al.* [43] where the

signing power was distributed among the multiple signers which is not a viable solution in VANETs. A certificateless two party authenticated key agreement protocol was proposed by He *et al.* [44] but the two party communication is not feasible in large scale vehicular ad hoc networks. So far, very little attention has been devoted for the design of certificateless signature schemes for specific application scenarios such as VANETs.

2.2 Security Frameworks

The subject related to security in VANETs has so far being overlooked by both academia and industry which has been postponed to the later stages of implementation and deployment. But, the security of these networks can not be overlooked as security is the major milestone to be accomplished before the deployment of VANETs. Gandhi *et al.* [45] gave the review of the security solutions in Mobile ad hoc networks. Many frameworks have been proposed so far for vehicular ad hoc networks and are being discussed in this section. Choi and Hong [46] described the management and operations of the next generation networks which comprised a heterogeneous environment of wired and wireless networks. The future internet requirements and the services provided were discussed by Hong *et al.* [47] with the special focus on issues of future internet and proposed the operations, requirements and management of future internet services. Raya *et al.* [48] proposed an authentication scheme for VANETs where the short lived certificates were preloaded in the vehicle OBU along with short pseudonyms. This approach is not much feasible in vehicular networks as it possesses the certificate overhead problem because each time a new pseudonym along with its certificate was used for new message. Moreover, it incured a revocation problem because CRL grows at a tremendous rate due to the large pool of certificates. Raya *et al.* [49] also proposed a mechanism based on ECDSA signature mechanism where anonymous key pairs were preloaded into the tamper

proof hardware of the vehicle along with the anonymous certificates. The revocation problem was dealt by proposing three protocols for revocation. Another security architecture was designed by Sun *et al.* [50] where pseudonymous based scheme was used for attaining privacy and threshold based signature scheme was used to achieve non-repudiation in the vehicular networks. It incorporated the threshold based authentication scheme where the authentication of the vehicle beyond some threshold might result in the revocation of the vehicle but there was limitation on defining the threshold. Moreover, it rendered signaling overhead problem as whole bandwidth of the network might be consumed in setting the threshold value. Many group based signature schemes [51][52][53] were proposed where privacy of the signer was conditional on the group leader but these schemes had the problem that the signer privacy could be revealed by the group leader and thus leading to the violation of security primitive of privacy. Moreover, the group formation and election of the group leader possess a constraint on the reliability of such group based security frameworks in highly dynamic networks such as VANETs.

The message verification policies should be appropriately chosen to enhance the message verification process of vehicles as multitude of messages needs to be verified in a small duration of time before new messages are received. Li *et al.* [54] proposed a message verification strategy where the messages were verified according to the priority set and the priority was determined by the distance between sender and receiver *i.e.* less the distance, more the priority. The rest of the messages were verified in a random manner. Aggregate verification schemes [55][56] were proposed for VANETs where bilinear pairings were used to verify the messages in a single batch. Cheon *et al.* [57] proposed a fast batch verification scheme which used the bilinear pairing to aggregately verify all the signatures. Kim *et al.* [58] proposed an inter-vehicular communication scheme where batch verification scheme was presented and multiple messages were verified using bloom filters [59]. This scheme

was proposed to reduce the overhead of group rekeying where the group key was updated in the vehicle using bloom filter which reduced the number of communications involved and optimized the time. Bloom filters are the space efficient data structures and possess a constant search time complexity. However, the authors did not utilize the bloom filter in verifying the received periodic messages to enhance the message verification process based on their priorities.

Another lightweight certificate based group key framework was proposed by Yeh *et al.* [60] where group leader was responsible for management of groups and keys of the members of the group. It was computationally lightweight but the certificate based framework itself creates high overhead in managing the certificates in highly dynamic network. Wagen *et al.* [61] proposed a security framework based on asymmetric and symmetric cryptography where asymmetric cryptography was used for securely exchanging the key and authentication process and symmetric key was used for safety applications to reduce the latency of the network. The ID based framework was proposed by Lu *et al.* [62] with identity based signatures for authentication between vehicles and RSUs; and ID Based Online/Offline Signature(IBOOS) scheme was proposed for authentication between vehicles. Self generated pseudonyms were used instead of real identities of the vehicles. IBOOS divided the signing process into two phases, offline phase and online phase to speed up the signing process. Initially, vehicles or roadside units execute offline phase employed for R2V(Roadside to Vehicle) or V2R (Vehicle to Roadside) communications and vehicles execute online phase for V2V communication. The IBOOS scheme was extended in ACPN scheme [63] where PKC based pseudonyms were generated for privacy preservation which were updated on the demand of vehicles. So, the scheme provided the privacy preserving authentication with non-repudiation. The revocation mechanism for vehicular ad hoc networks was also proposed by Ganan *et al.* [64] where Certification Authority (CA) accumulated all the revocation infor-

mation of the vehicles in one single value which was transmitted to all other vehicles in the network. Thus, it provided the accurate information regarding revocation of each vehicle while ensuring the privacy of the vehicles. Xue *et al.* [65] proposed a mechanism where top authority issued group certificates to vehicles through the RSUs and employed the digital signature generation and verification procedure for safety messages. Biswas *et al.* [66] proposed a identity based authentication scheme which was proven insecure by Tsai [67] as it was vulnerable to private key reveal attack. The weakness was improved by Tsai's scheme [67] which supported the identity revocation, where the signature receiving entity was able to check if the signature was received from the revoked vehicle or not. Wasef *et al.* [68] proposed a distributed certificate based signature scheme for vehicular ad hoc networks where the aggregate signature verification was employed to increase the efficiency of the network. Bhushan *et al.* [69] proposed a new methodology known as Common Junction Methodology to reduce the network overhead by optimizing the overlay traffic at underlay traffic. The traffic is routed through the common junction found by this methodology between the available paths. The availability issue was considered in mobile ad hoc networks by Chand *et al.* [70] where a strategy based on cooperative caching was proposed to improve the performance of data access.

A new secure congestion control protocol was proposed by Younes *et al.* [71] to provide the integrity and authenticity of the messages transmitted over the network and detect the security threats. It employed the public key cryptography for authenticating RSU at road intersection and employed the group signatures as well as identity based signatures for inter-vehicular communication. However, the proposed protocol inferred more communication overheads. The group based signatures were also implemented and evaluated on the mobile devices by Isern-Deya *et al.* [72] using android platform. Another trust based authentication scheme was proposed by Chuang *et al.* [73] for vehicle to vehicle communications. It was

a lightweight decentralized approach which adopted the transitive trust relationships to enhance the authentication method. A symmetric cryptography based secure communication network was given by Zhu *et al.* [74] by developing two party key and group key distribution and agreement protocols for various VANET scenarios. It solved the key leak problem which was caused by the vehicles joining or leaving the network. The aggregate signatures were employed and point addition was substituted by XOR operation but the symmetric cryptography itself imposed a high overhead in highly dense vehicular environments. Wang *et al.* [75] also proposed a lightweight symmetric encryption based authentication scheme which employed the Message Authentication Code (MAC) for message signing and verification processes. The scheme utilized the pseudo identities for the privacy preservation and conditional traceability in vehicles.

2.3 Classification of Security Mechanisms

The search is being classified based on two classifications namely, cryptographic techniques and trust management techniques. Figure 2.1 lists the various security schemes adopted by the researchers in a hierarchical manner to secure vehicular networks.

2.3.1 Cryptographic Techniques

The cryptographic techniques include the four major cryptographic techniques: symmetric key, public key, identity based and the certificateless cryptography. This section provides a concise study of recent literature related to proposed security frameworks and strategies used to secure vehicular communications.

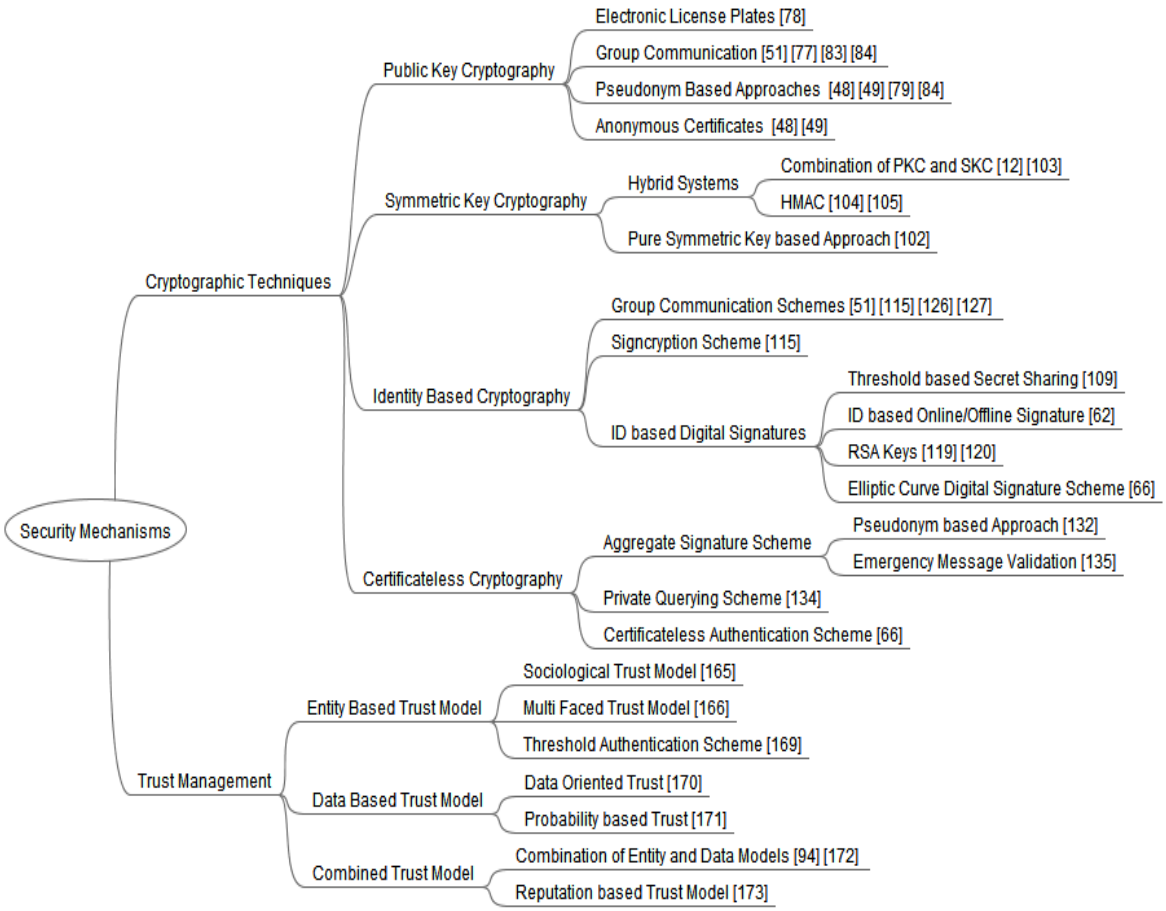

Figure 2.1: Overview of the literature for securing VANETs

Public Key Infrastructure

Since VANETs need to be protected from outsiders and malicious insiders, legitimacy of messages is mandatory. The messages exchanged among vehicles and trusted authorities must be authenticated. The vehicle firstly authenticates itself to a trusted authority which issues the pubic keys to vehicles. An infrastructure based on public key cryptosystem leads to the creation of digital certificates by Certification Authority (CA) upon authentication of vehicles and distribution of certificates among vehicles for secure communication among them. A central repository is used by CA to store the digital certificates which are revoked in case of malicious activity by some entity. The digital certificates so created actually maps the public keys with the vehicular entities. Digital certificates are used to verify that a particular

Table 2.1: Comparison of public key infrastructures for VANETs

Security Schemes	Anonymous certificates	Pseudonyms	Group Formation	RSU aided	Traceability by TA	Anonymity	Group signatures	Revocation
["Blum et al. 2004"][77]	×	×	✓	×	×	×	×	×
["Hubaux et al.2004"][78]	×	×	×	×	✓	✓	×	✓
["Gerlach et al.2007"][79]	×	✓	×	×	✓	✓	×	✓
["Raya et al. 2006a"][83]	×	×	✓	×	×	✓	✓	×
["Raya and Hubaux 2007"][49]	✓	✓	×	×	✓	✓	×	✓
["Huang et al. 2005"][84]	×	✓	✓	✓	×	✓	×	×
["Raya et al. 2006b"][85]	✓	✓	×	✓	✓	✓	×	×
["Lin et al. 2007"][51]	×	×	✓	✓	✓	✓	✓	✓

public key is associated to a specific node in network. Therefore, PKI finds use in message authentication with the help of digital certificates and in key distribution. Hu *et al.* [76] mentioned the security objectives of VANET framework as authenticity, privacy, information availability, short term linkability, efficiency, traceability and revocation. A new security architecture was described by Blum and Eskandarian [77] for VANETs to counter the attack known as intelligent collisions (which are intentionally caused). The knowledge of potential threats is necessary to build a security architecture. A virtual infrastructure was used by them where clusters of vehicles were used and cluster-heads were responsible for digitally signing the messages using PKI for their reliable dissemination. The drawback of this approach was that bottlenecks were created at cluster-heads and further, it was difficult to manage such clusters in highly ephemeral networks. Hubaux [78] focused on the privacy of vehicles by managing the tradeoff between privacy and liability and used the unique electronic identifiers of the vehicles known as Electronic License Plates (ELP). The security concepts for vehicular networks were defined by Gerlach *et al.* [79] by describing four viewpoints. Security aspects had been taken into consideration by Raya *et al.* [80] while talking about VANETs. Luo and Hubaux [81] proposed the introduction of the MAC layer in VANETs along with discussion on security issues by Raya *et al.* [82].

Secure aggregations were discussed by Raya *et al.* [83] to increase the channel efficiency

in vehicular networks where there existed geographically dissected maps into tiny area cells and vehicle compared its GPS location with the already loaded dissected area maps to know its group. The cell length was 400 m and group leader was in center which assigned group key to all the members of the group. The drawbacks of such a group based approach was that firstly, group leader was difficult to manage as vehicles continuously changed their location and secondly, group formation was difficult in vicinity of too few vehicles. Eichler *et al.* [86] provided a general overview of Car to Car communication (C2C comm.). Raya and Hubaux [49] proposed a new approach based on the pseudonyms where anonymous public keys were used along with the public key certificate for each anonymous public keys. However, this scheme had some shortcomings as it gave rise to high storage overhead of anonymous public keys and certificates leading to extra communication. Raya and Hubaux had focused on particular VANET security subjects and gave a complete overview of the architecture that could be used in the implementation of such networks [87][80]. The various challenges encountered in vehicular networks including attacks and adversary types were discussed by Parno *et al.* [88] and they discussed the issue by providing discrete security mechanisms for securing VANETs.

Zarki *et al.* [89] described architecture for vehicular ad-hoc networks by concisely remarking the various security concerns and their feasible resolutions. The concept of digital signatures usage in VANETs was given by Gollan *et al.*[90]. The CARAVAN scheme [34] preserved privacy of the vehicles with the help of formation of groups in case of applications where vehicles needed to communicate with infrastructure. The group leader accesses the infrastructure on behalf of the whole group members and when the infrastructure was not accessed by vehicles, eavesdroppers were prevented from tracking pseudonyms of the vehicles by remaining silent. Gerlach offered a different perspective for implementing security models in car to car communication [91] by focusing on the functional layer view and im-

plementing the concepts which are used for securing vehicular communications. Raya *et al.* [85] proposed a different authentication scheme for vehicular communications where large number of short-lived anonymous certificates were used and were preloaded in OBU of vehicle. When the vehicle needed to sign the message, a certificate was used from the certificate pool. This approach had the drawback that large certificate pool might lead to identity dispute as severe efforts were needed to resolve it. SeVeCom security framework was described by Raya and Papadimitratos [11] [92] in which architecture, vulnerabilities, challenges and cryptographic support were discussed in a detailed way to offer a more practical view on the problems that could occur. An architecture was described by Raya *et al.* [93] for private vehicular communications focusing on the management of identities and cryptographic keys. Zhang [94] also discussed the security in VANETs in which the author implemented attacks and discovered weaknesses in the VANET security layer. The PKI-based authentication was combined with TESLA [95] protocol for VANETs to present a new anonymous authentication approach [51]. The first message which is signed and sent by sender was verified by trusted authority. Then, by using the TESLA procedure, the subsequent messages were authenticated by receiver by directly comparing the Message Authentication Code (MAC) only if first message was authenticated. But, the receiver needed to store all digital certificates of adjoining nodes for long time leading to storage overhead. Moreover, message authentication started after the second message was received from the same sender which seemed to be infeasible in delay intolerant networks.

USA addressed the DSRC Consortium [96] as the most extrusive industrial effort in vehicular networks. There are many ongoing endeavours in the realm of vehicular networks such as network-on-wheels project [97], car-to-car consortium [98], DSRC consortium [99] and SEVECOM [100] among others. After going through various proposed schemes discussed above, it is quite evident that the public key infrastructure is not a viable solution in

Table 2.2: Comparison of the various symmetric key approaches

Security Schemes	Privacy	Scalability	pseudonyms	Group Formation	RSU aided	Non-Repudiation	Hybrid System
["Burmester et al. 2008"][101]	✓	×	×	×	×	×	✓
["Plob et al. 2008"][12]	✓	×	×	×	✓	✓	✓
["Choi et al. 2005"][102]	✓	×	×	×	✓	✓	×
["Freudiger et al. 2007"][103]	×	✓	×	×	✓	×	✓
["Chim et al. 2012"][104]	✓	✓	✓	×	✓	✓	✓
["Hu et al. 2012"][105]	✓	×	✓	✓	✓	✓	✓

VANETs in view of the high vehicle mobility and real time guaranties. The overhead of certificate management and the key sizes put a restraint on use of PKI in VANETs due to limited bandwidth. Further, if there occurs an identity dispute, rigid effort is needed to resolve the same. If anonymous keys and short lived certificates are used for privacy preservation, it renders a high overhead on the network to manage large number of certificates. Table 2.1 gives the comparative analysis of proposed public key infrastructures for VANETs.

Symmetric Key Approaches

The most primitive type of cryptosystems used for securing information is symmetric key cryptosystem where the session key is shared and agreed upon by the nodes that are used to process communication messages. In such approach, a common shared key is established between two nodes which is used to exchange all the messages between these two nodes for the current session. Such type of cryptographic mechanisms are in fact, time and space efficient. But, the pair wise shared keys are being prohibited from preloading in VANETs due to the huge scale of VANETs.

A hybrid system was proposed by Burmester *et al.* [101] that used both symmetric and asymmetric approaches to provide security in VANETs. The hybrid system provided the confidentiality, authentication and privacy preservation. It defined two types of communications: pair wise, when two nodes needed to communicate and group communication, when

more than two nodes required communication. Symmetric keys were used in pair wise communications to avoid the overhead of using public key pair. Another security architecture was given by Plob *et al.* [12] where PKI was employed at initialization exclusively for safety messages and the other messages such as periodically sent beacons employed symmetric key cryptography for maintaining the privacy of the participating entities. The symmetric key was established between the vehicle node and the trusted third party. However, drawback of this approach was that the vehicles had to contact the Trusted Third Party (TTP) to decrypt and verify message every time leading to high overhead in highly scalable vehicular networks. A lightweight security mechanism was proposed by Choi *et al.* [102] to balance the privacy and liability in VANETs. It was non suitable for inter vehicle communication as the neighboring vehicles required authenticating each other through the road side units, which is not feasible in such highly dynamic networks. Freudiger *et al.* [103] introduced mix zones which were developed at road crossings for achieving location based secrecy in vehicular communications by mixing the vehicle identifiers at the intersections. Vehicles within the mix-zones used the symmetric keys with RSUs to exchange messages with RSUs. These solutions were more efficient in high traffic congestions to prevent tracking of vehicles. However, drawback was that overhead was incurred in mix-zones and non-repudiation was difficult. A new scheme was proposed by Chim *et al.* [104] where authentication of regular messages was done by using Hash-based Message Authentication Code (HMAC) and endorsed public key cryptosystem for the verification of urgent messages by using some conditional privacy-preserving authentication scheme. Hu *et al.* [105] also provided the scheme using Hash-based Message Authentication Code in VANETs. The secure communications between vehicular nodes and road side units was achieved by symmetric encryption with HMAC checking. The groups of vehicles having a shared key were maintained and group communication among vehicles was done using symmetric encryption along with HMAC

calculation.

The symmetric keys are not viable solution for securing the VANETs as session key cannot be established between each pair of vehicles in the network so, it is not appropriate solution for highly scalable VANETs and exceeds in terms of overhead. The congestion-less wireless channel prevents the session key establishment for efficiency purposes in vicinity of only few vehicles. Besides, symmetric key establishment do not achieve non-repudiation, which is foremost requirement for VANETs. The various symmetric key schemes are discussed in table 2.2.

Certificate Revocation

Certificates of any vehicle are revoked when some vehicle misbehaves in the network and in turn, Road Side Unit (RSU) revokes its certificate to prohibit its communication with other vehicles in the network. Mostly, Certificate Revocation Lists (CRLs) are shared among all the VANET entities to revoke the certificates which are provided through the available infrastructure. Moreover, the keys are automatically revoked when short lived certificates are used. IEEE P1609.2/D2 draft standard [3] proposed these methods. Raya *et al.* [49] propounded three protocols for certificate revocation namely, Revocation protocol of Tamper-Proof Device (RTPD), Revocation protocol using Compressed Certificate Revocation Lists (RCCRL) and Distributed Revocation Protocol (DRP). These protocols were introduced because standard methods of revocation cause high overhead. A novel certificate revocation proposal was introduced by Lin *et al.* [106] where secret keys were granted for each RSU by trusted authority to sign all the messages communicated in the range of RSU. During certificate revocation, Trusted Third Party (TTP) sent messages to all the RSUs and the RSUs in turn broadcasted the messages to all the vehicles which were in range of RSU to revoke the appropriate vehicle and the vehicle was restricted from communication. A blacklisted anonymous

credential system was proposed by Tsang *et al.* [107] to block the misbehavior without use of trusted authority. This approach can be feasible in VANETs: the vehicular entity needed to assure that blacklist did not contain its ID and if it fails to do so, the messages from that vehicle will be ignored. A threshold based authentication mechanism was proposed by Sun *et al.* [108] and the traceability was provided by network authorities by tracing misbehaving vehicles. Few other schemes [109][110] were adopted to leverage the pseudonyms in vehicular networks where the revocation was possible only in few revocations feasible in finite settings. The privacy preserving revocation mechanism was proposed by Ganon *et al.* [111] by using the merkle hash trees and a crowds based anonymous protocol which reduced the certificate status checking overhead. Merkle Hash Tree [112] is a data structure that is build with one way hash function where children nodes carry the hash value of data and the internal nodes concatenate the hash values of their children. This approach provided a scalable way to distribute the revocation information in the network.

There are several problems incurred in distributing CRLs. First, it can be difficult to manage huge CRLs as these tend to be quite long in view of high number of vehicular nodes and their high mobile nature as the vehicle while travelling the long distances can confront a large number of vehicles. Moreover, it is not bandwidth efficient and requires additional communications to distribute huge CRLs. Second, if the short lived certificates are used, it still creates a vulnerability window as the CRL size grows at a high rate. Third, the additional storage requirements are needed in the onboard of vehicles to store large CRLs. Last but not least, the distribution of the CRLs depends heavily on the availability of infrastructure.

Identity Based Cryptography Approaches

Recently, the identity based approach has become the mainstream in VANETs security due to the properties of VANETs. Earlier security approaches relied on Public Key Cryptog-

raphy or Symmetric Key Cryptography but researchers have discovered recently that such security approaches are not the best choices for security of infrastructure-less networks like VANETs. Moreover distribution and management of keys, key sizes and certificate overhead pose a constraint on using the public key infrastructure due to limited bandwidth. Further, VANETs are delay intolerant networks and require real time services therefore; symmetric key cryptography is also not preferred. Hereby, ID based cryptography is presently believed as a practicable choice for VANETs. Few researchers have proposed usage of Identity based Cryptography for securing VANETs. A ring signature scheme [113] based on IDBC was proposed by Gamage *et al.* [114] where ring signature scheme was modified for achieving ambiguity of signer to enhance the privacy requirements in vehicular networks. However the ring signature scheme is not suitable in VANETs as it results in conditional privacy leading to non-repudiation unattainable, which is the foremost requirement of VANET. Chen *et al.* [115] proposed a group signature scheme based on IDBC where privacy of signer lied in the hands of group manager. The group members registered themselves to an authority named Group Registration Manager (GRM) and could sign any message on behalf of group. This scheme provided liability as GRM could disclose any identity of the vehicle. But, the limitation of group formation and election of group leader posessed a constraint on such group based schemes in VANETs. Lin *et al.* [51] proposed a new scheme by combining the group signature and ID based signature to provide anonymous authentication in VANETs. The OBU of vehicle used the short group signature based on bilinear pairings to sign a message. RSUs adopt the identity based signatures where the public key used was the location information of RSU. A secure scheme SECSPP was given by Li *et al.* [116] which was an efficient authentication scheme adopting ID based cryptography and included hash functions and blind signatures.

Another ID-based security framework was proposed by Kamat *et al.* [117] where sign-

cryption scheme was used to achieve security paradigms of anonymity, data integrity, authentication, non-repudiation and confidentiality. However, the framework relied heavily on road side infrastructure for generation of pseudonyms and pseudonyms were generated after vehicle signed a single message which rendered high signaling overhead problem. A novel ID-based framework was propounded by Sun *et al.* [109] to achieve anonymity and non-repudiation. Privacy was achieved by the use of pseudonyms based approach and non-repudiation was achieved through threshold based distributed control where the driver's identity could not be revealed by single authority. It was assumed that the Tamper Proof Hardware (TPH) was used in the vehicles and the master key of trusted third party was never revealed. The use of signcryption [28] was also proposed in VANETs which has considerable advantage over encryption and signature methods as VANET nodes are not computational power restricted. However, in all these ID based proposals; the main obstacle was that the Key Generation Center (KGC) generated the secret key of vehicular entity by utilizing KGC's master key. It did not ensure non-repudiation as any message could be signed and decrypted by KGC abusing access proficiencies of vehicles leading to key escrow problem [118].

An authentication framework was proposed for VANETs by Lu *et al.* [62] which utilized Identity Based Signature along with Identity Based Online/Offline Signature (IBOOS). The signing process was separated into online and offline phase in IBOOS to increase the efficiency of pairing processes. The IBS itself possessed the key escrow problem which might disrupt the VANET services. To deal with the problem of key escrow, another solution was adduced by Choi *et al.* [119] in which Regional Transportation Authority (RTA) verified vehicle's ID and then issued signature value (Γ) to generate the vehicle's public and private key using RSA algorithm and were generated on-board of the vehicle. Nonetheless, anonymity issues were not addressed. This drawback was mitigated by Dikmak *et al.* [120] where max-

imum anonymity was provided by updating the pseudonyms periodically. However, RSA public/private key pair generation was independent of the update of pseudonyms and validity period of key pair was generally longer than the expiry time of pseudonyms. The hierarchical distribution of Certification Authorities (CAs) solved the problem of central point failure. Biswas *et al.* [66] used the current position information and timestamp as the identity string which could be employed as public key for corresponding vehicle for signature generation to prevent the wormhole [121] as well as replay attacks. This scheme used a variation of Elliptic Curve Digital Signature Algorithm (ECDSA) with identity-based signature. Bloom filters were used to prioritize the messages in high traffic areas. Park *et al.* [122] proposed a protocol to achieve authentication and to provide location assurance by avoiding illicit tracking of vehicle's location. The authentication between the RSU and vehicle was done by identity-based authenticated key agreement protocol [123], and the hierarchical identity-based signature [124] was used for generating and verifying the location-based signature. Another security framework was proposed by Bradai and Afifi [125] based on identity based cryptography to achieve anonymity, non-repudiation and securing the messages in a confronted accident scene. Chim *et al.* [126] introduced a new ID based framework where a vehicle used a different pseudonym for each message protecting its privacy and only trusted authority was able to reveal the true identity of the vehicle. The vehicles in the range of particular RSU form a group and the group members communicate securely by authenticating with each other. An adequate authentication scheme was proposed by Hui *et al.* [127] where private vehicles used group signature to sign the messages. The RSUs and public vehicles (ambulance, public bus *etc.*) used an identity-based signature to sign messages. In addition, the verification time was reduced by adopting the batch verification techniques. Nasreen *et al.* [128] employed a scheme where the authentication for vehicle to RSU was done by employing ID based signature and inter-vehicle authentication through ID based

Table 2.3: Comparison of proposed ID based frameworks

Security Schemes	Key Escrow Problem	Signalling Overhead	Privacy	pseudonyms	Non-Repudiation	RSU aided	Group Formation	Location ID
["Lin et al. 2007"][51]	✓	×	✓	×	×	✓	✓	✓
["Sun et al. 2007"][109]	✓	×	×	✓	✓	✓	×	×
["Chen et al. 2003"][115]	✓	✓	✓	×	✓	×	✓	×
["Kamat et al. 2006"][117]	✓	✓	✓	✓	✓	✓	×	×
["Lu et al. 2012"][62]	✓	×	✓	✓	×	✓	×	×
["Choi et al. 2009"][119]	×	×	×	×	✓	×	×	×
["Dikmak et al. 2012"][120]	×	×	✓	✓	✓	×	×	×
["Biswas et al. 2013"][66]	×	✓	✓	×	✓	×	×	✓
["Chim et al. 2011"][126]	×	✓	✓	✓	✓	✓	✓	×
["Hui et al. 2010"][127]	✓	×	✓	×	✓	✓	✓	×
["Huang et al. 2011"][131]	×	×	✓	✓	✓	✓	×	×

online/offline signatures. Chaudhuri *et al.* [129] presented a new identity based secure algorithm for VANETs which attained the properties of security and privacy with management of identities and pair of public/private key pair. Lee *et al.* [130] proposed on demand secure routing protocol which used ID based cryptosystem and at the same time authenticated all the intermediate nodes. The Boneh and Franklin's scheme was applied for additional security features. A new ID based privacy preservation scheme was employed by Huang *et al.* [131] where pseudonyms were used by vehicles in place of their real identities for communicating. An adequate mechanism for revocation was also provided in this scheme for identifying and revoking vehicles if needed. Table 2.3 gives briefly the comparison of the major ID based frameworks which have been proposed for vehicular networks.

Certificateless Cryptography Approaches

Certificateless cryptography alleviates the overhead of certificates as in PKI and also solves the problem of escrowing an identity in ID based cryptography. Mohanty *et al.* [132] proposed a certificateless aggregate signature protocol for vehicular networks which made RSU responsible for authentication, aggregation and verification of messages sent from vehicles. The RSU also notified the results back to the vehicles which were in the range of RSU and to

other neighboring roadside units. The batch verification scheme was employed to reduce the verification time of large number of signatures from neighboring vehicles and privacy was attained by the use of pseudonyms. Taha *et al.* [133] propounded a key agreement scheme, based on certificateless cryptography where mutual authentication between a mobile network node and a mobile router was achieved and a secure shared key was created between them. Hu *et al.* [134] presented a pairing based certificateless aggregate signature scheme for ad-hoc networks. Certificateless Online/Offline Signature (CLOOS) Scheme was presented by Sharmila *et al.* [135] which was a light weight cryptographic scheme having high security and low communication overhead. The scheme was much efficient for resource constrained and low power devices. A new certificateless private querying scheme was presented by Wan [136] to solve the anonymity problem in querying services in VANETs based on location by applying the technique of pseudo identity. After authenticating himself/herself to a nearby RSU, a driver can use the service.

A secure authentication scheme was adduced by Tseng *et al.* [137] using certificateless cryptography for emergency messages validation in VANETs. The conditional privacy was ensured where vehicles should be traceable by law enforcement authorities. The scheme used aggregation and batch verification techniques for emergency message verification and thus reduced the computation overhead. A novel certificate based signature scheme for V2I communication was proposed by Hu *et al.* [76] by combining the best aspects of identity based cryptography and the traditional public key cryptography. Therefore, the certificateless cryptography retained the identity based key management characteristics but with key escrow problem being solved. Table 2.4 gives the relative study of the proposed certificateless approaches.

Table 2.4: Comparison of certificateless approaches in VANETs

Security Schemes	Privacy	Traceability	Aggregate Verification	RSU aided	Pseudonyms	Dynamic
["Mohanty et al. 2012"][132]	✓	✓	✓	✓	✓	×
["Taha et al.2012"][133]	✓	×	×	✓	×	✓
["Wan 2013"][136]	✓	×	×	✓	×	✓
["Tseng et al. 2011"][137]	✓	✓	✓	×	×	×

2.3.2 Trust Management

All the security solutions proposed so far, focus primarily on assuring that the message is delivered to its neighbours securely and there has been less attention towards grading the information quality which is exchanged among the vehicles as the malicious nodes may send the bogus information to compromise the vehicular ad-hoc network. So, the control system should be designed such that the malicious and incorrect information should be reduced to mitigate its effect on the vehicular network. Therefore, the notion of trust among the neighbouring vehicles in VANETs is a crucial matter that needs consideration. The trust is assimilated among the different vehicle nodes so that the false information sent by the malicious vehicles can be detected. It gives motivation to these vehicle peers to discourage self-centered behaviour and behave honestly.

Modelling trustworthiness among vehicles possess various exceptional challenges. Firstly, the vehicles on highway are highly mobile and at such mobility, reaction time to such an inevitable solution need to be very minimal, leading to the urgent need for vehicles to trust incoming messages in real time. Secondly, the highly scalable nature of VANETs poses a constraint on trust management among peers as millions of vehicles may pass through particular point in the network leading to high overload in the network as the vehicles receive lots of information from the neighbouring vehicles. Hence there is need for an effective system to react in such hazardous situations. Another major challenge in modelling the trust in

VANETs is the decentralized nature of VANETs. The vehicle which is interacting with other vehicle may not communicate with it in the future which hampers from building the long term relationships in such highly dynamic networks.

Existing Trust Models for VANETs

A substantial amount of research has been done in vehicular ad-hoc networks where security issues have been given paramount consideration. Many trust and reputation systems have been proposed so far, to accurately deal with the routing and security considerations.

Gomez *et al.* [138] provided the trust and reputation based proposal for vehicular networks to distinguish the malicious self-centered vehicles from the trustworthy vehicles which can be used to make accurate decisions whether the traffic warning from the other vehicles should be accepted or not. An event-based reputation system was presented by Lo *et al.* [139] for disseminating decisive and accurate traffic information to drivers and the false alarm from bogus messages can be easily detected. However, the drawback of the approach is that it does not provide real time responses and the reputation of the originator of the message is not considered. Yang [140] proposed the new trust and reputation management framework based on similarity mining technique for VANETs to identify the similar messages or vehicles where various recommenders' similarities are used as weight to compute reputation of the vehicle. It uses the similarity computing algorithm presented in [141] based on Euclidean distance theory [142]. Ayman *et al.* [143] introduced the privacy consideration in addition to the reputation based trust in VANETs. Anonymous group communication was used to enhance privacy where group members are anonymous within the groups but are identifiable to the group managers. The task of calculating trust from the received messages is simplified by employing the group formation. Minhas *et al.* [144] adduced a trust framework where role, experience, priority and majority based trust of agents is calculated and algorithm is pro-

posed to integrate various dimensionality of trust. Intelligent agents are used to assist the vehicles by processing the messages from other nodes and broadcasting the processed information to the vehicles. The predictive algorithms for vehicular ad hoc networks were given by Bali *et al.* [145] which gives the estimation of clustering duration and the total number of vehicles in a particular cluster. Zhang *et al.* [146] proposed two privacy preserving authentication protocols where first scheme employing significantly reduction in verification time of signatures in VANETs with tight security proof and second scheme employing the batch verification of a bunch of messages. Malhi *et al.* [147] proposed a certificateless aggregate signature scheme for achieving authentication and privacy in vehicular ad hoc networks to significantly reduce the signature verification time by verifying the signatures in an aggregate manner and security proof was given in random oracle model. Alawi *et al.* [148] proposed a gateway selection scheme for multi-Hop relaying in an integrated network of vehicular ad hoc networks and Universal Mobile Telecommunication System (UMTS). The scheme extends the coverage range and increases the connectivity of the vehicles with UMTS. Wang *et al.* [149] proposed a solution for reducing the deployment cost of RSUs by increasing the distance between two RSUs and enabling the multi hop communication between any vehicle and RSU. As the multi hop relays increase, there is crucial need for reducing the multi hop delay, so the RSU rerouting scheme is proposed which adjusts the multihop communication till the selection of RSU with shortest path.

A fuzzy based trust management for web services was given by Nepal *et al.* [150] where consumer's perception about the web services was queried and represented accordingly but the effective way to calculate the perception of a new one was not discussed. Pouyan *et al.* [151] proposed the secure Ad hoc On Demand Distance Vector (AODV) routing protocol for mobile ad hoc networks using fuzzy Petri nets. The fuzzy inference engine used the four fuzzy variables for representation of behaviour of misbehaving nodes in mobile ad hoc

networks. The route verification was performed securely for the selection of most secure route among the nodes in the network. Gazdar *et al.* [152] proposed a trust based architecture for public key infrastructure in VANETs for calculating the trust of vehicles. The fuzzy based inference system was used to calculate the trust of the vehicles where the vehicles which were trusted and had atleast one trusted neighbour could be used as the contender for certification authority within its cluster whereas managing the cluster formation in such dynamic network is itself a major concern. However, the trust based scheme was only used for the management of certificates in public key infrastructure but not for selection of the relaying nodes for path selection. Further, the contender CA having the lowest relative mobility was selected as the CA. Thus, the vehicle can be selected as the Certification Authority (CA), Registration Authority (RA), *etc.* according to the trust metric calculated. The drawback of the scheme was that whole network may be compromised if the wrong CA or RA is selected. Thus, the CA, RA *etc.* should always be trusted authorities and these should never be assigned to the vehicles. Raya *et al.* [153] propounded a data oriented trust model where the received message legitimacy was evaluated. The report about an event was computed by each vehicle firstly and then the reports about the single event from all the vehicles are combined to calculate the actual probability of event. However, high mobility of vehicles always poses a constraint in deriving of prior probability of an event in real time. A beacon based trust management scheme was adduced by Chen *et al.* [154] to restrict the malicious insiders to send false messages in the network which not only uses the event messages but also beacon messages for the trust computation and verisimilitude of these two messages is crosschecked to determine the trustworthiness of the messages. Huang *et al.* [155] proposed a voting scheme where the voting weight was assigned to each vehicle according to its distance from the event i.e. the vehicle closer to the event acquire more weight, to overcome the problem of information cascading [156] and oversampling [157].

Khokhar *et al.* [158] proposed a fuzzy based social routing protocol which aims to adopt the social behaviour of humans on the road to build a secure optimal decisions from the prior knowledge of real time traffic information. The fuzzy based inference mechanism employed the friendship mechanism at the intersections to make accurate decisions. In this system, the prior knowledge of the real time traffic information was needed for building the social relationships. Jain *et al.* [159] proposed an enhanced fuzzy based spray and wait routing protocol to enhance the delivery ratio and to reduce overhead. It determined the message priority by aggregating the properties of message using fuzzy logic to denote its importance compared to other messages which are stored in the buffer of node to select the message intelligently. The application of fuzzy logic has also been used in designing multiple attribute decision making scheme [160] in which four attributes were used to characterize the vehicle and obtain the fuzzy score for each attribute according to which weights of the attribute were selected. Finally, fuzzy performance score for each vehicle was calculated for the selection of target for next hop transmission. The fuzzy based trust prediction model was also employed for wireless sensor networks [161] where the behaviour of the neighbours is predicted from their past behaviour, trust value fluctuations and the recommenders. Recommenders are the nodes having maximum interactions with the requesting node. The past behaviour of the node may directly influence the trust value fluctuations thus, leading to incorrect results. Therefore, the trust prediction should always be done on the real time data. A fuzzy chessboard clustering method and artificial bee colony routing method was proposed for wireless sensor networks [162] for overcoming the bottleneck problem and for routing in an energy efficient manner. The proposed method helps in balancing the consumption of energy in WSNs and maximize the lifetime of the network. A User authentication scheme based on biometrics was given by Althobaiti *et al.* [163] for wireless sensor networks. However the proposed scheme was prone to many attacks such as node capture attack, impersonation attack and man-in-the-

middle attack. These drawbacks were improved by Das [164] by employing a biometric authentication scheme using fuzzy extractor for extracting the key data from biometric of user by using the smart card. The formal security verification of the scheme was proposed to ensure that the scheme was secure.

The trust models can be classified into three types namely, entity oriented, data oriented and hybrid trust models where entity-oriented trust models target the trust relationships among VANET entities, data-oriented trust models target the evaluation of the trustworthiness of data among entities and hybrid trust models focus on both entity trust and data trust.

a) Entity-oriented trust models

Gerlach [165] adduced a sociological trust model which was based on an entity trust where architecture was designed to incorporate the trust and location privacy among the entities of the network. This model had distinct levels of trust which included situational trust, dispositional trust and system trust and formation of belief regarding data was based on the various trusts. Nevertheless, it was not explained that how different trusts should be combined. Minhas *et al.* [166] proposed a multi-faceted trust modelling system for VANETs which included the role based trust and experience trust to be used as the metric to evaluate trust of vehicle nodes. The vehicles could inquire other vehicles regarding any event that had occurred and also restrict the number of received reports. Another trust framework was presented by Ayman *et al.* [167] which preserved the privacy and allowed the formation of trust based on the reputation of network entity. The framework employed the group formation where VANET entities preserved the anonymity and only group managers were able to identify the group members. Therefore, groups simplify the task of building group reputation and trust calculation of received messages without compromising privacy. Another hardware based security framework was presented by Wagan *et al.* [168] based on asymmetric and symmet-

ric cryptography and formed trusted groups to build an enhanced trust relationships among vehicles in the group. A privacy-preserving system that guaranteed message trustworthiness in vehicle-to-vehicle (V2V) communications was proposed by Wu *et al.* [169] for trustworthiness of messages in inter-vehicle message exchanges. Both a priori and a posteriori countermeasures were adopted to thwart attackers. Until and unless the vehicle sign the same message twice, the vehicle privacy was preserved. The threshold-authentication scheme for V2V communications was proposed and the authentication of messages was expedited by batch verification technique.

b) Data-oriented trust models

Data-oriented trust models are used to evaluate the data trustworthiness coming from the neighbouring vehicles. A data centric trust model which was applicable for VANETs was defined by Raya *et al.* [170] where distinct metrics for trust were given of which a priori trust relationships was considered as one of the parameter for trust evaluation and trust was dependent on the various metrics associated correlated with the typical vehicle entity. The level of trust of entity depended on the various events associated with nodes i.e, if the event associated with data took place or not. This trust model had shortcomings that only transitory trust was formed upon data therefore, trust needed to be established again and again. A trust model was designed to detect and amend the incorrect data by Golle *et al.* [171] in VANETs which had all the information about the other entities in VANETs. When the data received by particular entity matched with the already contained information in model with high probability then the data was accepted by the vehicle. However, it was not achievable that each vehicle had all the information about the network and exclusively assessed the data validity. Further, it also lead to storage overhead problem in vehicle entities.

c) Hybrid trust models

Hybrid trust models combine the entity level trust and data centric trust. Chen *et al.* [172] propounded a trust based framework where trust relationships were maintained with the help of distinct trust metrics to evaluate the data received from the other vehicle entities. This scheme employed an identity based aggregation scheme for data aggregation and calculating trust notions. The groups were formed and group leaders were responsible for calculation of trust based on the trustworthiness of other entities' by combining the trust based on role and experience which was then used for computing majority opinion to detect malicious information sent from sender. Ultimately, the decision about the data trustworthiness for the entity was derived from the evaluation result. Hereby, the proposed hybrid model approved the vehicles for evaluation of the information by taking the other entities' believes into consideration. Another hybrid trust based message propagation model was designed by Zhang *et al.* [94] where the information collected from the neighbouring vehicles was propagated securely and efficiently and dynamic dissemination of information was controlled thus, elevating scalability of network. A reputation based hybrid trust model was proposed by Patwardhan *et al.* [173] where it was assumed that anchor nodes were already authenticated, and the data supplied by them was considered to be accurate. The model approved the data by either having an opinion with neighbouring vehicles or explicitly communicating with any of the anchor node. If the validation algorithm disapproved the data received from a particular entity then that entity was termed as malicious entity. The weakness of the current model was that reputation of the neighbours was not determined while calculating the data trustworthiness and hence, this model was only dependent on the broadcasted information from neighbouring entities.

Table 2.5: Properties of existing trust models

Security Schemes	Decentralized	Robustness	Authentication	Privacy	Security	Confidence	Scalability	Dynamics
["Gerlach 2007"][165]	×	×	✓	✓	✓	✓	×	✓
["Minhas et al. 2010"][166]	✓	×	✓	✓	✓	✓	✓	✓
["Wu et al. 2010"][169]	×	✓	✓	✓	✓	✓	×	✓
["Raya et al. 2008b"][170]	✓	×	×	×	✓	✓	×	✓
["Golle et al. 2004"][171]	✓	✓	✓	✓	✓	×	×	×
["Chen et al. 2010"][172]	✓	×	✓	×	✓	✓	✓	✓
["Patwardhan et al.2006"][173]	✓	×	✓	×	✓	×	×	✓
["Zhang et al. 2010"][174]	✓	×	×	×	✓	✓	✓	✓

Properties of existing trust models

The distinct properties are aspired by trust management models in VANETs which include privacy, system level security, authentication *etc*. The trust management in VANETs need to be decentralized to manage with immensely scalable, mobile and distributed quality of VANETs. Since the environment of neighbouring nodes is changing rapidly and consistently, hereby the trust models should capture this dynamism for managing trust among entities. Trust management should also be able to deal best with the scalable nature of VANETs. Confidence measure should be included in trust management to capture uncertainty. The confidence level should depend on the various metrics that were available to calculate trust value. The mechanism of trust management should be robust enough to deal with the distinct attacks which can be mounted on VANETs. Table 2.5 lists the comparative analysis of the properties of existing trust models.

2.4 Comparative Analysis

This section presents the systematic chronological order of all the security schemes which have been discussed in the previous sections. Table 2.6 gives the comparison of the different schemes chronologically based on the distinctive characteristics providing a comprehensive review of recently proposed security solutions.

Table 2.6: Comparison of security approaches for VANETs based on distinctive characteristics

Security mechanism employed	Proposed approaches by Author (year)	Technique used in security mechanism	Properties of VANETs achieved by the proposed security mechanism	Pseudonyms	Group formation	Infrastructure support for communication	Unique Functional Description
"Public Key Cryptography"	"Blum *et al.*"[77] (2004)	Digital signatures, Group communication	Authentication	-	Yes	-	The messages were reliably disseminated by the cluster heads after signing them.
"Public Key Cryptography"	"Hubaux *et al.*"[78] (2004)	Inter-vehicle communication	Authentication, Anonymity, Non-repudiation, Scalability	-	-	-	Electronic license plates were used as electronic identifiers for communication among vehicles.
"Public Key Cryptography"	"Huang *et al.*"[34] (2005)	Group signatures	Anonymity	Yes	Yes	Yes	The group leader only accessed the infrastructure on behalf of group members.
"Public Key Cryptography"	"Raya *et al.*"[83] (2006)	Group signatures	Authentication, Anonymity	-	Yes	-	The dissected area maps helped vehicle to locate group by comparing its location with it.
"Public Key Cryptography"	"Raya *et al.*"[85] (2006)	Anonymous preloaded certificates	Authentication, Anonymity, Traceability	Yes	-	Yes	Revocation difficult due to large certificate pool.
"Public Key Cryptography"	"Raya and Hubaux"[49] (2007)	Anonymous preloaded certificates	Authentication, Anonymity, Non-repudiation	Yes	-	-	Anonymous certificates were preloaded in the on-board of vehicle.
"Public Key Cryptography"	"Gerlach *et al.*"[79] (2007)	Logical viewpoints presented	Authentication, Privacy, Non-repudiation	Yes	-	Yes	Security concepts were defined for VANET by describing four viewpoints.

Table 2.6: Comparison of security approaches for VANETs based on distinctive characteristics

Security mechanism employed	Proposed approaches by Author (year)	Technique used in security mechanism	Properties of VANETs achieved by the proposed security mechanism	Pseudonyms	Group formation	Infrastructure support for communication	Unique Functional Description
"Public Key Cryptography"	"Lin *et al.*"[51] (2007)	Group signatures	Authentication, Anonymity, Non-repudiation	-	Yes	-	Verification was only possible when second message was received, revocation difficult as OBU needed to store all certificates.
"Symmetric Key Cryptography"	"Choi *et al.*"[102] (2005)	Symmetric communication	Authentication, Anonymity, Non-repudiation	-	-	Yes	The peer vehicles needed to authenticate each other via a base station.
"Symmetric Key Cryptography"	"Freudiger *et al.*"[103] (2007)	Combination of symmetric and asymmetric	Anonymity, Scalability Traceability	-	-	Yes	Mix zones were created at intersections where vehicles used symmetric keys with RSU's to exchange messages.
"Symmetric Key Cryptography"	"Plob *et al.*" [12] (2008)	Asymmetric and symmetric communication	Authentication, Anonymity, Non-repudiation	-	-	-	Vehicles needed to contact Trusted third part each time to verify each message
"Symmetric Key Cryptography"	"Burmester *et al.*"[101] (2008)	Hybrid system	Authentication, Anonymity	-	-	-	Symmetric keys were used for pair-wise communication and public keys for group communication.
"Symmetric Key Cryptography"	"Chim *et al.*"[104] (2012)	HMAC and public key infrastructure	Authentication, Anonymity, Non-repudiation, Scalability	Yes	-	Yes	HMAC based authentication for regular messages and PKI for urgent messages.
"Symmetric Key Cryptography"	"Hu *et al.*"[105] (2012)	HMAC and symmetric encryption	Authentication, Anonymity, Non-repudiation	Yes	Yes	Yes	Symmetric encryption was used to establish a secure communication among group members in a group.

Table 2.6: Comparison of security approaches for VANETs based on distinctive characteristics

Security mechanism employed	Proposed approaches by Author (year)	Technique used in security mechanism	Properties of VANETs achieved by the proposed security mechanism	Pseudonyms	Group formation	Infrastructure support for communication	Unique Functional Description
"Identity Based Cryptography"	"Chen *et al.*"[115] (2003)	Identity Based group signatures	Authentication, Anonymity, Traceability	-	Yes	-	The vehicles register themselves to GRM and any message could be signed by them on group's behalf.
"Identity Based Cryptography"	"Kamat *et al.*"[117] (2006)	Signcryption scheme	Authentication, Anonymity, Confidentiality, Non-repudiation	Yes	-	Yes	Availability of infrastructure for pseudonym generation but it lead to signaling overhead problem.
"Identity Based Cryptography"	"Sun *et al.*"[109] (2007)	ID based digital signatures scheme	Authentication, Anonymity, Non-repudiation, Scalability	Yes	-	Yes	Pseudonymous based approach through the use of threshold based secret sharing scheme to achieve non-repudiation.
"Identity Based Cryptography"	"Lin *et al.*"[51] (2007)	ID based signature and group signature	Authentication, Anonymity	-	Yes	Yes	Vehicles used group signature to sign messages and RSUs use location information as public key.
"Identity Based Cryptography"	"Choi *et al.*"[119] (2009)	ID based cryptosystem with self generated RSA public keys	Authentication, Anonymity, Non-repudiation	-	-	-	RTA verified the vehicle ID and generated signature value which was then used to generate signatures.
"Identity Based Cryptography"	"Hui *et al.*"[127] (2010)	Identity based signature and group signature	Authentication, Anonymity, Non-repudiation	-	Yes	Yes	Identity based signature for public vehicles or RSUs and group signature for private vehicles.
"Identity Based Cryptography"	"Huang *et al.*"[131] (2011)	Identity based signature	Authentication, Anonymity, Non-repudiation	Yes	-	Yes	Psuedo identities were used and an adequate mechanism for revocation was provided in this scheme.

Table 2.6: Comparison of security approaches for VANETs based on distinctive characteristics

Security mechanism employed	Proposed approaches by Author (year)	Technique used in security mechanism	Properties of VANETs achieved by the proposed security mechanism	Pseudonyms	Group formation	Infrastructure support for communication	Unique Functional Description
"Identity Based Cryptography"	"Lu *et al.*"[62] (2012)	ID based online/offline signature	Authentication, Anonymity	Yes	-	Yes	ID based signature was used for authentication between RSU and vehicles. Identity based online/offline signatures for authentication among vehicles.
"Identity Based Cryptography"	"Dikmak *et al.*"[120] (2012)	ID based cryptosystem with RSA keys	Authentication, Anonymity, Traceability	Yes	-	-	RSA public/private key pair was independent of pseudonym update.
"Identity Based Cryptography"	"Biswas *et al.*"[66] (2013)	Elliptic curve digital signature algorithm	Authentication, Anonymity, Non-repudiation	-	-	-	Current position information and timestamp of vehicle were used as ID and bloom filters were used to prioritize the messages.
"Certificateless Cryptography"	"Tseng *et al.*"[137] (2011)	Certificateless authentication scheme	Authentication, Anonymity, Non-repudiation, Scalability	-	-	-	The scheme used aggregation and batch verification schemes for emergency message verification.
"Certificateless Cryptography"	"Mohanty *et al.*"[132] (2012)	Certificateless aggregate signature scheme	Authentication, Anonymity, Traceability, Scalability	Yes	-	-	The user generated the public key by using public parameters of KGC and secret key.
"Certificateless Cryptography"	"Taha *et al.*"[133] (2012)	Certificateless signature scheme	Authentication, Anonymity	-	-	Yes	The scheme achieved mutual authentication between mobile node and mobile router.

Table 2.6: Comparison of security approaches for VANETs based on distinctive characteristics

Security mechanism employed	Proposed approaches by Author (year)	Technique used in security mechanism	Properties of VANETs achieved by the proposed security mechanism	Pseudonyms	Group formation	Infrastructure support for communication	Unique Functional Description
"Certificateless Cryptography"	"Wan"[136] (2013)	Certificateless based private querying scheme	Anonymity	-	-	Yes	The scheme applied pseudo identity and after authenticating to a nearby RSU, driver could use location based services.
"Entity Based Trust Model"	"Gerlach"[165] (2007)	Sociological trust model	Authentication, Anonymity, Confidence	-	-	-	It presented sociological trust model which was based on an entity trust where architecture was designed to incorporate the trust and location privacy among the entities of the network.
"Entity Based Trust Model"	"Minhas *et al.*"[166] (2010)	Multi-faced trust model	Authentication, Anonymity, Confidence, Scalability	-	-	-	The calculation of trust based on the trustworthiness of other entities' by combining trust based on role and experience which was utilized to detect malicious information.
"Entity Based Trust Model"	"Wu *et al.*"[169] (2010)	Threshold authentication scheme	Authentication, Anonymity, Confidence	-	-	-	A framework designed to preserve privacy for trustworthiness of messages in inter-vehicle message exchanges. Attackers were thwarted by adapting both a priori and a posteriori countermeasures.
"Data Based Trust Model"	"Golle *et al.*"[171] (2004)	Probability based trust	Authentication, Anonymity, Decentralized	-	-	-	This model had all the information about the other entities in VANETs. When the data received by entity was accepted if it matched the model with high probability.

Table 2.6: Comparison of security approaches for VANETs based on distinctive characteristics

Security mechanism employed	Proposed approaches by Author (year)	Technique used in security mechanism	Properties of VANETs achieved by the proposed security mechanism	Pseudonyms	Group formation	Infrastructure support for communication	Unique Functional Description
"Data Based Trust Model"	"Raya *et al.*"[170] (2008)	Data oriented trust	Confidence, Decentralized	-	-	-	The level of trust of entity depended on the various events associated with nodes. The shortcoming being that only transitory trust was formed and no trust relationships were built.
"Hybrid Trust Model"	"Patwardhan *et al.*"[173] (2006)	Reputation based trust model	Authentication, Decentralized	-	-	-	The model approved the data by either having an opinion with neighbours or communicating with any of the anchor node where anchor nodes were already authenticated.
"Hybrid Trust Model"	"Chen *et al.*"[172] (2010)	Identity based aggregation scheme	Authentication, Confidence, Decentralized, Scalability	-	Yes	-	In this model, the trust relationships were maintained with the help of distinct trust metrics to evaluate the data and employed an identity based aggregation scheme.
"Hybrid Trust Model"	"Zhang *et al.*"[94] (2010)	Trust based message propagation scheme	Confidence, Decentralized, Scalability	-	-	-	The information collected from the neighbours was propagated securely and efficiently in this hybrid trust model.

2.5 Attacks in VANETs

VANETs are exposed to various attacks which hampers the communication process in this network. The various mechanisms have been proposed to detect and mitigate the different attacks in VANETs.

Sybil attacks can be detected using the method of resource scheduling [175] under an assumption that all the physical resources are limited and the computational puzzles are used to test the computation power of each node. This technique was not feasible for VANETs as the vehicles in this network can have more computational resources so, radio resource testing technique [176] was proposed for VANETs. Yan *et al.* [177] proposed a radar based solution to sybil attacks in VANETS where radar detected the actual physical existence of a vehicle that could be used to validate the abstract information about the vehicle. Another approach was proposed for VANETs by Yu *et al.* [178] where position evidence system was designed to improve the detection accuracy by employing the statistical methods and was able to identify the direction of the vehicle. A distributed data fusion method [179] had also been proposed to detect sybil attacks where distributed confidence over the vehicular ad hoc network was built. The signal strength distribution [180] of a suspected node was observed over a period of time to detect the sybil attacks in VANETs and verification error rate was significantly reduced by using the statistical methods. A timestamp series approach [181] was another approach to secure VANETs from sybil attacks with infrastructure support. The digital certificates were issued by the road side infrastructure and thus, it was impossible for two vehicles to pass by multiple RSUs at the same time. Thus, the two messages issued under the same timestamp series under RSUs were considered as sybil attacks by the vehicle. RobSAD approach [182] with limited infrastructure support was proposed where the difference between normal and abnormal motion trajectories of vehicle was used to detect sybil attacks and each node was able to detect attacks individually without the support from

infrastructure. The success rate of sybil attacks in VANETs was calculated based on the assumptions of transmission power or antenna [183] where the number of cheated nodes were calculated from the sender's as well as receiver's point of view. A sybil detection approach in VANETs based on signal strength variations [184] used the node to verify authenticity of other nodes according to their localizations and a metric was used to define the degree to distinguish between two nodes. A lightweight and scalable P^2DAP mechanism [185] was used to detect sybil attacks in distributed manner in VANETs where set of fixed nodes called Road Side Boxes undergo passive overhearing of the network to detect the malicious vehicles.

Another model known as plausibility validation network was proposed by Lo *et al.* [186] to secure the network against illusion attack. It worked by taking two types of inputs: data from antennas and data collected by sensors. The data checking module validated the input data and took the necessary actions as required. Thus, the rule set was needed to be stored for each and every message which might lead to storage overhead in vehicles. Therefore, an efficient mechanism called Message Content Validation Algorithm[187] was proposed where possibilities of an illusion attacker were explored in all dimensions and security goals were designed accordingly. An approach known as Packet leash [188] was proposed to prevent the wormhole attacks in wireless ad hoc networks where temporal leashes ensure that each packet had an upper bound on its lifetime restricting the maximum travel distance and geographical leashes ensured that a packet could only be received within a certain distance from sender. All the nodes were tightly synchronized by clock and a leash based protocol TIK implemented these leashes. Further an improved approach, HEAP [189] was proposed having more security and less overhead. HEAP was an improvement of the previously proposed packet leash scheme to detect wormhole attacks in AODV routing protocol in VANETs. HEAP used the geographic leashes with loosely synchronized clocks and the packets were dropped when the claimed passing distance by the packet was not correct thus solving the

problem of limitation on packet travel. Another approach known as DEIPHI [190] was given for wormhole detection in wireless ad hoc networks where the sender was able to detect the wormhole attacks by observing the delays of different paths to the receiver. This method incurred less cost as it did not require the synchronized clocks and on board units need to be equipped with some special hardware. A trust based approach [191] against sinkhole attack was proposed to detect sinkhole in AODV based vehicular ad hoc network where the route was decided by the node after it got the route reply messages from all its neighboring nodes which was based on the type of association between the nodes. Thus, sinkhole nodes were detected and were not given preference in route selection.

A mechanism to mitigate the effects of DoS attacks [192] was proposed where each vehicle kept track of the invalid signatures received in particular time period based on which invalid signature ratio was calculated. When the invalid signature ratio reached a threshold, it indicated DoS attacks warning. Another approach was given for minimizing DoS attacks in VANETs where the data packets received by a node passed through a number of tests and if any of these test failed, the node dropped that data packet [193]. These constraints also helped to identify if the node's claimed position as a nearest node was true or not. The synchronization based DDoS attacks in VANETs were mitigated by randomizing the RSU schedule during each cycle of periodic transmission and minimizing the contention window size which reduced the back-off delay [194]. To reduce the position based attacks in VANETs, set of plausibility checks [195] were proposed which did not require extra special hardware and were able to mitigate the effects of position based attacks. The proposed mechanism was able to adapt to different road conditions and traffic conditions. The IBV scheme [56] was unable to fulfill the privacy requirement and suffered from the impersonation attack. The mechanism known as SPECS [126] was designed to ensure privacy in vehicular ad hoc networks and to detect impersonation attacks.

2.6 Intrusion Detection in VANETs

The masquerade, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are some serious and severe attacks on the availability of the network in vehicular communications. The network availability in VANETs is very important as all the entities; vehicles, road side units rely on the network for the communication. In DoS attacks, the attacker jams the communication channel of the network and the network is no longer available to the legitimate vehicles. Therefore, the main intention of the attacker is to prevent the network users from accessing the network services [49][88]. DDoS attacks are more severe than DOS attacks as these attacks are launched by attackers in distributed manner as the attackers launch the attack from the different locations and different time slots. The major aim of the attacker is to achieve network inaccessibility by the vehicles on a large scale of the network.

The study of such attacks on vehicular ad-hoc networks is an important open axis of research. Many security frameworks have been proposed so far for vehicular ad-hoc networks but very few works have studied these attacks on VANET scenarios and proposed the efficient solution for such attacks. The comprehensive survey of the various taxonomies and vulnerabilities of various attacks were discussed in detail by Igure and Williams[196]. Yu *et al.* [178] proposed a mechanism for detecting sybil attacks in VANETs where cooperative method was employed for detecting the positions of sybil nodes and a statistical method was designed to verify the direction of incoming vehicle and the whole system was termed as Presence Evidence Systems (PES). The sybil nodes may launch the DoS attacks to disrupt the normal functioning of the network. The distinct intrusion detection mechanisms for VANETs have been proposed to detect the intruders in the network which may launch disparate attacks in VANETs. Tomandl *et al.* [197] proposed a new intrusion detection mechanism known as REST-Net which employs a dynamic detection engine to monitor the data transmitted in the network for the detection of fake messages as these fake messages may

launch various types of attacks. The attacker was being identified from the fake messages and the fake messages were being revoked. The scheme offered high detection rates and warning signals to prevent the interruptions. Sedjelmaci and Senouci [198] adduced a new intrusion detection framework for vehicular networks where the vehicles reputation scheme was used to evaluate the trust level of the vehicle. The proposed scheme offered efficiency in terms of fast attacks' identification, high detection rate and low false positive rate. Coussement *et al.* [199] presented a decision making protocol where intrusion detection systems were installed in vehicles as well as RSUs and the groups of vehicles were formed according to their speed. The probabilistic model was formed which was based on the ratio computation between network entities which have answered to the signatures of the attack and then, the neighbours were alerted for the same. The intrusion detection system was proposed for wireless mesh networks by Deb *et al.* [200] where cluster based reward-oriented intrusion detection system was proposed and whose efficiency was evaluated using QualNet simulator. Mitchell [201] provided a survey of the intrusion detection techniques in all the wireless network applications.

Bibmeyer *et al.* [202] propounded a new signature based intrusion detection approach in VANETs which employs the plausibility model to verify the vehicle movement data. This approach was very convenient as a single fake vehicle can also be identified with this mechanism. A collaborative trust aware mechanism was employed for the detection of intruders by Kumar *et al.* [203] where learning automata was used to capture the different state's information of the vehicles and a markov chain model was used for the representation of states. Finally, a collaborative trust index was calculated to detect the attacks and abnormalities in the network. Ruj *et al.* [204] proposed a data centric misbehaviour detection mechanism where misbehaviour was detected from the false alert messages and the actions of misbehaving nodes are observed after dissemination of false alert messages. Therefore, each node

can detect if the information received was correct or not and fines were imposed on the misbehaving nodes. Misra *et al.* [205] proposed a learning automata based intrusion detection solution for VANETs considering the privacy concerns of each vehicle. The mechanism presented could detect 90-95% of the malicious packets in the network thus, giving the effective approach for misbehaviour detection.

A new bloom filter based DoS attack detection scheme in VANETs was proposed by Verma *et al.* [206] where IP addresses of the vehicles were verified and the duplicacy of the IP addresses in the database of the vehicle leads to the detection of DoS attacks. Thus, the fake identities of malicious network entities were examined consistently by the IP address information of the nodes. A model for the prevention of DoS attacks in VANETs was developed called the IP CHOCK which was able to locate the malicious nodes. Then, Verma and Halabi [207] proposed a scheme where Internet Protocol (IP) spoofing addresses of DoS attacks were defended by bloom filter based IP-CHOCK detection scheme. The IP spoofing addresses were obstructed the data transfer between two network entities. The IP addresses spoofing by malicious vehicles were also detected by using the proposed mechanism. Wasef *et al.* [192] proposed a defense mechanism to mitigate the DoS attacks in VANETs with the help of Public Key Infrastructure (PKI). Each vehicle kept the track of the invalid signatures received and calculated the invalid signature ratio and set the predefined threshold for invalid signature ratio. If the vehicle crossed the invalid signature ratio, then HMAC was appended on each outgoing signed message by the vehicle. Upon receiving the HMAC, if there exists the match of HMAC, it continued to verify the signature. The new security scheme was proposed for preventing the DDoS attacks caused due to route request flooding in AODV routing protocol in Mobile Ad-Hoc Networks (MANETs) by Sanyal *et al.* [208]. The solution was proposed against forwarding the fake route requests which leading to exhausting of the network resources which leads to distributed DoS attacks. Biswas *et al.* [194] analyzed

the synchronization based DDoS attacks on VANETs mathematically and through simulations and proposed the various mitigation techniques such as modification of MAC layer's contention window size and randomizing the message inter-arrival time during broadcasting to circumvent such attacks in VANETs. Neither sender nor receiver of the broadcast periodic beacons were aware of the attacks as such broadcasts do not have any acknowledgements.

2.7 Misbehaviour Detection in VANETs

VANETs are more prone to inside attacks as insiders have full access on the network and can act maliciously in the vehicular communications. Harit *et al.* [209] proposed a misbehaviour detection scheme where data collected from the neighboring vehicles regarding the event and the neighbour's responses were collected by vehicle to calculate the truth value of the event alert. Bibmeyer *et al.* [210] categorized the internal attackers so that the most relevant attacker was identified and feasibility of location based attacks was demonstrated. Dietzel *et al.* [211] proposed three graph based metrics for the detection of insider attackers in three different dissemination protocols. Another proposal was given by Zhang *et al.* [212] where the spurious messages were filtered using incremental learning part of back propagation neural network using vehicles' reputation. A framework for detection of malicious behaviour was proposed by Jaeger *et al.* [213] where Kalman Filter [214] was used to detect such misbehavior based on vehicles' past activities. Hussain *et al.* [215] proposed both event driven as well as data driven approaches for the misbehavior prevention on the basis of traffic. Sybil attack detection scheme was proposed in case of dense traffic region whereas location-based misbehaviour detection scheme was proposed for less dense regions. The misbehaviour detection scheme for message correction which was based on the analysis of mobility patterns of the vehicles nearby to the concerned vehicle was given by Razzaque *et*

al. [216]. Another scheme was presented by Yang *et al.* [140] which used state automata and supervision for detection of any fraudulent messages and the behavioural characteristics of the target vehicles were stored in the special security log maintained by the system. The end to end delay in mobile ad hoc networks was studied by Kumar *et al.* [217] to provide the quality of service support in terms of delay and bandwidth for transmitting the video or voice in delay intolerant applications.

2.8 E-Health Systems

Recently, a variety of wireless healthcare solutions are being proposed for vehicular network applications for safety improvement, such as seeded cloud [218] and V-Cloud [219]. The proposed solutions focus mainly on long tenure monitoring of health for vehicular users or are considering the real time emergency events in vehicular traffic to avoid any mishappening on the road [220]. The work has been done in patient monitoring which includes mobile telemedicine [221] [222] [223] [224], home monitoring [225], Bluetooth-based system for digitized ECGs [226], ECG based cardiac diseases [227], wireless telemetry system for EEG epilepsy [228], a hospital-wide mobile monitoring system [229], and real-time home monitoring of patients [230]. Sensors used for getting the vital signs of the patient include wireless sensors for health-monitoring [231] [232], ring-based sensor [233], clothing-embedded transducers for ECG [234] and stress monitoring sensors [235]. Moreover, the several ways for improving the medical decision making are included in [236] [237] [238].

The basic design principles and the authentication processes for the remote patient monitoring were described in [239]. Another remote patient monitoring system was designed by Niyato *et al.* [240] and Hu *et al.* [241] where patient data was collected by sensors to transmit it to the healthcare centres periodically. Lin *et al.* [242] proposed a privacy preserv-

ing mechanism for E-health services against the global adversary in the network to address the patient privacy issues by achieving both content oriented privacy and contextual privacy. A privacy preserving framework for mobile healthcare emergency was provided by Lu *et al.* [243] where the resource utilization of smart phones was done to process the personal health information of the patients efficiently during healthcare emergency. Masi *et al.* [244] provided an effective communication protocol to exchange the mobile patient information among the disconnected health centres and clinics where network connection was not available such as in rural areas. The opportunities and challenges for ubiquitous computing were discussed by Sneha *et al.* [245] who proposed a framework for patient monitoring by utilizing mobile ad hoc networks [246] to ensure the end to end connectivity. Doorenbos *et al.* [247] provided an initiative by enhancing healthcare systems of rural areas by giving them professional healthcare education. Another healthcare scheme called Rcare [248] was proposed which utilized the vehicular ad hoc networks for collecting and transmitting the patient specific information from rural areas for providing connectivity to these areas. All the proposed works utilize the wireless technologies for the timely and efficient transmission of the patient specific health information of the mobile patients to the health providers.

2.9 Problem Formulation

After doing the exhaustive survey on the VANETs, it has been realized that VANETs are the promising field of research for the future networks and definitely will be a major step forward towards the intelligent transportation systems. One of the focus which will ensure successful deployment of these networks initially is security. Protection of VANETs from attacks and important issues which need special consideration are authentication of messages. The trade off between the security and privacy is another important issue which needs thorough

consideration. Vehicles can be associated with locations, i.e. places a driver visits and the locations of the driver or the identities of the vehicle need to be preserved. At the same time, the messages need to be authenticated for the valid vehicle node such that the messages are not tampered by the adversaries.

Tamper proof hardware needs to be installed in vehicle nodes to mitigate the effect of mischievous insiders and to preserve the security keys and the various other security parameters. Further, secure VANETs need to have security mechanisms by incorporating the trusted authorities and secure keys, without any delay in computation and message authentication as it may affect the critical real time VANET applications. It has been observed that most of the prior work focused only on measuring security properties, largely ignoring the performance impact of the security mechanisms introduced into the system.The non-repudiation is the utmost requirement for maintaining security in VANETs.

Although identity based cryptography has been discussed significantly by researchers as one of the solutions for VANETs, its major limitation is that it suffers from the problem of key escrow problem which needs to be dealt in the vehicular communication process. Further, the signatures need to be verified aggregately before the next periodic beacons arrive so that the message drop reduces in the network. Therefore the signature verification strategies need to be improved to enhance the vehicular communication process in the network. Such schemes can be considered for providing a complete security framework, enabling majority of security requirements such as data integrity, consistency and availability.

2.10 Objectives

Main objectives of this work are:

(i) To study, analyze and explore the already existing security frameworks in VANETs

and identify important security issues which have not been addressed.

(ii) To propose and implement an ID based security framework for VANETs.

(iii) To test and validate the proposed framework on a simulated environment using various security testing parameters.

Chapter 3

Certificateless Aggregate Signature Scheme

The state-of-the-art telecommunication technologies have widely been adapted for sensing and collecting the traffic related information and Vehicular Ad-Hoc Networks (VANETs), the future of the Intelligent Transportation Systems (ITS) aim to improve traffic safety. Inter-vehicular communication needs to be secure and anonymous as the effective and robust operations including security and privacy are critical for the deployment of vehicular ad-hoc networks. The received message in vehicular ad-hoc networks can contain the malicious content that may affect the entire network. The digital signature scheme is used to validate the authenticity of the sender so that the message received may be trusted.

Certificateless-PKC is considered to be well suited for VANETs in perspective of limited bandwidth and the dynamic nature of such networks. The certificateless signature scheme presented by [27] can not be used in VANETs as it employs more computational cost in signature generation and verification processes and the high mobility of vehicles in the networks puts an urgent need to reduce the computational time as much as possible to support the reliable message delivery in the highly dynamic vehicular ad-hoc networks. Thus, a for-

mal security model of CLS schemes is given and a new certificateless aggregate signature scheme for vehicular ad-hoc networks is adduced which provides the security requirements of integrity, authenticity, privacy and non-repudiation. The authenticity and integrity are provided itself by the digital signatures. Privacy is achieved by the issuance of short term identifiers called pseudonyms by the road side infrastructures which prevents the tracking of vehicles but at the same time, provides the non-repudiation so that the authorities can not link the pseudonyms with the actual identity of the entity. Aggregate signatures have the advantage of verifying all the signatures together leading to reduction in computation time. Assuming the hardness of computational diffie-hellman problem over groups in bilinear maps, the CLAS scheme is proven secure in random oracle model [249].

3.1 Adversarial Model of Certificateless Signature Schemes

This section reviews the adversarial model [238] of certificateless signature scheme. Two types of adversaries are considered in certificateless cryptography namely, Type I and Type II adversary. Let $\mathscr{A}_1$ denote a Type I attacker and $\mathscr{A}_2$ denote a Type II attacker. Two games are considered, 'Game I' where challenger $\mathscr{C}$ interacts with adversary $\mathscr{A}_1$ and 'Game II' where $\mathscr{C}$ interacts with adversary $\mathscr{A}_2$. The master key of KGC cannot be accessed by adversary $\mathscr{A}_1$, but the public key of any entity can be replaced by $\mathscr{A}_1$ with the value chosen by it whereas the master key of KGC can be accessed by the adversary $\mathscr{A}_2$ but $\mathscr{A}_2$ cannot perform public key replacement. The certificateless signature scheme is existentially unforgeable against the adaptive chosen message attack, if the both adversaries $\mathscr{A}_1$ and $\mathscr{A}_2$ have negligible success probability. The six oracles which can be accessed by the adversaries are RevealPartialKey, RevealSecretKey, RevealPublicKey, RevealPseudonym, ReplacePublicKey and Sign oracles.

Game I (for $\mathscr{A}_1$ adversary):

In this game, adversary $\mathscr{A}_1$ interacts with the challenger $\mathscr{C}$.

Phase I-1:

The Setup algorithm is run by challenger $\mathscr{C}$, which takes the input security parameter ℓ to generate the *master key* and system parameter list *params*. The parameter list *params* is sent by challenger $\mathscr{C}$ to the adversary $\mathscr{A}_1$ while keeps the *master key* as secret to itself.

Phase I-2:

The polynomially bounded number of oracle-query operations are performed by the adversary $\mathscr{A}_1$. The adversary $\mathscr{A}_1$ can make *RevealPartialKey*, *RevealSecretKey*, *RevealPublicKey*, *RevealPseudonym*, *ReplacePublicKey* and *Sign* queries onto oracle during this stage of simulation.

Phase I-3:

Finally, $\mathscr{A}_1$ outputs a message and signature pair $< m_i^*, \sigma_i^* >$ corresponding to the identity ID_i^* with a public key P_i^*.

$\mathscr{A}_1$ wins Game I if;

- σ_i^* is a valid signature on message m_i^* with identity ID_i^* and pubic key P_i^*.
- The identity ID_i^* has not queried partial private key pp_i^* during *RevealPartialKey* queries. Moreover, oracle *Sign* has never been queried with ID_i^* and m_i^*.

Game II (for $\mathscr{A}_2$ adversary):

In this game, adversary $\mathscr{A}_2$ interacts with the challenger $\mathscr{C}$.

Phase II-1:

The Setup algorithm is run by challenger $\mathscr{C}$, which takes the input security parameter ℓ for the generation of the *master key* and system parameter list *params*. The parameter list *params* and the *master key* both are sent by challenger $\mathscr{C}$ to the adversary $\mathscr{A}_2$.

Phase II-2:

The polynomially bounded number of oracle-query operations are performed by the adversary $\mathscr{A}_2$. The adversary $\mathscr{A}_2$ can make *RevealSecretKey*, *RevealPublicKey*, *RevealPseudonym* and *Sign* queries onto oracle during this stage of simulation. The oracle *RevealPartialKey* is no longer needed by $\mathscr{A}_2$ as $\mathscr{A}_2$ has the access to the master key.

Phase II-3:

Finally, $\mathscr{A}_2$ outputs a message and signature pair $< m_i^*, \sigma_i^* >$ corresponding to the identity ID_i^* with a public key P_i^*.

$\mathscr{A}_2$ wins Game II if;

- σ_i^* is a valid signature on message m_i^* with identity ID_i^* and public key P_i^*.
- The identity ID_i^* has not queried secret key x_i^* during *RevealSecretKey* queries. Moreover, oracle *Sign* has never been queried with ID_i^* and m_i^*.

Definition 1: A Certificateless Signature scheme is existentially unforgeable under adaptively chosen message attack if the success probability $succ_{\mathscr{A}}(\ell)$ of any Probabilistic Polynomial Time (PPT) adversary $\mathscr{A}$ in any of the above two games is negligible.

3.2 Certificateless Signature Scheme for VANETs

Here, an efficient certificateless signature scheme based on bilinear pairings is proposed which comprises the seven algorithms. The proposed certificateless signature scheme's security depends on the hardness of the Computational Diffie-Hellman (CDH) problem in the group.

Setup

There is one Key Generation Center (KGC) located in the region under one Regional Transportation Authority (RTA). The input is a security parameter 1^{ℓ} where $\ell \in$ N, firstly a cyclic additive group $\mathbb{G}_1$ of prime order q is chosen by KGC. And finally, the cyclic multiplicative group $\mathbb{G}_2$ of the same prime order q is chosen. The bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$ is defined by it. Choose a generator point of the group $\mathbb{G}_1$ as P $\in \mathbb{G}_1$. A master key s $\in {}_R\mathbb{Z}_q^*$ is uniformally selected and the public key of KGC as P_{pub} = s.P is selected. The two distinct hash functions H_2: $\{0,1\}^* \longrightarrow \mathbb{Z}_q^*$ and H_3: $\{0,1\}^* \longrightarrow \mathbb{Z}_q^*$ are chosen. The message space is defined as $\mathscr{M} = \{0,1\}^*$. Each RSU in the region under RTA sets $y_i \in \mathbb{Z}_q^*$ as the secret key of RSU_i and $P_{rsu_i} = y_i.P$ as the public key of RSU_i. The public keys of all the RSUs $P_{rsu_1}, P_{rsu_2}, P_{rsu_3}.....P_{rsu_n}$ under the region of RTA are sent to the KGC and published under *params* list. The system parameter list is defined as *params* = $\{\mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_2, H_3, P_{rsu_1}, P_{rsu_2}, P_{rsu_3}.....P_{rsu_n}\}$.

Registration

This algorithm is run by RTA to register the vehicle with Identity ID_i. RTA maps the relationship between ID_i and Q_{ID_i} as the actual identity of the vehicle ID_i is concealed and Q_{ID_i} is only used as the identity by the vehicle for all the communications. Whenever the law

enforcement authorities want to trace the vehicle for liability issues, then RTA can reveal the actual identity of the vehicle. When the vehicle enters the region of another RTA, then the vehicle again registers its ID_i to get the new pseudo identity.

- Choose the distinct hash function $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$.
- The vehicle's identity space is $ID_i \in \{0,1\}^*$. The vehicle with identity ID_i registers itself with RTA as $Q_{ID_i} = H_1(ID_i) \in \mathbb{G}_1$.
- The RTA sends the Q_{ID_i} to the vehicle.

PartialKeyGen

In the region under single RTA, there is single KGC and partial private key is generated once for each vehicle under the region of one RTA. All the RSUs in the region are directly under the control of RTA of that region. It is assumed that the KGC and RTA do not collude as both of these are different authorities and RTA does not have any authority over KGC. It implies that the KGC and RSUs do not collude with each other.

- KGC runs this algorithm, and takes the inputs parameter list *params*, master key s and $Q_{ID_i} \in \mathbb{G}_1$.
- KGC then generates the partial private key of the vehicle as $pp_i = s.Q_{ID_i}$ by using the identity Q_{ID_i}.

The partial private key pp_i of vehicle is a signature on Q_{ID_i} with the public/private key pair (P_{pub}, s) and the correctness of the signature is checked by vehicle by checking whether $e(pp_i, P)$ = $e(Q_{ID_i}, P_{pub})$ which can be verified as

$$e(pp_i, P) = e(s.Q_{ID_i}, P) = e(Q_{ID_i}, s.P) = e(Q_{ID_i}, P_{pub})$$

UserKeyGen

This algorithm is used to generate the secret as well as public keys of the vehicles for vehicular communications in VANETs.

- The vehicle updates the secret and public key each time it enters the region of new RTA as it gets the new pseudo identity Q_{ID_i}.
- The vehicle and RSU takes as input *params*, to generate the secret and public keys. The vehicle with identity Q_{ID_i} selects $x_i \in_R \mathbb{Z}_q^*$ at random and sets x_i as the secret key of vehicle and sets the public key of vehicle as $P_i = x_i.P$.

PseudonymGen

This algorithm is run by the corresponding RSU_i under whose coverage, the vehicle is requesting for the pseudonym. The pseudonyms are allocated to vehicles each time a new RSU is encountered. The frequent updation of pseudonyms under each RSU may lead to consumption of network bandwidth and signalling overhead problem. Therefore, the RSU may combine to form the autonomous networks which will help in solving signaling overhead problem and bandwidth consumption, which may be caused due to the frequently updating of the pseudonyms under each RSU.

- It is assumed that autonomous network is comprised of 4 RSUs in scarcely populated areas and 2 RSUs in densely populated areas. Pseudonym is generated once under one autonomous network. This solution provides privacy and liability at the same time.
- The inputs taken by this algorithm are *params* and vehicle identity Q_{ID_i} and generates the pseudonym of the vehicle in two parts $PS1_j$ and $PS2_j$ such that $PS_j = PS1_j + PS2_j$.
- The autonomous network RSU_i selects $a_j \in_R \mathbb{Z}_q^*$ at random and sets $PS1_j = a_j.Q_{ID_i}$.

- Then it calculates the hash value of $PS1_j$ as $T_j = H_3(PS1_j) \in \mathbb{Z}_q^*$.
- The second part of pseudonym $PS2_j$ is calculated as $PS2_j = a_j.T_j$.
- Finally the pseudonym PS_j is calculated as $PS_j = PS1_j + PS2_j$.

Sign

To sign a message $m_k \in \mathscr{M}$ using the partial private key and private key pair (pp_i, x_i) with vehicle identity Q_{ID_i} and public key P_i, the following steps are performed:

- Choose a random $r_i \in_R \mathbb{Z}_q^*$ and compute $U_i = r_i.P \in \mathbb{G}_1$.
- Compute $h_{ijk} = H_2(m_k, PS1_j, P_i, U_i) \in \mathbb{Z}_q^*$.
- Compute $V_{ijk} = pp_i.PS2_j + h_{ijk}.r_i.P_{pub} + h_{ijk}.x_i.P_{rsu_i}$.
- Output the signature on m_k as $\sigma_{ijk} = (U_i, V_{ijk})$.

The first scalar multiplication $(pp_i.PS2_j)$ in V_{ijk} can be pre-computed whenever the pseudonym is generated for Q_{ID_i} in the current autonomous network as it saves one scalar multiplication during signature generation.

Verify

To verify the signature $\sigma_{ijk} = (U_i, V_{ijk})$ signed by the vehicle with pseudonym PS_j, given the *params*, pseudonym $PS1_j$, the public key P_i, the message m_k and the signature $\sigma_{ijk} = (U_i, V_{ijk})$, the vehicle:

- Computes $h_{ijk} = H_2(m_k, PS1_j, P_i, U_i)$.
- Computes $T_j = H_3(PS1_j)$.

- The signatures are accepted if the following equation holds:

$$e(V_{ijk}, P) = e(PS1_j.T_j + h_{ijk}.U_i, P_{pub})e(h_{ijk}.P_i, P_{rsu_i}) \tag{3.1}$$

- If the equation holds, output is true; otherwise, output is $\perp$.

The correctness of the scheme follows from the fact:

$$\begin{aligned}
e(V_{ijk}, P) &= e(pp_i.PS2_j + h_{ijk}.r_i.P_{pub} + h_{ijk}.x_i.P_{rsu_i}, P) \\
&= e(pp_i.PS2_j, P)e(h_{ijk}.r_i.P_{pub}, P)e(h_{ijk}.x_i.P_{rsu_i}, P) \\
&= e(s.Q_{ID_i}.a_j.T_j, P)e(h_{ijk}.r_i.s.P, P)e(h_{ijk}.x_i.y_i.P, P) \\
&= e(a_j.Q_{ID_i}.T_j, s.P)e(h_{ijk}.r_i.P, s.P)e(h_{ijk}.x_i.P, y_i.P) \\
&= e(PS1_j.T_j, P_{pub})e(h_{ijk}.U_i, P_{pub})e(h_{ijk}.P_i, P_{rsu_i}) \\
&= e(PS1_j.T_j + h_{ijk}.U_i, P_{pub})e(h_{ijk}.P_i, P_{rsu_i})
\end{aligned}$$

The current setup allows the KGC to choose a secret key $x_i^{'} \in \mathbb{Z}_q^*$ and compute new public key of user $P_i^{'} = x_i^{'}.P$ with identity Q_{ID_i}. Therefore, KGC is able to know both the partial private key and the private key of the vehicle which implies that both KGC and vehicle may deny signature generation. But in this scheme, the pseudonyms are generated by the RSUs and thus each RSU verify the user identity and then generates the pseudonym corresponding to that identity. The signatures are generated using pseudonyms for those identities. So KGC does not have access to pseudonyms and it cannot forge the signatures. Moreover, if public key is replaced by KGC, it can easily be detected by law enforcement authorities as the KGC is the only entity having that capability. The various steps for initiation of vehicular communication are depicted in Figure 3.1.

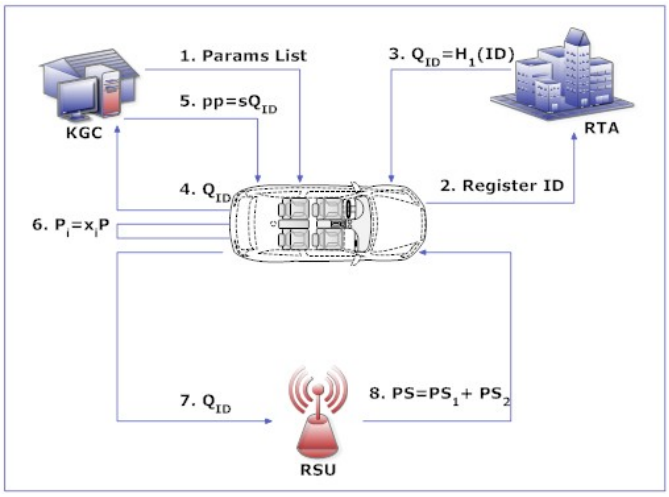

Figure 3.1: The various steps involved for registration and key generation of vehicle

3.3 Certificateless Aggregate Signature Scheme

This section describes the construction of a new certificateless aggregate signature scheme for VANETs. All the six algorithms *Setup*, *Registration*, *PartialKeyGen*, *UserKeyGen*, *PseudonymGen* and *Sign* algorithms remain same as proposed in the basic CLS scheme (section 3.2). Two new algorithms used in CLAS are:

Aggregate

This algorithm aggregates the collection of individual signatures. The vehicle acts as an aggregate signature generator, aggregating a collection of n signatures from n users $\{\mathscr{U}_1.....\mathscr{U}_n\}$ with pseudonyms $\{\mathscr{PS}_1.....\mathscr{PS}_n\}$, public keys $\{\mathscr{P}_1.....\mathscr{P}_n\}$ with messages $\{\mathscr{M}_1.....\mathscr{M}_n\}$ and signatures $\{\sigma_1 = (U_1, V_1)$ ..... $\sigma_n = (U_n, V_n)\}$ from corresponding users $\{\mathscr{U}_1.....\mathscr{U}_n\}$ respectively. It aggregates all the signatures signed under the same RSU. The aggregate signatures can be computed as $V = \sum_{i=1}^{n} V_i$ and $\sigma = (U_1....U_n, V)$ is an output for an aggregate signature pair.

AggregateVerify

An aggregate signature $\sigma = (U_1.....U_n, V)$ which is signed by n users $\{\mathscr{U}_1....\mathscr{U}_n\}$ on n messages $\{\mathscr{M}_1.....\mathscr{M}_n\}$ is verified by AggregateVerify algorithm with the help of following steps:

- Compute $h_i = H_2(m_i, PS1_i, P_i, U_i)$ for i = 1 to n.
- Compute $T_i = H_3(PS1_i)$ for i = 1 to n.
- Check the following equation if it holds or not:

$$e(V,P) = e(\sum_{i=1}^{n}[PS1_i.T_i + h_i.U_i], P_{pub})e(\sum_{i=1}^{n} h_i.P_i, P_{rsu}) \tag{3.2}$$

for all the messages signed under single RSU. The vehicle accepts the signature if the equation holds, otherwise outputs $\perp$.

3.4 Security Proof

Assuming the hardness of computational diffie-hellman problem, the security of the certificateless aggregate signature scheme is hereby shown.

Theorem 1. *In the random oracle model, an adversary $\mathscr{A}_1$ exists having an advantage ε to forge a signature in game I modelled attack within a time span t and performs queries to various oracles by making q_i queries to H_i for i = 1,2,3, q_k queries to RevealPartialKey, q_s queries to the RevealSecretKey, q_p queries to RevealPublicKey, q_{ps} queries to RevealPseudonym and q_{sig} queries to sign, then CDH problem can be solved in time*

$$t + \varphi(q_1 + q_2 + q_3 + q_k + q_s + q_p + q_{ps} + q_{sig})t_m$$

where t_m is computation time for scalar multiplication in $\mathbb{G}_1$ with probability

$$\varepsilon' \geq \frac{1}{(q_k+1).e}\varepsilon$$

Proof. Let $\mathscr{C}$ be an attacker receiving a random instance (P, aP, bP) of the CDH problem in cyclic group $\mathbb{G}_1$. Point P is a generator of $\mathbb{G}_1$ having prime order q. Now, $X = a.P$ and $Y = b.P$ where a and b are randomly chosen in ${}_R\mathbb{Z}_q^*$. A Type I adversary $\mathscr{A}_1$ interacts with $\mathscr{C}$ as modelled in Game I. $\mathscr{C}$ uses $\mathscr{A}_1$ for solving the CDH problem by computing abP in $\mathbb{G}_1$ with the construction of an algorithm S_1. $\mathscr{C}$ sends the params = $(\mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_2, H_3, P_{rsu})$ to $\mathscr{A}_1$.

S_1 chooses random $c \in {}_R\mathbb{Z}_q^*$ and sets P_{pub} = X and $P_{rsu} = c.P$ and then start performing oracle queries. The hash functions H_1, H_2 and H_3 are considered random oracles. It is assumed that $H_1(.)$ oracle query has been previously made on that identity for which key extraction or signature query has been made. A list L = $(ID_i, pp_i, x_i, P_i, PS_j)$ is maintained by S_1 while $\mathscr{A}_1$ makes queries throughout the Game I and $\mathscr{C}$ maintains S_1 algorithm. S_1 responds to all the $\mathscr{A}_1$ queries. $\mathscr{A}_1$ performs the following queries:

H_1 queries:

After an identity ID_i is being submitted to oracle H_1, same answer will be given if the request has been asked before. Otherwise, S_1 flips a coin $c_i \in \{0,1\}$ yielding 0 with probability ζ and yielding 1 with probability $(1-\zeta)$. It then randomly pick $\alpha_i \in {}_R\mathbb{Z}_q^*$. If c_i = 0, then $H_1(ID_i)$ is defined as $Q_i = \alpha_i.Y \in \mathbb{G}_1$. If c_i = 1, then $H_1(ID_i) = \alpha_i.P \in \mathbb{G}_1$. In both cases, S_1 inserts a tuple $(ID_i, \alpha_i, c_i, Q_i)$ in a list $L_{H_1} = (ID_i, \alpha_i, c_i, Q_i)$ to keep the track of the queries.

H_2 queries:

S_1 maintains a list $L_{H_2} = (m_k, PS1_j, P_i, U_i, h_{ijk})$ which is initially empty. When $\mathscr{A}_1$ issues a query $H_2(m_k, PS1_j, P_i, U_i)$, the same answer from the list L_{H_2} will be given if the request has been previously made. Otherwise S_1 selects random element $h_{ijk} \in_R \mathbb{Z}_q^*$ and adds the tuple $(m_k, PS1_j, P_i, U_i, h_{ijk})$ to the list L_{H_2} and returns h_{ijk} as the answer to the hash value of $H_2(m_k, PS1_j, P_i, U_i)$ to $\mathscr{A}_1$.

H_3 queries:

S_1 maintains a list L_{H_3} = $(PS1_j, t_{1_j})$ which is initially empty. When $\mathscr{A}_1$ issues a query $H_3(PS1_j)$, same answer will be returned if the query has been previously made. Otherwise, S_1 selects a random $t_{1_j} \in_R \mathbb{Z}_q^*$ and adds $(PS1_j, t_{1_j})$ to the list L_{H_3} and return t_{1_j} as answer to $\mathscr{A}_1$.

RevealPseudonym queries:

The request is issued on an identity ID_i.

- The corresponding tuple $(ID_i, pp_i, x_i, P_i, PS_j)$ is recovered from the list L. S_1 checks if PS_j is $\perp$. If $PS_j \neq \perp, S_1$ returns PS_j to $\mathscr{A}_1$. Otherwise, S_1 randomly chooses $k_j \in_R \mathbb{Z}_q^*$ and computes $PS1_j = k_j.Q_i \in \mathbb{G}_1$ with ID_i corresponding to the list L_{H_1} = $(ID_i, \alpha_i, c_i, Q_i)$ if c_i = 1 and $PS2_j = k_j$. t_{1_j} where t_{1_j} corresponds to the list $L_{H_3} = (PS1_j, t_{1_j})$. S_1 returns PS_j = $(PS1_j + PS2_j)$ to the adversary $\mathscr{A}_1$ and adds $(ID_i, pp_i, x_i, P_i, PS_j)$ to the list L.

- If the list L does not contain $(ID_i, pp_i, x_i, P_i, PS_j)$, then S_1 sets $PS_j = \perp$ and then randomly chooses $k_j \in_R \mathbb{Z}_q^*$ and computes $PS1_j = k_j.Q_i$ and $PS2_j = k_j.t_{1_j}$ from corresponding lists $L_{H_1} = (ID_i, \alpha_i, c_i, Q_i)$ and $L_{H_3} = (PS1_j, t_{1_j})$ respectively. S_1 answers

$PS_j = (PS1_j + PS2_j)$ to the adversary $\mathscr{A}_1$ and adds $(ID_i, pp_i, x_i, P_i, PS_j)$ to the list L.

RevealPartialKey queries:

The request is issued on an identity ID_i.

- The corresponding tuple $(ID_i, \alpha_i, c_i, Q_i)$ is recovered from the list L_{H_1}. If c_i = 0, then S_1 returns failure.

- If c_i = 1, and if list L contains $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 checks if $pp_i = \perp$. If $pp_i \neq \perp$, then S_1 returns pp_i to S_1. If $pp_i = \perp, S_1$ recovers the tuple $(ID_i, \alpha_i, c_i, Q_i)$ from the list L_{H_1}. Now, c_i = 1 i.e. $H_1(ID_i)$ is defined as $\alpha_i.P \in \mathbb{G}_1$ and $pp_i = \alpha_i.P_{pub} = \alpha_i.X \in \mathbb{G}_1$. S_1 returns partial private key pp_i to $\mathscr{A}_1$ and adds tuple $(ID_i, pp_i, x_i, P_i, PS_j)$ into list L.

- Again if c_i = 1, and list L does not contain the tuple $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 sets $pp_i = \perp$ and recovers $(ID_i, \alpha_i, c_i, Q_i)$ from the list L_{H_1}. S_1 sets $pp_i = \alpha_i.P_{pub} = \alpha_i.X \in \mathbb{G}_1$ and returns pp_i to $\mathscr{A}_1$ and adds $(ID_i, pp_i, x_i, P_i, PS_j)$ into the list L.

RevealPublicKey queries:

The request is issued on an identity ID_i.

- If the list L contains $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 checks whether $P_i = \perp$. If $P_i \neq \perp$, then S_1 returns P_i to S_1. Otherwise if $P_i = \perp$, S_1 randomly selects $v_i \in_R \mathbb{Z}_q^*$ and $P_i = v_i.P \in \mathbb{G}_1$ and $x_i = v_i$. S_1 returns P_i as answer to $\mathscr{A}_1$ and saves (P_i, x_i) into the list L.

- If the list L does not contain $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 sets $P_i = \perp$ and sets $x_i = v_i$, $P_i = v_i.P \in \mathbb{G}_1$; $v_i \in_R \mathbb{Z}_q^*$ and returns P_i to $\mathscr{A}_1$ and adds the tuple $(ID_i, pp_i, x_i, P_i, PS_j)$ to the list L.

RevealSecretKey queries:

The request is issued on an identity ID_i.

- If the list L contains $(ID_i, pp_i, x_i, P_i, PS_j)$, then S_1 checks if $x_i = \perp$. If $x_i \neq \perp$, then S_1 returns x_i to $\mathscr{A}_1$. Otherwise, S_1 selects at random $v_i \in {}_R\mathbb{Z}_q^*$ and sets $x_i = v_i$ and $P_i = v_i.P \in \mathbb{G}_1$. It returns x_i to $\mathscr{A}_1$ and adds $(ID_i, pp_i, x_i, P_i, PS_j)$ into the list L.

- If the list L does not contain $(ID_i, pp_i, x_i, P_i, PS_j)$, then S_1 sets $x_i = \perp$ and selects randomly $v_i \in {}_R\mathbb{Z}_q^*$ and $P_i = v_i.P \in \mathbb{G}_1$ and $x_i = v_i$. It returns x_i to $\mathscr{A}_1$ and adds $(ID_i, pp_i, x_i, P_i, PS_j)$ into the list L.

ReplacePublicKey queries:

Suppose $\mathscr{A}_1$ chooses new public key $P_i^{'}$ for an identity ID_i.

- S_1 searches the list L and if L contains an element $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 replaces P_i with $P_i^{'}$ and sets $x_i = \perp$.

- If the list L does not contain $(ID_i, pp_i, x_i, P_i, PS_j)$, then S_1 sets $P_i = P_i^{'}$ and $x_i = \perp$. It also sets $pp_i = \perp$ and adds $(ID_i, pp_i, x_i, P_i, PS_j)$ into the list L.

Sign queries:

On receiving a sign query on ID_i , S_1 firstly recovers L_{H_1} list as $(ID_i, \alpha_i, c_i, Q_i)$, then list L as $(ID_i, pp_i, x_i, P_i, PS_j)$, list L_{H_2} as $(m_k, PS1_j, P_i, U_i, h_{ijk})$ and list L_{H_3} as $(PS1_j, t1_j)$ and generates the signature as follows:

- If c_i = 1 and if the list L contains $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 checks if $x_i = \perp$. If $x_i = \perp$, S_1 makes *RevealPublicKey* query to generate $x_i = v_i$ and $P_i = v_i.P$.

- If L does not contain $(ID_i, pp_i, x_i, P_i, PS_j)$, S_1 makes *RevealPublicKey* query to generate x_i and P_i and adds it to list L.

- To generate the signature, if c_i = 0, choose r_i, $\gamma_i \in {}_R\mathbb{Z}_q^*$, set $U_i = r_i.P - h_{ijk}^{-1}.PS1_j.t1_j$ and computes

$$\begin{aligned} V_{ijk} &= pp_i.PS2_j + h_{ijk}.r_i.P_{pub} + h_{ijk}.x_i.P_{rsu} \\ &= h_{ijk}.r_i.X + h_{ijk}.x_i.P_{rsu} \end{aligned} \tag{3.3}$$

  The output σ_{ijk} can be expressed as $\sigma_{ijk} = (U_i, V_{ijk})$

- If c_i = 1, to generate the signature, choose at random $r_i \in {}_R\mathbb{Z}_q^*$ and $U_i = r_i.P \in \mathbb{G}_1$ and set the values $pp_i = \alpha_i.X, PS2_j = k_j.t1_j, P_{rsu} = c.P$. It computes the value of V_{ijk} as

$$V_{ijk} = \alpha_i.X.k_j.t1_j + h_{ijk}.r_i.X + h_{ijk}.x_i.c.P \tag{3.4}$$

If the tuple containing h_{ijk} already appears in the list L_{H_2}, then S_1 selects another $r_i, h_{ijk} \in {}_R\mathbb{Z}_q^*$ and tries again. Finally S_1 responds to $\mathscr{A}_1$ with $\sigma_{ijk} = (U_i, V_{ijk})$. All the responses to *Sign* queries are valid, i.e. the output (U_i, V_{ijk}) of sign query is a valid signature generated on message m_k.

Now, when $c_i = 0$, $V_{ijk} = h_{ijk}.r_i.X + h_{ijk}.x_i.P_{rsu}$

$$\begin{aligned} e(V,P) &= e(h_{ijk}.r_i.X + h_{ijk}.x_i.P_{rsu}, P) \\ &= e(h_{ijk}.r_i.a.P, P)e(h_{ijk}.x_i.c.P, P) \\ &= e(h_{ijk}.r_i.P, aP)e(h_{ijk}.x_i.P, c.P) \\ &= e(h_{ijk}.U_i + PS1_j.t1_j, X)e(h_{ijk}.P_i, P_{rsu}) \end{aligned}$$

By forking lemma [29], replaying $\mathscr{A}_1$ with some random tape, S_1 obtains two valid signatures $\sigma^*_{ijk}(ID^*_i, m^*_k, h^*_{ijk}, U^*_i, V^*_{ijk})$ and $\sigma^{'*}_{ijk}(ID^*_i, m^*_k, h^{'*}_{ijk}, U^*_i, V^{'*}_{ijk})$ within polynomial time, where

$$V^*_{ijk} = pp^*_i.PS2^*_j + h^*_{ijk}.r^*_i.P^*_{pub} + h^*_{ijk}.x^*_i.P^*_{rsu} \tag{3.5}$$

$$V^{'*}_{ijk} = pp^*_i.PS2^*_j + h^{'*}_{ijk}.r^*_i.P^*_{pub} + h^{'*}_{ijk}.x^*_i.P^*_{rsu} \tag{3.6}$$

Multiplying both sides of equation (3.5) by $(h^*_{ijk})^{-1}$ and both sides of equation (3.6) by $(h^{'*}_{ijk})^{-1}$

$$(h^*_{ijk})^{-1}V^*_{ijk} = (h^*_{ijk})^{-1}pp^*_i.PS2^*_j + (h^*_{ijk})^{-1}h^*_{ijk}(r^*_i.P^*_{pub} + x^*_i.P^*_{rsu}) \tag{3.7}$$

$$(h^{'*}_{ijk})^{-1}V^{'*}_{ijk} = (h^{'*}_{ijk})^{-1}pp^*_i.PS2^*_j + (h^{'*}_{ijk})^{-1}h^{'*}_{ijk}(r^*_i.P^*_{pub} + x^*_i.P^*_{rsu}) \tag{3.8}$$

Subtracting (3.8) from (3.7)

$$(h^*_{ijk})^{-1}V^*_{ijk} - (h^{'*}_{ijk})^{-1}V^{'*}_{ijk} = [(h^*_{ijk})^{-1} - (h^{'*}_{ijk})^{-1}]pp^*_i.PS2^*_j \tag{3.9}$$

Then, S_1 recovers the corresponding $(ID_i, \alpha_i, c_i, Q_i)$ from the list L_{H_1}. If $c_i = 1$, S_1 aborts. Otherwise, if $c_i = 0$, $Q_i = \alpha_i.Y = \alpha_i.b.P, PS2_j = k_j.t_{1_j}$. Now P_{pub} = a.P , where a is the secret key of KGC. Then, $pp_i = a.Q_i = a(\alpha_i.b.P) = \alpha_i.abP$. Now, in equation (3.9),

$$(h^*_{ijk})^{-1}V^*_{ijk} - (h^{'*}_{ijk})^{-1}V^{'*}_{ijk} = [(h^*_{ijk})^{-1} - (h^{'*}_{ijk})^{-1}]\alpha_i.abP.k_j.t_{1_j}. \tag{3.10}$$

$$abP = [(h^*_{ijk})^{-1}V^*_{ijk} - (h^{'*}_{ijk})^{-1}V^{'*}_{ijk}][\alpha_i.k_j.t_{1_j}.((h^*_{ijk})^{-1} - (h^{'*}_{ijk})^{-1})]^{-1} \tag{3.11}$$

Thus, algorithm S_1 outputs abP as the solution to Computational Diffie Hellman problem.

The proof is completed by showing that S_1 solves the given instance of CDH problem with the probability

$$\varepsilon' \geq \frac{1}{(q_k+1).e}\varepsilon$$

S_1 needs three events in order to succeed:

E_1**:** The result of any $\mathscr{A}_1$'s *RevealPartialKey* queries does not abort S_1.

E_2**:** A valid and non trivial signature is generated by $\mathscr{A}_1$.

E_3**:** Probability that $\mathscr{A}_1$ outputs a valid and nontrivial forgery and S_1 does not abort.

Probability that S_1 succeeds after all these events happen is

$$P[E_1 \wedge E_2 \wedge E_3] = P[E_1] \cdot P[E_2|E_1] \cdot P[E_3|E_1 \wedge E_2]$$

- Claim 1: Probability that result of any $\mathscr{A}_1$'s *RevealPartialKey* queries does not abort S_1 is atleast $(1-\zeta)^{q_k}$. Hence, P$[E_1] \geq (1-\zeta)^{q_k}$

  Proof: $P[c_i = 1] = (1-\zeta)$, therefore probability that S_1 does not abort is $(1-\zeta)$. As it takes atmost q_k times *RevealPartialKey* queries, probability of S_1 not aborting after the queries of $\mathscr{A}_1$ is atleast $(1-\zeta)^{q_k}$.

- Claim 2: The probability of S_1 not aborting with $\mathscr{A}_1$'s signature queries and key extraction queries is ε. $P[E_2|E_1] \geq \varepsilon$.

- Claim 3: Probability that $\mathscr{A}_1$ outputs a valid and nontrivial forgery and S_1 does not abort is ζ. $P[E_3|E_1 \wedge E_2] \geq \zeta$

  Proof: Suppose $\mathscr{A}_1$ generated a valid and nontrivial forgery after the events E_1 and E_2 occurred. Thus, $P[E_3|E_1 \wedge E2] \geq \zeta$.

Thus,

$$\begin{aligned} P[E_1 \wedge E_2 \wedge E_3] &= P[E_1] \cdot P[E_2|E_1] \cdot P[E_3|E_1 \wedge E_2] \\ &= (1-\zeta)^{q_k} \cdot \varepsilon \cdot \zeta \\ &= \zeta(1-\zeta)^{q_k} \cdot \varepsilon \end{aligned} \tag{3.12}$$

Now, $\zeta_{opt} = \frac{1}{q_k+1}$. Thus,

$$\begin{aligned} \varepsilon^{'} &\geq \zeta(1-\zeta)^{q_k} \cdot \varepsilon \\ \varepsilon^{'} &\geq \frac{1}{q_k+1}[1-\frac{1}{q_k+1}]^{q_k} \cdot \varepsilon \end{aligned}$$

With sufficiently large q_k, the term $\left[1-\frac{1}{q_k+1}\right]^{q_k}$ tends to $\frac{1}{e}$. Thus the probability is,

$$\varepsilon^{'} \geq \frac{1}{(q_k+1).e}\varepsilon$$

□

Theorem 2. *In the random oracle model, an adversary $\mathscr{A}_2$ exists having an advantage ε to forge a signature in a game II modelled attack within a time span t and performs queries to various oracles by making q_2 queries to H_2, q_3 queries to H_3, q_p queries to RevealPublicKey, q_s queries to RevealSecretKey, q_{ps} queries to RevealPseudonym and q_{sig} queries to sign, then the CDH problem in $\mathbb{G}_1$ can be solved in time*

$$t + \varphi(q_2 + q_3 + q_s + q_p + q_{ps} + q_{sig})t_m$$

where t_m is the computational time for scalar multiplication in $\mathbb{G}_1$ with probability

$$\varepsilon' \geq \frac{1}{(q_p+1).e}\varepsilon$$

Proof. Let $\mathscr{C}$ be an attacker receiving a random instance (P,aP,bP) of the CDH problem in cyclic group $\mathbb{G}_1$. Point P is a generator of $\mathbb{G}_1$ having prime order q. X = a.P and Y = b.P where a and b are randomly chosen in ${}_R\mathbb{Z}_q^*$. A type II adversary $\mathscr{A}_2$ interacts with $\mathscr{C}$ as modelled in Game II. $\mathscr{C}$ uses $\mathscr{A}_2$ for solving the CDH problem by computing abP in $\mathbb{G}_1$ with the construction of an algorithm S_2. $\mathscr{C}$ sets P_{rsu} = aP = X. S_2 randomly sets the master key of KGC as $\lambda \in {}_R\mathbb{Z}_q^*$ and sets the public key of KGC as $P_{pub} = \lambda.P$. S_2 then sends the system parameters *params* $(\mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_2, H_3, P_{rsu})$ to $\mathscr{A}_2$. The adversary $\mathscr{A}_2$ is also provided the master key λ by S_2. Now, $\mathscr{A}_2$ has the master key so it can generate the partial public key itself. $\mathscr{C}$ maintains S_2 algorithm and S_2 responds to all the $\mathscr{A}_2$ queries and the partial private key $pp_i = s.H_1(ID_i)$ can be computed by both S_2 and $\mathscr{A}_2$. So, there is no need to model the hash function H_1 as random oracle. S_2 maintains a list $(ID_i, x_i, P_i, PS_j, c_i)$ in list L.

H_2 queries:

S_2 maintains a list L_{H_2} = $(m_k, PS1_j, P_i, U_i, h_{ijk})$ which is empty initially. Suppose $(m_k, PS1_j, P_i, U_i, h_{ijk})$ is submitted to $H_2(.)$. S_2 first checks if the request has been asked before on the same input and if so, the previous value is returned. Otherwise, S_2 selects random $h_{ijk} \in {}_R\mathbb{Z}_q^*$ and adds the tuple $(m_k, PS1_j, P_i, U_i, h_{ijk})$ to L_{H_2} and returns h_{ijk} as answer to the query made by $\mathscr{A}_2$.

H_3 queries:

S_2 maintains a list $L_{H_3} = (PS1_j, t_{1_j})$ which is empty initially. When $\mathscr{A}_2$ issues a query on $H_3(.)$ oracle, S_2 checks if the request has been asked previously on same input and returns

the same answer. Otherwise, S_2 selects a random $t_{1_j} \in_R \mathbb{Z}_q^*$ and adds $(PS1_j, t_{1_j})$ to the list L_{H_3} and return t_{1_j} as an answer to $\mathscr{A}_2$.

RevealPseudonym queries:

The request is issued on an identity ID_i.

- S_2 recovers the corresponding $(ID_i, x_i, P_i, PS_j, c_i)$ and checks if $PS_j = \perp$. If $PS_j \neq \perp$, S_2 returns PS_j to $\mathscr{A}_2$. Otherwise, S_2 randomly selects $k_j \in_R \mathbb{Z}_q^*$ and computes $PS1_j = k_j.Q_i$ where $Q_i = H_1(ID_i)$ and $PS2_j = k_j.t_{1_j}$ where the corresponding list is L_{H_3} = $(PS1_j, t_{1_j})$. S_2 returns PS_j = $(PS1_j + PS2_j)$ to $\mathscr{A}_2$ and adds $(ID_i, x_i, P_i, PS_j, c_i)$ to the list L.

- If the list L does not contain $(ID_i, x_i, P_i, PS_j, c_i)$, then S_2 sets $PS_j = \perp$ and randomly selects $k_j \in_R \mathbb{Z}_q^*$, computes $PS1_j = k_j.Q_i$ and $PS2_j = k_j.t_{1_j}$ where the corresponding list is L_{H_3} = $(PS1_j, t_{1_j})$ and $Q_i = H_1(ID_i)$. S_2 returns $PS_j = (PS1_j + PS2_j)$ to $\mathscr{A}_2$ and adds $(ID_i, x_i, P_i, PS_j, c_i)$ to the list L.

RevealPublicKey queries:

When the RevealPublicKey query is issued on an identity ID_i, the following three cases hold:

- S_2 checks the list L and if it contains $(ID_i, x_i, P_i, PS_j, c_i)$, S_2 returns P_i to $\mathscr{A}_2$.

- If the list L does not contain $(ID_i, x_i, P_i, PS_j, c_i)$, then a coin $c_i \in \{0,1\}$ is flipped by S_2 yielding 0 with probability ζ and yielding 1 with probability $(1-\zeta)$. If c_i = 0, S_2 randomly selects $\gamma_i \in_R \mathbb{Z}_q^*$ and sets $P_i = \gamma_i.P \in \mathbb{G}_1$. S_2 sets $x_i = \gamma_i$ and inserts a tuple $(ID_i, x_i, P_i, PS_j, c_i)$ to the list L and P_i is returned to $\mathscr{A}_2$.

- If c_i = 1, S_2 returns $P_i = \gamma_i.Y \in \mathbb{G}_1$ to $\mathscr{A}_2$ where a random $\gamma_i \in_R \mathbb{Z}_q^*$ and sets $x_i = \gamma_i$ and inserts a tuple $(ID_i, x_i, P_i, PS_j, c_i)$ to the list L.

RevealSecretKey queries:

The request is issued on an identity ID_i, the following three cases hold:

- It checks if the list L contains $(ID_i, x_i, P_i, PS_j, c_i)$, then it returns x_i to $\mathscr{A}_2$.
- If the list does not contain $(ID_i, x_i, P_i, PS_j, c_i)$, then if c_i = 1, it halts.
- If $c_i = 0$, S_2 makes *RevealPublicKey* query and the tuple $(ID_i, x_i, P_i, PS_j, c_i)$ is added to the list L and returns x_i to $\mathscr{A}_2$.

Sign Oracle:

On receiving a sign query on ID_i, S_2 initially recovers the list L = $(ID_i, x_i, P_i, PS_j, c_i)$, then $L_{H_2} = (m_k, PS1_j, P_i, U_i, h_{ijk})$ and $L_{H_3} = (PS1_j, t1_j)$ and generates the signature as follows:

- If c_i = 1, then if the list contains $(ID_i, x_i, P_i, PS_j, c_i)$, S_2 checks as $x_i = \gamma_i$ and $P_i = \gamma_i.Y \in \mathbb{G}_1$.
- If c_i = 0, then list contains $(ID_i, x_i, P_i, PS_j, c_i)$, S_2 checks as $x_i = \gamma_i$ and $P_i = \gamma_i.P \in \mathbb{G}_1$.

Now, for generating the signature, if c_i =1, then S_2 checks if the adversary $\mathscr{A}_2$ has not made the *sign* query on $(ID_i, x_i, P_i, PS_j, c_i)$. In addition, the forged signature must satisfy

$$\begin{aligned} e(V,P) &= e(PS1_j.t1_j + h_{ijk}.U_i, P_{pub})e(h_{ijk}.P_i, P_{rsu}) \\ &= e(k_j.Q_i.t1_j + h_{ijk}.U_i, P_{pub})e(h_{ijk}.P_i, P_{rsu}) \end{aligned} \tag{3.13}$$

The above equation holds for a valid signature. Otherwise, S_2 aborts. If the equation holds i.e. if S_2 does not abort, then the signature on $(ID_i^*, x_i^*, P_i^*, PS_j^*, c_i)$ is

$$e(V^*,P) = e(PS1_j^* \cdot t1_j^* + h_{ijk}^* \cdot U_i^*, P_{pub})e(h_{ijk}^* \cdot P_i^*, P_{rsu}) \tag{3.14}$$

By setting the values as $PS1_j^* = k_j \cdot Q_i^*$, $Q_i^* = H_1(ID_i^*)$, $P_{pub} = \lambda \cdot P$, $P_{rsu} = a \cdot P$, $P_i = \gamma_i^* \cdot Y = \gamma_i^* \cdot bP$, and $t_{1_j}^* = H_3(PS1_j^*)$:

$$\begin{aligned} e(V^*, P) &= e(k_j \cdot Q_i^* \cdot t_{1_j}^* + h_{ijk}^* \cdot U_i^*, \lambda \cdot P) e(h_{ijk}^* \cdot \gamma_i^* \cdot bP, aP) \qquad (3.15) \\ e(h_{ijk}^* \cdot \gamma_i^* \cdot bP, aP) &= e(V^*, P) e(k_j \cdot Q_i^* \cdot t_{1_j}^* + h_{ijk}^* \cdot U_i^*, \lambda \cdot P)^{-1} \\ e(h_{ijk}^* \cdot \gamma_i^* \cdot abP, P) &= e(V^*, P) e((k_j \cdot Q_i^* \cdot t_{1_j}^* + h_{ijk}^* \cdot U_i^*)\lambda, P)^{-1} \\ e(h_{ijk}^* \cdot \gamma_i^* \cdot abP, P) &= e(V^* - \lambda(k_j \cdot Q_i^* \cdot t_{1_j}^* + h_{ijk}^* \cdot U_i^*), P) \end{aligned}$$

Now,

$$\begin{aligned} h_{ijk}^* \cdot \gamma_i^* \cdot abP &= V^* - \lambda(k_j \cdot Q_i^* \cdot t_{1_j}^* + h_{ijk}^* \cdot U_i^*) \qquad (3.16) \\ abP &= (h_{ijk}^* \cdot \gamma_i^*)^{-1} [V^* - \lambda(k_j \cdot Q_i^* \cdot t_{1_j}^* + h_{ijk}^* \cdot U_i^*)] \end{aligned}$$

Thus, S_2 outputs abP as the solution of the Computational Diffie Hellman problem. Similar to Theorem 1, it can be shown that the given instance of CDH problem is solved by S_2 with probability

$$\varepsilon' \geq \frac{1}{(q_p + 1).e} \varepsilon$$

□

Theorem 3. *The certificateless aggregate signature scheme is considered secure against existential forgery if the proposed certificateless signature scheme is secure against adaptive chosen message attacks in the aggregate model.*

Proof. There exists an adversary $\mathscr{A}$ having an advantage ε in forging a signature in certificateless aggregate signature scheme in the random oracle model. An algorithm S is con-

structed to output the forgery of the certificateless aggregate signature scheme. S chooses random $c \in {}_R\mathbb{Z}_q^*$ and sets P_{pub} = X and P_{rsu} = c.P and then start performing oracle queries. Algorithm S maintains a list L = $(ID_i, pp_i, x_i, P_i, PS_i)$ while $\mathscr{A}$ makes queries throughout the game and algorithm S responds to all the queries of $\mathscr{A}$.

H_1 queries:

On submitting an identity ID_i to oracle H_1, it returns same answer if the request has been asked before. Otherwise, a coin $c_i \in \{0,1\}$ is flipped by S yielding 0 with probability ζ and yielding 1 with probability $(1-\zeta)$ and picks α_i randomly from ${}_R\mathbb{Z}_q^*$. If $c_i = 0, H_1(ID_i)$ is defined as $Q_i = \alpha_i.P_{pub} \in \mathbb{G}_1$. If c_i = 1, then the hash value $H_1(ID_i) = \alpha_i.P \in \mathbb{G}_1$. A tuple $(ID_i, \alpha_i, c_i, Q_i)$ is inserted in the list $L_{H_1} = (ID_i, \alpha_i, c_i, Q_i)$ by algorithm S in both cases to keep the track of all the queries. Now, ultimately adversary $\mathscr{A}$ has to output n users set with identities from $L_{ID}^* = \{ID_1^*.....ID_n^*\}$, public keys from $L_P^* = \{P_1^*.....P_n^*\}$, pseudonyms from $L_{PS}^* = \{PS_1^*.....PS_n^*\}$, n messages from the set $L_m^* = \{m_1^*.....m_n^*\}$ and aggregate signature $\sigma^* = (U_1^*....U_n^*, V^*)$. Now, S finds the corresponding n tuples $(ID_i, \alpha_i, c_i, Q_i)$ for i = 1 to n from L_{H_1} and precedes only when c_k = 0 and c_j = 1 for j = 1 to n and $j \neq k$. The signature $(m_k^*, PS1_k^*, P_k^*, U_k^*, h_k^*)$ has never been requested before. Otherwise, S will fail and halt. When $Q_k = \alpha_k.P_{pub}$ and $Q_j = \alpha_j.P$ for j = 1 to n and $j \neq k$, S succeeds. The generated aggregate signature is $\sigma^* = (U_1^*....U_n^*, V^*)$ satisfying the aggregate verification equation:

$$e(V^*, P) = e(\sum_{i=1}^{n}[PS1_i^*.T_i^* + h_i^*.U_i^*], P_{pub})e(\sum_{i=1}^{n} h_i^*.P_i^*, P_{rsu}) \tag{3.17}$$

Then, S searches the tuple $(m_i^*, PS1_i^*, P_i^*, U_i^*, h_i^*)$ from the list L_{H_2}, $(PS1_i^*, t_{1_i}^*)$ from the list L_{H_3} and the tuple $(ID_i^*, pp_i^*, x_i^*, P_i^*, PS_i^*)$ from the list L. It sets V_i^* =$\alpha_i.P_{pub}$, then $e(V_i^*, P) =$

$e(Q_i^*, P_{pub})$ for i = 1.....n, $j \neq k$. Finally S constructs $V_i^{'*}$ as $V^* - \sum_{i=1, i\neq k}^{n} V_i^*$. Now,

$$V_i^{'*} = pp_k^*.PS2_k^* + \sum_{i=1}^{n} h_i^*.r_i^*.P_{pub}^* + \sum_{i=1}^{n} h_i^*.x_i^*.P_{rsu}^* \tag{3.18}$$

As $U_i^* = r_i^*.P$ and $r_i^* \in {}_R\mathbb{Z}_q^*(1 \leq i \leq n)$. Algorithm S now chooses a random number $w_k^* \in {}_R\mathbb{Z}_q^*$ and computes $U^{'*} = (w_k^*)^{-1} \sum_{i=1}^{n} h_i^*.U_i^*$. After this, S computes $P_k^{'*} = (w_k^*)^{-1} \sum_{i=1}^{n} h_i^*.P_i^*$.

S updates P_i to $P_i^{'}$ by invoking *ReplacePublicKey* query. Then, S defines the hash value $H_2(m_k^*, PS1_k^*, P_k^*, U_k^*) = w_k^*$. If the tuple $(m_k^*, PS1_k^*, P_k^*, U_k^*)$ already appears in list L_{H_2} then it tries another w_k^* until there is no collision. Thereupon, $(U^{'*}, V^{'*})$ is a valid signature for identity ID_k^* on message m_k^* with pseudonym PS_k^* and corresponding public key P_k^*. Its verification equation is:

$$\begin{aligned}
& e(w_k^*.U^{'*} + PS1_k^*.t_{1_k}^*, P_{pub}) e(w_k^*.P_k^{'*}, P_{rsu}) \\
&= e(w_k^*.(w_k^*)^{-1} \sum_{i=1}^{n} h_i^*.U_i^* + PS1_k^*.t_{1_k}^*, P_{pub}) e(w_k^*.(w_k^*)^{-1} \sum_{i=1}^{n} h_i^*.P_i^*, P_{rsu}) \\
&= e(\sum_{i=1}^{n} h_i^*.U_i^* + PS1_k^*.t_{1_k}^*, P_{pub}) e(\sum_{i=1}^{n} h_i^*.P_i^*, P_{rsu}) \\
&= e(\sum_{i=1}^{n} h_i^*.r_i^*.P_{pub} + pp_i^*.PS2_k^*, P) e(\sum_{i=1}^{n} h_i^*.x_i^*.P_{rsu}, P) \\
&= e(V^{'*}, P)
\end{aligned} \tag{3.19}$$

Thus, the output $(U^{'*}, V^{'*})$ is given by algorithm S which acts as a forgery of the basic certificateless signature scheme.

To complete the proof, it is to be shown that S's advantage in forging the basic certificateless signature is atleast

$$\varepsilon^{'} \geq \frac{1}{(q_k + n).e} \cdot \varepsilon$$

There are three events needed for S to succeed:

E_1: The result of any $\mathscr{A}$'s *RevealPartialKey* queries does not abort S.

E_2: A valid and non trivial signature is generated by $\mathscr{A}$.

E_3: Probability that $\mathscr{A}$ outputs a valid and nontrivial forgery and S does not abort.

Probability that S succeeds after all these events happen is

$$P[E_1 \wedge E_2 \wedge E_3] = P[E_1] \cdot P[E_2|E_1] \cdot P[E_3|E_1 \wedge E_2]$$

- Claim 1: Probability that S does not abort as a result of the *RevealPartialKey* queries is atleast $(1-\zeta)^{q_k}$ Hence, $P[E_1] \geq (1-\zeta)^{q_k}$

  Proof: $P[c_i = 1] = (1-\zeta)$, for key extraction queries, probability that S does not abort is $(1-\zeta)$. As it takes atmost q_k times *RevealPartialKey* queries, probability that S does not abort as result of $\mathscr{A}$ queries is atleast $(1-\zeta)^{q_k}$.

- Claim 2: The probability of S not aborting with $\mathscr{A}$'s signature queries and key extraction queries is ε . $P[E_2|E_1] \geq \varepsilon$.

- Claim 3: Probability that $\mathscr{A}$ outputs a valid and nontrivial forgery and S does not abort is ζ. $P[E_3|E_1 \wedge E_2] \geq \zeta(1-\zeta)^{n-1}$

  Proof: Suppose events E_1 and E_2 have occurred and $\mathscr{A}$ has generated some valid and nontrivial forgery. Hence $P[E_3|E_1 \wedge E_2] \geq \zeta(1-\zeta)^{n-1}$

Thus,

$$\begin{aligned} P[E_1 \wedge E_2 \wedge E_3] &= P[E_1] \cdot P[E_2|E_1] \cdot P[E_3|E_1 \wedge E_2] \\ &= (1-\zeta)^{q_k} \cdot \varepsilon \cdot \zeta(1-\zeta)^{n-1} \\ &= \zeta(1-\zeta)^{q_k+n-1} \cdot \varepsilon \end{aligned} \tag{3.20}$$

Now, $\zeta_{opt} = \frac{1}{q_k+n}$. Thus,

$$\begin{aligned} \varepsilon' &\geq \zeta(1-\zeta)^{q_k+n-1} \cdot \varepsilon \\ &\geq \frac{1}{q_k+n}\left[1-\frac{1}{q_k+n}\right]^{q_k+n-1} \cdot \varepsilon \end{aligned}$$

With sufficiently large q_k, the term $\left[1-\frac{1}{q_k+n}\right]^{q_k+n-1}$ tends to $\frac{1}{e}$. Thus the probability is,

$$\varepsilon' \geq \frac{1}{(q_k+n)\cdot e} \cdot \varepsilon$$

□

3.5 Conclusion

A new efficient certificateless aggregate signature scheme is proposed for vehicular communications which is proven existentially unforgeable against the chosen message attack under the assumption that CDH problem is intractable in the random oracle model. The proposed CLAS scheme is adduced specifically for securing vehicular communications by reducing the signature verification time drastically and helps in verifying more messages in the specific stipulated time, thus increasing the efficiency of the network. This scheme can be successfully implemented in networks having limited bandwidth. The proposed scheme is employed for the design of security framework in the next chapter.

Chapter 4

Privacy Preserving Authentication Framework

The data on traffic conditions is of prime importance due to which the Intelligent Transportation Systems (ITS) have developed various techniques that allow them to characterize the traffic flow conditions on the road and make intelligent decisions accordingly. VANETs enable the vehicles to exchange traffic related information by communicating with other entities. An On Board Unit (OBU) installed in the vehicle, periodically broadcasts its position and state information to all its neighbouring vehicles to allow them to make opinions according to the traffic flow information received.

The information received should be authentic as the received message may contain the invalid or false information which violate the traffic safety conditions but the anonymity of vehicles should also be preserved that adversary may not track the vehicle to violate its privacy. To preserve the authenticity of vehicles, digital signature schemes [250][251] are used to verify if the messages are received from legitimate vehicles. Besides, the fundamental security aspect of vehicular networks, privacy is violated by the digital signatures as the vehicles are authenticated for useful information. The unconditional privacy may also

jeopardise the network as any anonymous sender may inject any malicious information in the network. Therefore, conditional privacy preservation of vehicles should be incorporated where the vehicles will communicate with each other anonymously and the law enforcement authorities should be able to trace the vehicle's actual identity in case the vehicle acts maliciously. Fundamentally, the security design of VANETs should assure authenticity, integrity, privacy, traceability, non-repudiation and confidentiality to protect the network against intruders. A new security system is proposed for VANETs to efficiently solve all the security constraints and considerations. The proposed scheme includes the following contributions:

1. A pseudonymous based approach is proposed where the pseudonyms are used for anonymous communications.

2. The vehicle identity cannot be revealed by single authority as multiple authorities are involved to locate the actual identity of the vehicle.

3. A privacy preserving signature scheme is designed for inter-vehicle communication to allow anonymous inter-vehicle communication.

4. Aggregate signature verification is proposed to enhance the message verification process so that the important messages may not be discarded.

5. Bloom filters are used to enhance the verification process by preventing the message drop in case of heavy busy traffic hours.

6. The security analysis of the scheme is done to assure the accuracy of the system.

A privacy preserving authentication scheme is proposed which employs the use of certificateless cryptography for the signature generation and verification process. The existing proposed frameworks are mainly based on the identity based cryptography or the Public Key Cryptography which have the issue of Key escrow problem [118] and the certificate overhead

Table 4.1: Properties of related security schemes

Security Schemes	Privacy	Pseudonyms	Non-Repudiation	Certificates	Storage Overhead	Computation Overhead	RSU-aided	Aggregate Verification
ECDSA [49]	✓	×	×	✓	✓	✓	×	×
GSIS [51]	✓	×	×	×	×	✓	✓	×
ECPP [52]	✓	×	✓	✓	✓	✓	✓	×
PASS [50]	✓	✓	✓	✓	✓	✓	✓	×
DCS [68]	✓	×	✓	✓	✓	✓	✓	✓
LPA [65]	✓	×	✓	✓	×	×	✓	×
ACPN [63]	✓	✓	✓	×	×	×	✓	×
CAPA [66]	✓	×	×	×	×	×	×	×
Proposed Scheme	✓	✓	✓	×	×	×	✓	✓

problem respectively. Hence, these are less suited authentication approaches for VANETs. Moreover, the symmetric cryptography too is not much suitable as it requires the pairwise shared keys among all the entities. The certificateless cryptography solves the key escrow problem and the certificate overhead problem and does not require the pairwise shared keys, making it one of the most feasible solution for VANETs. Table 6.1 compares the properties of the proposed security framework with the related works.

4.1 System Overview

The communication in VANETs necessitates the reliable transmission of messages as well as authenticated delivery of messages. Hence, the security architecture of VANETs should be capable of attaining the security requirements of message integrity, authentication and non-repudiation. The messages transmitted in vehicular networks should be verified on vehicle's onboard expeditiously and effectively. The RSUs have high computational and communication capability as compared to vehicles. The RSUs are connected with trusted authorities via Ethernet, whereas the V2V communication and V2I communication take place through the IEEE 802.11p. The idea is that inter-vehicular communications are aggregately verified by the signature scheme generated for V2V communication with the adoption of bloom filter to upsurge the signature verification process. The bloom filters have the advantage of constant

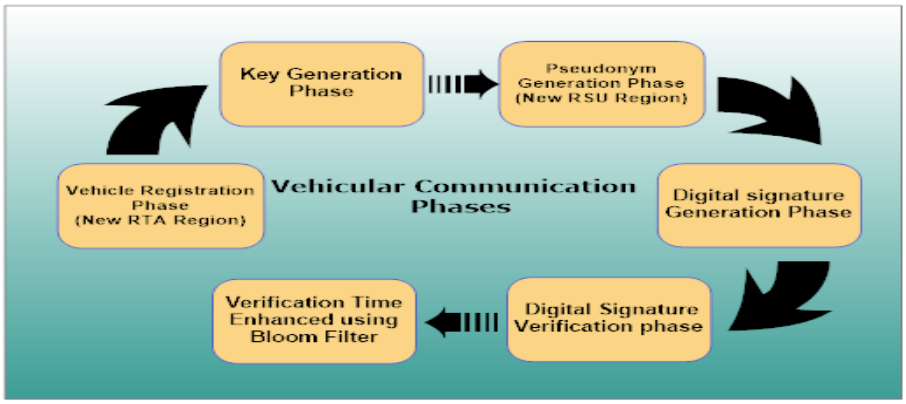

Figure 4.1: Phases of vehicular communication

search time complexity and moreover, it just takes 'm' bits to store the 'm' entries making it space and time efficient. The ID based cryptography is employed for V2I and I2V communication. Further, two trusted authorities are proposed, Regional Transportation Authority (RTA) and Key Generation Centre (KGC) where former is used for registering the vehicle ID and latter is employed for the generation of keys. The general Vehicular communication phases for the proposed framework are depicted in the Figure 4.1.

4.1.1 System Assumptions

OBUs: The minor changes are adopted in the capability of OBUs apart from the already existing capabilities of storage, computation and communication facilities:

i) Password protected OBU

ii) GPS enabled units

iii) Bloom filter

iv) Tamper proof hardware

It is assumed that all the vehicles possess an ID when the vehicle is purchased, it is allocated by RTA only after registering the personal details of the vehicle owner and further,

this ID is stored in the database of the Trusted Authority (TA). The initial security parameters and the public keys are embedded in the vehicle's OBU. Further, it is assumed that the number of dishonest vehicles is very less as compared to the honest vehicles and each vehicle is under the communication range of 1 RSU or the other.

Trusted Authorities: The Trusted Authority (TA), Regional Trusted Authority (RTA) and Key Generation Centre (KGC) are assumed to be trusted by all the entities in the network and it is impossible for an attacker to compromise them.

RSUs: The Road Side Units (RSUs) are static and situated along the roads. There is regular and uninterrupted coverage of RSUs along the roads. These are more prone to the attacks as they are exposed to the open environments. It is assumed that the functionality of RSUs are monitored by the RTA at regular intervals and any attack to RSU can be detected in the bounded time. The RSUs are connected with each other via secure channel of Ethernet. It is assumed that RSUs have tamper proof hardware and very scarce number of RSUs are compromised (at any given instant of time).

4.1.2 System Model

The system model for the proposed framework as shown in Figure 4.2 consists of the top trusted authorities who control the immobile RSUs on the road side and each road side infrastructure controls the vehicles under their range. The communication among various vehicles takes place via IEEE 802.11p communication technology in the bandwidth spectrum from 5.850 GHz to 5.925 GHz. The various RSUs communicate with each other via trusted authorities or directly with each other through a secure channel of Ethernet.

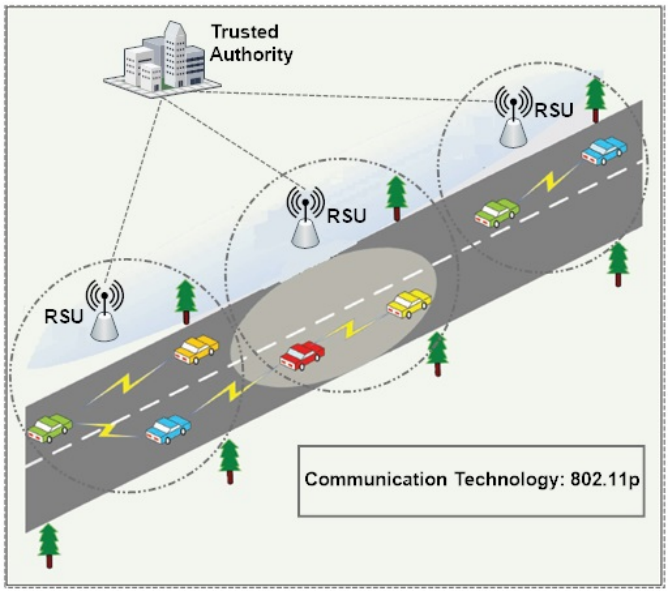

Figure 4.2: System model

4.1.3 Network Design

The network design architecture of the proposed scheme is divided into three units (Figure 4.3), consisting of trusted authorities, RSUs and the vehicles.

- The trusted authorities are responsible for the registration of the vehicle and for embedding the public security parameters and public keys in the vehicles OBU. The KGC is responsible for the generation of keys to the network entities. Trusted authorities directly monitor the RSUs and can detect any faulty RSU.

- Next, RSUs monitor the vehicles under their range and allocate pseudonyms to them. RSUs communicate with trusted authorities and other RSUs via internet backbone and with the vehicles via short range wireless communication. RSUs can detect the malicious vehicles under its range and inform the other entities about the misbehaving vehicles.

- The vehicles communicate with each other via wireless channel 802.11p for vehicular safety. The vehicles constitute OBUs, capable of computation and communication fa-

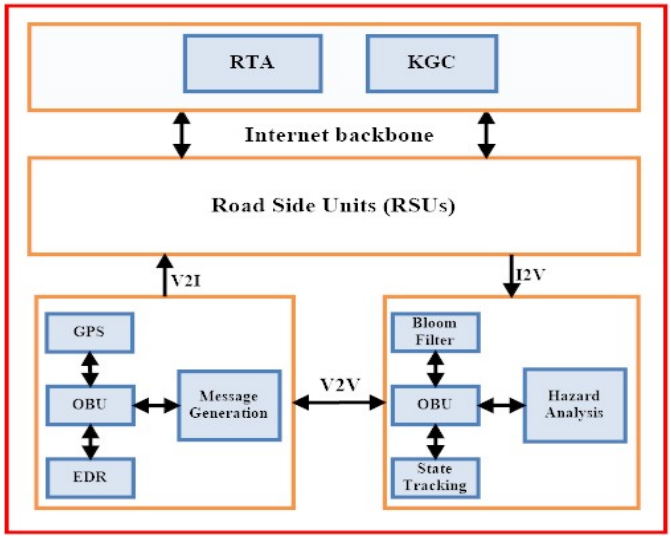

Figure 4.3: Network design architecture

cility along with the various units as Event Data Recorder (EDR), Tamper Proof Device (TPD), Global Positioning System (GPS) for determining the location of the vehicle along with its neighbours and bloom filter for fast and efficient message verification.

4.2 The Proposed Scheme

In the proposed scheme, the anonymous authentication is achieved along with security requirements of authentication and non-repudiation. Firstly, the vehicle registers itself to the trusted authorities and the security public parameters and the keys are allocated to the vehicle by the trusted authorities. Then, the RSUs are used to allocate the pseudonyms to the vehicle for anonymous communication with other vehicles in its range. The inter-vehicle communication takes place by authenticating each other through the digital signatures generated while the messages in V2I communication are signcrypted with the help of identity based cryptography. In V2I communications, the messages are signed as well as encrypted. The various notations used in our scheme are defined in Table 4.2.

Table 4.2: The various notations used in the proposed security scheme

Notation	Description
ID	The identity of vehicle
QID	The pseudo-identity allocated by the RTA
λ	The master key of RTA
P_{rta}	The public key of RTA
s	The master key of KGC
P_{pub}	The public key of KGC
x	The secret key of vehicle
P_v	The public key of the vehicle
pp	The partial private key of vehicle
M	The message space
Y_i	The private keys of RSU_i
P_{rsu_i}	The public keys of RSU_i
PS1+PS2	The pseudonym allocated to the vehicle
T_h	H_3(PS1)
h	$H_2(m, PS1, P_v, U)$
σ	The signature generated for inter-vehicle communication
SIG(m;k)	ID-based signature generated on m with key k
$E_{P_{rsu_i}} < m >$	The message m encrypted with the public key of RSU_i
$E_{P_{rsu_i}} < m, SIG(m;k) >$	The signcryption of message m with ID based cryptography
T	Timestamp used
loc	Location coordinates

4.2.1 System Setup

The scheme uses the set of publicly known security parameters (Table 4.3) which are embedded in the vehicles onboard at the time of purchase of the vehicle. The system public parameters are params = $\mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_2, H_3$. The vehicle's owner registers its details to the trusted authority when the vehicle is purchased and the vehicle is allocated an ID which is mandatory before the vehicle is driven on roads. The P_{rta} is the public key of the Regional Transportation Authority (RTA) under whose region the vehicle is registered. The vehicle consists of tamper proof hardware which is password protected *i.e.* only the authorised person will be able to activate the credentials of the vehicle. Moreover, the tamper proof devices are used i.e. if anyone tries to tamper with the inner credentials of the system, an automatic alarm will be generated.

The scheme uses the identity based cryptography proposed by A. Shamir [29] for V2I communication and signature scheme is generated onboard of the vehicle for V2V commu-

Table 4.3: Publicly known security parameters

Notation	Description
$\mathbb{G}_1$	Additive group of prime order q
$\mathbb{G}_2$	Multiplicative group of prime order q
$e : \mathbb{G}_1 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_2$	Bilinear pairing
$P \in \mathbb{G}_1$	P is the generator of group $\mathbb{G}_1$
P_{pub}	Public key of KGC
H_2	$H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$
H_3	$H_3 : \{0,1\}^* \longrightarrow \mathbb{Z}_q^*$

nication. The scheme uses the ID based signature scheme and Boneh and Franklin [252] ID based encryption scheme for V2I communication.

4.2.2 Initial Registration Phase

The vehicles register themselves to the RTA by sending their ID to the RTA which are allocated to them at the time of purchase of the vehicle. The trusted authority forwards the list of vehicles IDs from its database to RTA beforehand. So when the vehicle sends the request for registration with the RTA, it checks the ID in its database. If the ID exists, RTA registers the vehicle and allocates pseudo-identity to the vehicle which is to be used for all the communications in the network. Thus, the actual identity of the vehicle is concealed and only RTA can map the relationship between QID and ID. RTA chooses the distinct hash function $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$ and master key is randomly chosen as $\lambda \in_R \mathbb{Z}_q^*$ and public key $P_{rta} = \lambda.P \in \mathbb{G}_1$.The vehicle after receiving the signcrypted message $E_{P_v} < T, QID, SIG(QID, T; \lambda) >$ decrypts the message with its secret key x and verifies the signature with the public key P_{rta} of RTA. Now the vehicle uses its pseudo-identity QID for the communication in the network. Next, Key Generation Centre (KGC) chooses the master key as $s \in_R \mathbb{Z}_q^*$ at random and calculates its public key as P_{pub} = s.P $\in \mathbb{G}_1$. The public key of KGC is communicated to RTA. The RSUs also authenticate themselves to the trusted authority to ensure that these are not tampered by the external attacker. Each RSU under the control of RTA uses its location

$< loc >$ and its ID to calculate the Public key (P_{rsu}) where:

$$P_{rsu} = b.P \tag{4.1}$$

and b= $H_2(ID, loc)$.

The RSU transmits and authenticates its public key to KGC, corresponding to it the private key of RSU is calculated $Y = s.P_{rsu}$ by KGC and it is sent to the RSU via secure channel of Ethernet. The list of public keys of RSUs is also transmitted to RTA. RTA broadcasts the public key of KGC as P_{pub} to all the vehicles and also sends the public keys of all the RSUs which are registered to KGC.

Algorithm 4.1 Registration phase executed by vehicle

Require: $params = \mathbb{G}_1, \mathbb{G}_2, e, P, P_{rta}, H_2, H_3$

1: Choose $x_i \in_R \mathbb{Z}_q^*$ which is selected as the secret key of vehicle.
2: Compute public key as P_v = x.P $\in \mathbb{G}_1$.
3: Vehicle sends message to RTA as $E_{P_{rta}} < T, ID, P_v > \longrightarrow RTA$

$$< T, P_{pub}, P_{rsu_1}, P_{rsu_2}, P_{rsu_3}, ...P_{rsu_n}, SIG(P_{pub},$$

$$P_{rsu_1}, P_{rsu_2}, P_{rsu_3}, ...P_{rsu_n}, T; \lambda) > \longrightarrow * \tag{4.2}$$

The public key of KGC and all RSUs is broadcasted to all the vehicles. The vehicle receives the message and verifies the signature to check the validity of the message.

Algorithm 4.2 Registration of vehicle by RTA

Require: $E_{P_{rta}} < T, ID, P_v >$

1: Decrypts the message with master key λ of RTA
2: Computes $QID = H_1(ID) \in \mathbb{G}_1$.
3: Store the mapping $< ID, QID >$ in the database.
4: Store the mapping of $< QID, P_v >$ in the database.
5: It sends the message to vehicle as: $E_{P_v} < T, QID, SIG(QID, T; \lambda) >$

4.2.3 Key Generation Phase

The vehicle generates the secret key x and public key P_v onboard but the vehicle needs to authenticate the public key to KGC. KGC also generates the partial private key for the vehicle which is required for the signature generation in inter-vehicular communication. The vehicle sends the request for partial private key encrypted with the public key of KGC P_{pub}.

$$E_{P_{pub}} < QID, T, loc, P_v > \longrightarrow KGC \tag{4.3}$$

After receiving the request, KGC decrypts the message and verifies the mapping between P_v and QID which it has received from RTA. If the mapping is correct, it generates the partial private key for the vehicle as pp = s.QID which is transmitted to the vehicle encrypted with the public key of vehicle.

$$E_{P_v} < pp, T, SIG(pp, T; s) > \longrightarrow vehicle \tag{4.4}$$

The vehicle checks the correctness of the signature by checking whether $e(pp_i, P) = e(QID_i, P_{pub})$ which can be verified as:

$$e(pp_i, P) = e(sQID_i, P) = e(QID_i, sP) = e(QID_i, P_{pub}) \tag{4.5}$$

Algorithm 4.3 Partial private key generation

1: Vehicle sends the request to KGC as $E_{P_{pub}} < QID, T, loc, P_v >$
2: KGC verifies the mapping of P_v and QID
3: KGC computes pp = s.QID where pp is the partial private key of vehicle
4: KGC sends partial private key to vehicle as $E_{P_v} < pp, T, SIG(pp, T; s) >$
5: Vehicle verifies if $e(pp_i, P) = e(QID_i, P_{pub})$

4.2.4 Pseudonym Allocation Phase

The inter-vehicular communication needs to be secure and anonymous but the messages should be authenticated at the same time. There is need of additional layer of abstraction in the communication phase which disrupts the linkability of the messages due to the changing pseudonyms as the pseudonyms are updated when the vehicle reaches the range of next RSU. As the vehicle reaches the range of particular RSU, it requests for pseudonyms from RSU and RSU allocates the pseudonyms to the vehicle which are used for communication. When the vehicle enters the region of RSU, it sends the message

$$E_{P_{rsu}} < T, loc, P_v, SIG(T, loc, P_v; x) > \longrightarrow RSU \tag{4.6}$$

RSU, after receiving the message, decrypts it with the private key of RSU. The RSU checks the database for the mapping between P_v and QID. The mapping database is transmitted from the RTA to all the RSUs. After checking the databases, RSU correlates received P_v with QID. The checking is done in O(1) search time. The RSU sends the QID to the vehicle to give the proof of its authenticity.

$$E_{P_v} < T, loc, P_v, QID, P_{rsu}, SIG(QID, T, loc, P_v; Y) > \longrightarrow vehicle \tag{4.7}$$

The vehicle decrypts the message using its secret key x and verifies the signature to get the QID. If QID received is accurate, it implies that the RSU is authentic. Now the vehicle sends the message to RSU requesting for pseudonym.

$$E_{P_{rsu}} < QID, T, loc, P_v, SIG(QID, T, loc; x) > \longrightarrow RSU \tag{4.8}$$

The RSU receives the message, decrypts it and verifies the signature. Then it generates the pseudonym for the vehicle and transmits them to the vehicles as

$$E_{P_v} < PS1, PS2, T, SIG(PS, T; Y) > \longrightarrow vehicle \tag{4.9}$$

$$< PS1, T, P_{rsu}, SIG(PS1, T; Y) > \longrightarrow * \tag{4.10}$$

RSU at the same time broadcasts the pseudonym to all the vehicles which are in range of RSU. The schematic of all the steps in the registration, key generation and pseudonym allocation phases are depicted in Table 4.4.

4.2.5 Anonymous Communication

After the completion of initial registration, key generation and pseudonym allocation; the communication among the vehicles in the network takes place. The communication is considered as broadcast communication among the vehicles where the vehicles periodically send the location and state information to its neighbouring vehicles in every 300ms. Then, the vehicles can communicate with the RSUs to transmit some messages or to send the network information and transmit the state information. RSUs can send the important network related information to the vehicles regarding the revoked vehicles, misbehaving vehicles or any other crucial information. Moreover, in case of some emergency situations, the safety messages are transmitted among the network entities to report some critical situation and such type of messages should be given higher priority while verification and appropriate action should be taken in the bounded time. Therefore, the flags are set while communicating the messages to differentiate between different types of messages. The safety messages should be given the highest priority followed by the messages from RSUs and the lowest priority to the periodic beacons.

Table 4.4: Schematic of registration, key generation and pseudonym generation phases

Vehicle	RSU	KGC	RTA
params = $\{\mathbb{G}_1, \mathbb{G}_2, e, P, P_{rta}, H_2, H_3\}$ 1.Choose $x_i \in_R \mathbb{Z}_q^*$ as the secret key of vehicle 2.Compute public key as P_v = x.P $\in \mathbb{G}_1$ 3.Vehicle sends message to RTA as: $C_1 = E_{P_{rta}} < T, ID, P_v > \longrightarrow$ RTA			
			4.Decrypts C_1 with secret key λ of RTA 5.RTA chooses the distinct hash function $H_1 : \{0,1\}^* \longrightarrow \mathbb{G}_1$ 6.Computes QID = H_1(ID) $\in \mathbb{G}_1$ 7.Store the mapping $< ID, QID >$ in database 8.Store the mapping of $< QID, P_v >$ in database 9.It sends the message to vehicle as: $C_2 = E_{P_v} < T, QID, SIG(QID, T; \lambda) >$ 10.Sends the mapping of $< QID, P_v >$ to RSU and KGC
11.Decrypts C_2 and verifies the signature with x and P_{rta} respectively			
	12.Sends the public key $P_{rsu} = H_2$ (ID, loc).P		
		13.Receives the public key of RSU 14.The RSU private key $Y = s.P_{rsu}$ is sent to RSU 15.KGC sends the list of public keys of RSUs to RTA	
			16.RTA broadcasts list of public keys of RSU and public key of KGC to vehicles
17.Vehicle sends the request to KGC as: $C_3 = E_{P_{pub}} < QID, T, loc, P_v >$			
		18.Decrypts C_3 with master key s 19.KGC verifies the mapping of P_v and QID 20.Computes partial private key as pp = s.QID 21.KGC sends pp to vehicle as: $E_{P_v} < pp, T, SIG(pp, T; s) >$	
22.Decrypts pp and verifies the signature with the keys x and P_{pub} respectively 23.Verifies if e(pp_i, P) = e(QID_i, P_{pub}) 24.It sends $C' = E_{P_{rsu}} < T, loc, P_v, SIG(T, loc, P_v; x) >$ to RSU			
	25.Decrypts C' and verifies the signature with the keys Y and P_v respectively 26.Checks the mapping of P_v and QID 27.$C'' = E_{P_v} < T, loc, P_v, QID, P_{rsu} SIG(QID, T, loc, P_v; Y) >$ to vehicle		
28.Decrypts C'' and verifies the signature with the keys x and P_{rsu} respectively 29.$C_4 = E_{P_{rsu}} < QID, T, loc, P_v, SIG(QID, T, loc; x) >$ to RSU			
	30. Decrypts C_4 and verifies the signature with the keys Y and P_v respectively 31.PS = PS1 + PS2 32.Sends $C_5 = E_{P_v} < PS1, PS2, T, SIG(PS, T; Y) >$ to vehicle		
33.Decrypts C_5 and verifies the signature with the keys x and P_{rsu} respectively			

Safety message $>$ I2V/V2I $>$ V2V

So, the flags are set for each type of message, F=0 for V2V communication, F=1 for V2I or I2V communication and F=2 for safety messages

Safety Messages

The vehicle sends the safety messages in case of the emergency situations and the message is broadcasted to all the network entities in its range.

$$< 2, m, T, loc1, loc2, P_v, PS1, \sigma) \longrightarrow * \tag{4.11}$$

Here the flag 2 indicates the safety message, m is the safety message to be transmitted, T is the timestamp, loc1 is the location of sender, loc2 is the location of the emergency event, σ is the signature generated by the sending vehicle on the message with the secret key x and partial private key pp of the sending vehicle.

V2I/I2V messages

The vehicle to infrastructure communication is described as:

$$E_{P_{rsu}} < 1, m, T, PS1, loc, SIG(m, T, PS1, loc; x) > \longrightarrow RSU \tag{4.12}$$

The RSU receives the message and decrypts it with the private key Y of RSU. Then the RSU verifies the message and checks for its validity. The flag value of 1 indicates the vehicle to RSU or RSU to vehicle communication. Next the RSU uses the ID based signature and ID based encryption for communicating with vehicles.

$$E_{P_v} < 1, m, T, P_{rsu}, loc, SIG(m, T, loc; Y) > \longrightarrow vehicle \tag{4.13}$$

The vehicle decrypts the message with its secret key x and verifies the signature with P_{rsu}, the public key of RSU .

V2V message broadcast

The V2V communication takes place with flag value set to 0, which indicates the lowest priority assigned to periodic beacons which are broadcasted by the vehicles to their neighbours every 300 ms. The messages are signed by the vehicles before these are broadcasted to its neighbours. Suppose the vehicle V broadcasts its state and location information to its neighbours every 300ms. Now, the vehicle V wants to broadcast the information to its neighbours, the message it wants to send must be signed by the vehicle before it is transmitted to ensure the authenticity of the messages. The ID of the vehicle is never revealed to anyone to preserve the anonymity of the vehicle. Therefore, the pseudonyms are used for establishing the communication so that the private information should not be disclosed to anyone but at the same time messages should not be linked with each other to allow the attacker to get the information about the network. To prevent tracking and linkability, pseudonyms are updated as the vehicle enters the region of next RSU. The pseudonyms are prevented from being updated multiple times in the region of same RSU to prevent the signaling overhead problem leading to the congestion of network as more bandwidth will be consumed if pseudonyms are updated after every single message. The signature generation process is started by the vehicle V. The message m $\in$ M is signed using the partial private key and private key pair (x, pp) with vehicle identity QID and public key P_v, using the *Sign* algorithm as discussed in section 3.2. The output of the signature on m is generated as σ = (U, V). The message is broadcasted to the other vehicles in its neighbourhood as:

$$< 0, m, PS1, P_v, T, loc, \sigma > \longrightarrow * \tag{4.14}$$

All the neighbours in the range of vehicle V receives the message signed by vehicle V. The algorithm $Verify$ is used to verify the signature σ = (U, V) signed by the vehicle V with

pseudonym PS.

4.2.6 Aggregate Message Verification

This module allows the vehicle to verify n different signatures from various vehicles. The batch verification should be performed at a rate higher than the vehicles can broadcast the messages. The algorithms *Aggregate* and *AggregateVerify* are used to aggregately sign and verify the signatures respectively.

Invalid Signatures in the Aggregate Scheme

If any of signatures in the batch is invalid, then equation 3.2 will not hold and the whole messages will be rejected. This is not recommended as most of the signatures in the batch can be valid and accepted. Thus, a binary search technique is opted in our scheme to enhance the aggregate scheme. The vehicle needs to verify n signatures aggregately. If the aggregate signature verification fails, the mid of the list is located and aggregate verification equation is applied to first half of the list and the second half of the list. Further, if any of the lists causes failure, the process is repeated until there is one element in the list or certain threshold limit is reached.

4.3 Proposed Security Framework for VANETs

The framework for message generation and verification process is described in Figure 4.4. The MAC addresses of the received vehicles are checked by the bloom filter1 and if the results are verified, then the pseudonyms generated by RSU are checked in bloom filter2 and the results are stored in database. The MAC address verifier and the bloom filter1 are encapsulated from the application layer where bloom filter2 is located. The EDR unit is also

encapsulated from the application layer of the vehicle. The ID based cryptography is used for the V2I/I2V communication where ID is evaluated by ID evaluator unit which verifies the ID of the vehicle with the help of generated pseudonyms by the RSU. The encryption and decryption processes are carried out by the vehicles for the communication with infrastructure. The computing platform performs the required computation needed for the digital signature generation and verification processes. The digital signature generator performs the signature generation procedure and digital signature verifier performs the signature verification from the other vehicles in collaboration with the information collected from the log 1. The information is stored in the database log. The anonymizer uses the pseudonyms to provide the anonymity to the vehicle while communicating. The vehicle may receive the plenty of messages from the neighbouring vehicles which need to be verified before the other vehicles can broadcast new updated beacons. The number of messages increases considerably in the urban scenario; so there is an urgent need to increase the message verification process so that the vehicles should be able to verify the messages before the new updated messages are received. Therefore, we employ the use of bloom filter in this scheme to enhance the speed of message verification process.

4.3.1 Bloom Filter

Bloom filter is a space efficient data structure which is used to check the membership of an item *i.e.* whether the item is a member of a set or not [59]. It employs the use of multiple hash functions for storing the data in a large m bit array. It is space efficient as it can store the m elements in m bit array. It reduces the search time complexity from O(n) to constant time. The search time complexity depends on the size of bloom filter and the number of hash functions (k) used. Bloom filter of size n consists of an array of m bits $b_1, b_2, b_3 ... b_m$ which are all initialized to zero. The set of elements $s_1, s_2, s_3 ... s_n$ are represented using the bloom

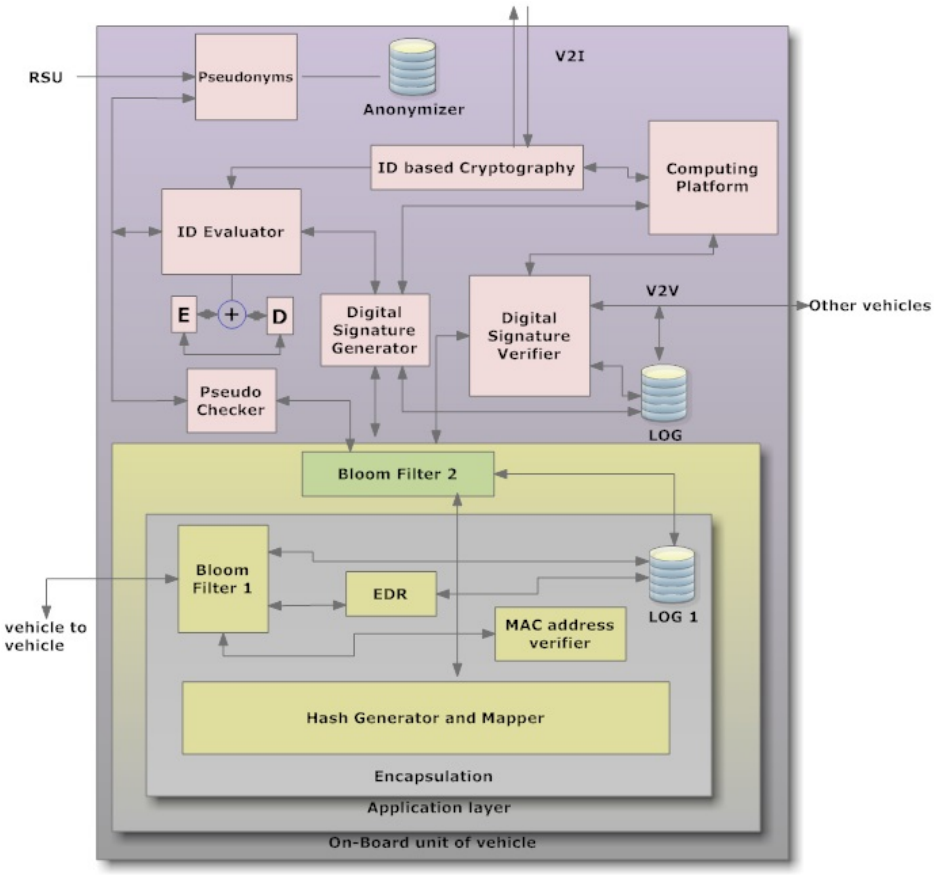

Figure 4.4: Framework for message generation and verification process

filter. The filter uses the k independent hash functions $h_1, h_2, h_3 ... h_k$ which returns the value between 1 and m. When any element is added for membership, the element s_i is hashed through all the k hash functions and the corresponding bits in the bloom filter are set to 1. If any of the bit in the array corresponding to the k value is already set 1, it is left as unchanged. When any element is checked for membership query, the element is hashed by all the k hash functions and corresponding bits are checked. If all the bits corresponding to the k values are 1, the element is a member of the set. The important property of bloom filter is that there are no false negatives but there may exist false positives. The false positive exists when an element x has all the elements corresponding to the k hash functions as set to 1, although the element is not actually a member of set. Thereupon, to choose the size of bloom filter, the steps used are:

- Choose a value for n
- Choose a value for m
- The optimal value of k = ln 2.$(\frac{m}{n}) \approx 0.69(\frac{m}{n})$ (calculated from analysis in [253]).
- Calculate the error rate for the chosen values of n, m, and k. The false positive rate will be approximately $(1 - e^{-kn/m})^k$
- If it is unacceptable, return to step 2 and change m;

4.3.2 Utility of Bloom Filter

Bloom filter is a space efficient data structure which utilizes only 1 bit for storage of single entity. Therefore, it gives the advantage of storing multiple entities in the database by utilizing small amount of space. The proposed security framework uses two bloom filters BF_1 and BF_2 to check the MAC addresses and pseudonyms of the incoming messages respectively and if these entities are already stored in the bloom filter, then the messages are directly accepted from that senders. It indicates that the senders are already authenticated by the receiver. If the incoming entity does not match with the entry stored in bloom filter, then the sender of the incoming message is verified by the aggregate verification equation. Thus, a lot of computation overhead is reduced as the receiver need not to authenticate the message signatures from the same sender again and again. The signature verification time is greatly reduced by this approach leading to increase in efficiency of vehicular communications in the network.

When any message is received by vehicle, the bloom filter BF_1 checks MAC address for the incoming message. The MAC address bloom filter is located in the data link layer and its details are hidden from the application layer (Figure 4.5). If the MAC is not matched with entry in the bloom filter, the message is sent for verification. If the signature verification is

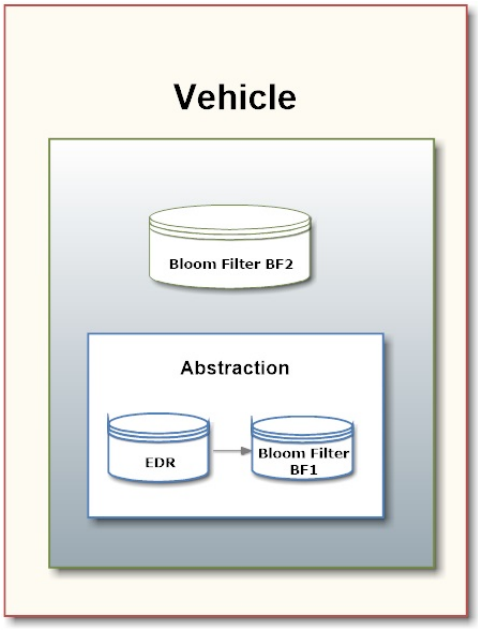

Figure 4.5: Bloom filters BF_1 and BF_2 in vehicle

valid, the MAC address corresponding to that identity is added in the bloom filter BF_1. If the MAC address is already stored in the bloom filter, then the corresponding pseudonym is checked in second bloom filter BF_2 which is at the application layer. If the pseudonym exists in the bloom filter, the message is accepted and if the pseudonym does not exist, the message is sent for verification. If it holds the verification equation, the pseudonym is added to the bloom filter, otherwise the message is discarded. All the messages whose pseudonyms do not exist in the bloom filter are aggregately verified and those pseudonyms are added to the bloom filter whose signatures are valid. For a particular bloom filter of size m bits; when the hash functions are applied on the input x, $hash_i(x)$ returns the value between 1 and m. The probability that a single bit is set to 1 after applying a single hash function is $\frac{1}{m}$, hence, the probability that a particular bit is 0 is (1-($\frac{1}{m}$)). The probability that a bit remains 0 after applying k hash functions is $(1-(\frac{1}{m}))^k$. The probability that the bit remains 0 after the n elements are processed is $(1-(\frac{1}{m}))^{kn}$. The probability that the bits are 1 after applying k hash functions after processing all the n elements is $(1-(1-(\frac{1}{m}))^{kn})$. The probability that

the particular bits are set to 1 after applying k hash functions without the element being actually present is

$$P = (1 - (1 - (\frac{1}{m}))^{kn})^k \tag{4.15}$$

$$P \approx (1 - e^{\frac{-kn}{m}})^k \tag{4.16}$$

The expression $(1 - e^{\frac{-kn}{m}})^k$ is minimized when k = $ln2.(\frac{m}{n}) \approx 0.69 \times (\frac{m}{n})$ Thus the probability can be calculated as:

P = $(1 - e^{\frac{-kn}{m}})^k$

= $(1 - e^{\frac{ln2.mn}{mn}})^k$

= $(1 - e^{ln2})^k$

= $(\frac{1}{2})^k = (\frac{1}{2})^{(0.69 \times \frac{m}{n})}$

$$P = 0.6198^{(\frac{m}{n})} \tag{4.17}$$

Similarly, the probability for the second bloom filter can be calculated as $0.6198^{(\frac{r}{q})}$ where r is the size of bit array for BF_2 which is equal to m and q is the number of entities processed by BF_2 which is equal to n because entities processed by BF_1 will be processed by BF_2. Thus, the total error probability for any false positive to occur is:

$$\mathbb{P} = 0.6198^{(\frac{m}{n} + \frac{r}{q})} \tag{4.18}$$

The false positive error probability is greatly reduced by using the two bloom filters leading to more accurate results as the number of elements in the bloom filters increase. The mes-

sages corresponding to the identities which already exists in the bloom filters BF_1 and BF_2, need not be verified. So, these identities are assumed to be trusted and there is no need to verify the signatures from these entries again. However, the case may be considered where messages from the already existing entries may be invalid, so some messages from already existing pseudonyms in BF_2 need to be verified. Moreover, we need to take into consideration false positive error probability. Therefore, even though the identities have checked their membership in the bloom filters, still there is requirement to verify some messages randomly with some probability to deal with the false positive error rate and small ratio of vehicles which are assumed to be dishonest. The entries checked for membership in bloom filter BF_1 are passed to BF_2. So in BF_2, signatures corresponding to few pseudonyms which already exist in the bloom filter are verified with some probability.

4.4 Evaluation Methodology

Suppose there are V_n vehicles in the range of RSU. Then the total number of messages generated in the region of RSU is considered as T_d. One vehicle can generate m messages in 1 sec. Therefore, the total number of messages, T_{mn} , generated by all the vehicles in the range of single RSU are:

$$T_{mn} = (V_n \times m) messages. \tag{4.19}$$

Total number messages generated in time limit T_l is V_{mnl} given as:

$$T_{mnl} = (V_n \times m \times T_l) messages \tag{4.20}$$

Now, T_{rec} = total number of messages received by the vehicle in time T_l. Probability for verifying the signatures randomly form the list of pseudonyms which already exist in bloom

filter BF_2 is considered as P_{ver}.

$$P_{ver} = \frac{T_{rec}}{T_{mnl}} \times \frac{T_{ids}}{T_{ver}} \times \mathbb{P} \tag{4.21}$$

Where $\mathbb{P}$ is false positive error probability, T_{ids} is the total number of vehicles from which messages are received and T_{ver} is the number of vehicles whose entries already exist in bloom filter BF_2.

$$P_{ver} = \frac{T_{rec} \times 0.6198^{(\frac{m}{n}+\frac{r}{q})}}{(V_n \times m \times T_l)} \times \frac{T_{ids}}{T_{ver}} \tag{4.22}$$

The expected number of pseudonyms whose signatures are randomly verified with probability P_{ver} are E_x:

$$E_x = E_{exists} \times P_{ver} \tag{4.23}$$

$$E_x = E_{exists} \times \frac{T_{rec} \times 0.6198^{(\frac{m}{n}+\frac{r}{q})}}{(V_n \times m \times T_l)} \times \frac{T_{ids}}{T_{ver}} \tag{4.24}$$

where E_{exists} is the total number of pseudonyms which already exist in the bloom filter BF_2. Thus, E_x calculates the number of pseudonyms from the already existing pseudonyms in the bloom filter, corresponding to which the signatures need to be verified at random. There may be a scenario where a malicious vehicle injects false messages in the network and number of messages injected may be tremendously large that it may consume the bandwidth of the network and lead to congestion. So this type of situation needs to be tackled by the vehicles and RSU. When the messages are received by the vehicle, the counter is initialized. When the message is received from particular pseudonym, the counter is incremented by one. As the number of messages with particular pseudonyms goes on increasing, the counter keeps incrementing. As the counter value of particular pseudonym crosses the threshold value of m, the particular pseudonym is added to the list of the suspicious vehicles and the information

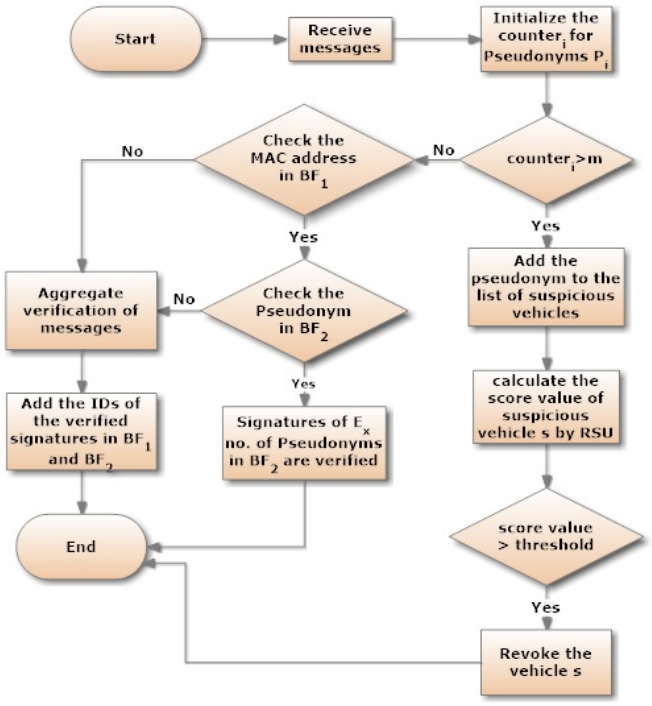

Figure 4.6: Flowchart for message verification process

is sent to the RSU. RSU calculates the score value of the suspicious vehicle 's' as:

$$S = \|1 - \frac{1}{V_s^2}\| \tag{4.25}$$

Where V_s is the number of vehicles who report the vehicle s as the suspicious vehicle. The score value of the suspicious vehicle is also communicated to neighbouring RSUs along with the pseudo identities QIDs of the suspicious vehicles. As more vehicles report of the suspicious vehicle, the score value is updated by the RSU as:

$$S_c = \begin{cases} S_p; & if\ s\ is\ not\ in\ history \\ S_p + \|1 - \frac{1}{V_s^2}\|; & if\ s\ is\ in\ history \end{cases} \tag{4.26}$$

If the value of $S_c \geq$ threshold; the particular suspicious vehicle s is revoked and all the vehicles and authorities are informed that the credentials of that particular vehicle are can-

celled. Figure 4.6 gives the flowchart for the message verification process of vehicle.

Algorithm 4.4 To check suspicious vehicle

Require: $Counter_i$ is initialized to 0;
  while the pseudonyms P_i from i $\leq$ n for each pseudonym P_i received **do**
    $counter_i++$;
    if $counter_i \geq m$ **then**
      add it to the list of suspicious vehicles and reports to RSU;
      stop receiving messages with pseudonym P_i;
    end if
    i=i+1
  end while
  RSU computes score value as: S = $\|1-\frac{1}{V_s^2}\|$
  If s is not in history
  $S_c = S_p$;
  If s is in history
  $S_c = S_p + \|1-\frac{1}{V_s^2}\|$;
  If $S_c \geq$ threshold
  s is revoked and all network entities are informed

4.5 Security Analysis

The proposed framework intends to provide the security requirements of authentication, anonymity, integrity, location assurance, non-repudiation and traceability. The security considerations which can be achieved through the proposed framework are:

I Authentication: The authentication is achieved by employing the digital signatures in V2V communication as well as by employing ID based signatures in I2V communication. The RSU sends message signed with an ID based signature $< 1,m,T,loc,SIG(1,m,T,loc;Y) >$ to vehicle. Vehicles send message $< 1,m,T,loc,\sigma > \longrightarrow$ RSU and $< 0,m,T,loc,\sigma > \longrightarrow$ vehicle. Thus each and every message is digitally signed before it is communicated in the network. Suppose the vehicle has generated the signature on any message m with its key pair (x,pp,P_v) with

pseudonym PS. The digital signatures bound the message to particular public key and the pseudonym. Thus, the receiver will have the pseudonym as well as public key of the sender. If the message is intended to be false, the pseudonyms can be easily used by the higher authorities to track the actual identity of the sender.

II Anonymity: The private and anonymous communication is the foremost requirement of vehicular networks so that the private information of the vehicle cannot be used for tracking. Therefore, in the proposed scheme the anonymity of the vehicles is achieved but at the same time, the vehicle should be traceable by the law enforcement authorities. Firstly, the ID allocated to the vehicle is registered to RTA and in correspondence to it, pseudo identity QID is allocated to the vehicle by RTA. The vehicle sends the ID encrypted with public key of RTA as $E_{P_{rta}} < T, ID, P_v > \longrightarrow$ RTA. RTA verifies the ID and assigns pseudo identity QID to vehicle and sends signcrypted message as $E_{P_v} < T, QID, SIG(QID, T; \lambda) > \longrightarrow$ vehicle. Then this pseudo identity QID is used for allocation of pseudonyms by RSU. When the vehicle enters the region of particular RSU, it authenticates its QID to RSU by sending $E_{P_{rsu}} < QID, T, loc, P_v, SIG(QID, T, loc; x) >$ to RSU. The RSU authenticates the QID of vehicle and assigns the pseudonym PS=PS1+PS2 to the vehicle $E_{P_v} < PS(PS1 + PS2), T, SIG(PS, T; Y) >$. Further, the layer of abstraction is added by using PS1 for communication in the network and PS2 is kept private with the vehicle. When the authorities want to trace the malicious vehicle, they can track the pseudonym PS1 from the signature which can be used to locate the corresponding QID from the RSU as RSU keeps the record of allocated PS1s and PS2s to the vehicles. The corresponding QID will be submitted to RTA to find the actual ID of the vehicle which is submitted to TA to find all the personal registration information.

III Integrity: The message integrity is of prime importance to safety messages and messages from RSUs. Thus, the communication messages between RSU

and vehicle are encrypted before sending as $E_{P_{rsu}}$ <1, m, T, PS1, loc, SIG(m,T,PS1,loc;x)>$\longrightarrow$ RSU and $E_{P_v} < 1, m, T, P_{rsu}, loc, SIG(m, T, loc; Y) > \longrightarrow$ vehicle. The safety messages are firstly sent to RSU for authentication as $E_{P_{rsu}} < 2, m, T, PS1, loc1, loc2, SIG(m, T, PS1, loc1, loc2; x) > \longrightarrow$ RSU and then the safety messages are broadcasted in the network. Therefore, the messages with flags 1 and 2 are critical messages and the integrity of these messages is important. These are encrypted with the public keys of the receiver before sending so that any attacker may not forge and alter the message. The message is encrypted with the public key of the receiver so the adversary will not be able to decrypt the message as it does not possess the private key of the receiver.

IV Location assurance: The messages communicated in the network include the location information and timestamp to prevent the location based attacks such as wormhole attacks [121] and sinkhole attacks [254]. The messages $< 1, m, T, loc, \sigma > \longrightarrow$ RSU and $< 0, m, T, loc, \sigma > \longrightarrow$ vehicle has the location information in them which is located by using Global Positioning System (GPS) in vehicles to get the accurate locations. The more accurate system DGPS [255] is used which gives the error of only few centimetres in retrieving the location coordinates. Moreover, the RSUs use the location based public keys for identity based cryptography and the messages can only be verified using the location information of the RSU. Thus, it is difficult for an attacker to act as fake RSU as the location information of RSU is firstly authenticated by RTA.

V Traceability: The vehicle cannot be traced based on its identity as the pseudonyms are used for communication among network entities and these pseudonyms allocated to vehicles are updated as the vehicle enters the region of next RSU. Thus the pseudonyms keep on changing as the range of next RSU begins. Hence, the vehicles cannot be traced based on pseudonyms. On the other hand, the authorities can trace the vehicles

if required. The law enforcement authorities can trace the malicious vehicle by locating the pseudo identity QID corresponding to PS_m of the malicious vehicle and then the QID is sent to all the RSUs and the current PS_c allocated to the vehicle is located which is broadcasted to all the vehicles in that RSU region and the communication with that PS_c is halted and all the RSUs are informed not to allocate the pseudonyms to the vehicle with pseudo identity QID. After locating the QID, it is submitted to RTA to find the actual ID of the vehicle and finally, the credentials of that vehicle are revoked. Thus, the single authority can not reveal the identity of the vehicle.

VI Revocation: The malicious vehicles which are responsible for sending false information need to be revoked. The vehicle cannot identify if the information transmitted to it is false or not. The RSU calculates the score value of the suspicious vehicles according to the responses received from the vehicles by the equation S = $\|1 - \frac{1}{V_s^2}\|$. Further, S is updated as $S_c = S_p + \|1 - \frac{1}{V_s^2}\|$ if s is in history otherwise; it remains same. If the calculated value $S_c >$ threshold, the suspicious vehicle is revoked and the revocation information is sent to all the vehicles in its range. Thus, the actual identity is identified by first locating the QID from the RSU and then ID from RTA and all the vehicle information from TA. Other criterion is that the vehicle can detect the false information from the forged signatures or the tampered message if the verification equation fails from the vehicle with pseudonym PS_m. In that case, the vehicle may directly send the message to RSU to revoke the vehicle and thus, the vehicle with pseudonym PS_m is revoked by the RSU and the information is sent to all the vehicles in the region to halt the communication with that vehicle possessing pseudonym PS_m.

4.6 Conclusion

A novel privacy preserving pseudonymous based security framework is designed which employs the use of bloom filters in message verification process. A new digital signature scheme is designed for inter-vehicular communication allowing the vehicles to anonymously communicate with each other. Aggregate signature verification is proposed and the bloom filters are used to enhance the verification process by preventing the message drop in case of busy traffic hours. The analysis of the security scheme is done with various parameters on the simulated environment in the next chapter.

Chapter 5

Experiments and Implementation Details

The experiments are performed to test the proposed certificateless signature scheme and the proposed security framework to test its applicability in the vehicular ad hoc networks. The implementation details are included to show the practicability of the proposed scheme.

5.1 Results Analysis

Firstly the proposed certificateless aggregate signature scheme is compared with the already existing signature schemes to prove its feasibility. One of the important parameter is that the aggregate signature verification time need to be reduced when compared with other existing schemes. In practice, element size in group $\mathbb{G}_1$ can be reduced by a factor of 2 using the various compression techniques. The certificateless aggregate signature scheme proposed here is a short CLAS scheme like BLS signature scheme [18]. Elliptic curve are used to choose the group and bilinear map resulting in a group size of 160 bits and thus, the signatures generated by this scheme are of length 160 bits approximately (half-size comparing to other proposed CLAS schemes). Therefore, the proposed scheme is much more efficient in terms of bandwidth which is a must requisite for the bandwidth limited VANETs. The comparison

of the computational costs of the proposed scheme and the computational costs of already existing schemes [41, 174, 256] is made.

Table 5.1 gives the detailed comparison of the proposed scheme with other schemes based on type, sign cost, verify cost and aggregate verify cost. The major goal is to reduce the signature verification cost to enhance the signature verification process. Here, the two main operations are considered on the basis of which comparison is made, scalar multiplication(S) in $\mathbb{G}_1$ and pairing operation(P). The pairing operation is the most costly operation, so there is need to minimize the pairing operations. The scheme presented by Zhang *et al.* [41] takes (n+3) pairing operations for signature verification process, thus the pairing operations increase linearly as the number of signatures increase. The scheme by Zhang *et al.* [174] takes 5 pairing operations and 2n scalar multiplications; therefore it takes 5 constant pairing operations and the scalar multiplications increase linearly. The first scheme in Gong *et al.* [256] takes (2n+1) pairing operations and the second scheme in Gong *et al.* [256] takes (n+2) pairing operations and n scalar multiplications. Both the schemes presented in Gong *et al.* [256] are highly costly as the pairing operations increase linearly with the number of signatures. The aggregate verify procedure of the proposed scheme is much efficient as it takes just 3 pairing operations and 3n scalar multiplications which is less as compared to all other schemes whereas the sign procedure is comparable to other schemes. In vehicular ad-hoc networks, vehicle has high computational power and the vehicle needs to sign only one signature whereas it needs to verify multiple signatures. Therefore, the signing cost can be compromised but one cannot compromise on the signature verification cost. It can be seen that the computational cost of the proposed scheme is more efficacious than the already existing schemes.

Further, the proposed security framework is tested and implemented using various parameters. The proposed framework is compared with the existing solutions to show its fea-

Table 5.1: Comparison of the proposed signature scheme with four other schemes

CLS scheme	Type	Sign Cost	Verify Cost	Aggregate Verify Cost
Zhang *et al.* [41]	*Sync*#	3S	4P	(n+3)P
Zhang *et al.* [174]	Sync	5S	5P+2S	5P+2nS
First scheme in [256]	Ad hoc*	2S	3P	(2n+1)P
Second scheme in [256]	Sync	3S	3P	(n+2)P+nS
Our scheme	Ad hoc	3S	3P+3S	3P+3nS

#Sync means normal mode of transfer

*Ad hoc means temporary mode of transfer

sibility. The proposed framework is implemented using the MIRACL library [257] on Intel Core i5 2.40 GHz Linux machine with 2 GB RAM. The 160 bit elliptic curve is taken into consideration which is equivalent to 1024 bit RSA security and the number of nodes is varied as 30, 50, 70 and 100 nodes. The Type 1 pairing on a characteristic 2 curve of embedded degree k = 2 on a prime field GF(p) (assumed to be more secure than binary fields) is used for implementation.

Table 5.2: Error probability for three cases considered

Cases	$\frac{m}{n}$	$\frac{r}{q}$	$\mathbb{P}$
Case I	1000/350	1000/350	0.064
Case II	1000/500	1000/500	0.146
Case III	1000/600	1000/600	0.20

The simulation of the proposed scheme is done using network simulator NS-2.34 and the

Table 5.3: P_{ver} and E_x for various cases and scenarios considered

	$\mathbb{P}$	% of entries exist in BF_2	P_{ver}				E_x			
			30 nodes	50 nodes	70 nodes	100 nodes	30 nodes	50 nodes	70 nodes	100 nodes
	0.064	66.67%	0.0030	0.0051	0.0067	0.0096	1	2	2	3
		50%	0.0038	0.0064	0.0089	0.0128	1	2	3	4
Urban	0.146	66.67%	0.0065	0.0109	0.0153	0.0219	3	5	7	11
		50%	0.0087	0.0146	0.0204	0.0292	4	7	10	14
	0.20	66.67%	0.009	0.015	0.021	0.03	5	9	13	18
		50%	0.012	0.02	0.028	0.04	7	12	17	24
	0.064	66.67%	0.0057	0.0096	0.013	0.0192	2	3	5	7
		50%	0.0076	0.0128	0.0179	0.0256	3	4	6	9
Rural	0.146	66.67%	0.013	0.0219	0.0306	0.0438	6	11	15	21
		50%	0.0175	0.029	0.041	0.0584	8	14	20	29
	0.20	66.67%	0.018	0.03	0.042	0.06	11	18	25	36
		50%	0.024	0.04	0.056	0.08	14	24	33	48

results are compared without using the bloom filter and with bloom filter with the average speed varying from 10m/s to 30m/s (36km/hr to 108km/hr) for 1000s on an area of 3 km^2 with three RSUs, 1 RTA and 1 KGC located in the area. The periodic beacons containing location and state information are broadcasted by each vehicle every 300 ms. Both the bloom filters of size 1000 bits are considered in the implementation. As the MAC addresses are processed by the first bloom filter BF_1, all the processed elements will be processed in second bloom filter BF_2 also for pseudonyms. Therefore, if n elements are processed in BF_1, all will be processed by BF_2 because BF_2 processes all the messages for pseudonyms whose MAC addresses have been processed by BF_1. The BF_1 and BF_2 of 1000 bits array size is considered and we consider the three cases, 60% of the MAC will be processed by BF_1 and the same 60% of the pseudonyms will be processed, followed by the case of 50% and 35%. The false positive error probability can be calculated for all the three cases as shown in Table 5.2. The total number of vehicles under the region of 1 RSU in urban scenario are assumed to be 1000 and the number of vehicles in rural scenario are assumed to be 500. It is assumed that each vehicle can receive the messages from its neighbours and 1 vehicle at a particular time can receive messages from at most 100 vehicles. Therefore, number of nodes considered in the simulation are 30, 50, 70 and 100 nodes. The two possibilities are considered when the pseudonyms are verified in BF_2 where $\frac{2}{3}$rd of the received pseudonyms match with the existing entries and second case where half of the received pseudonyms match with existing entries in BF_2.

Table 5.3 gives the verification probability and number of messages to be verified in BF_2 for the various cases. The verification probability is the probability with which the messages corresponding to the pseudonyms which already exist in bloom filter BF_2 are verified. E_x is the expected number of pseudonyms against which the messages will be verified. The proposed scheme with bloom filters is simulated for various values of $\mathbb{P}$ (false positive error

Table 5.4: Comparison of various security schemes

Schemes	Sign Message	Verify Signature	Verify k Signatures
ECDSA[49]	T_{mul}	$4T_{mul}$	$4kT_{mul}$
BLS[30]	$T_{mul}+T_{mtp}$	$4T_{par}+2T_{mtp}$	$(2k+2)T_{par}+2kT_{mtp}$
GSIS[51]	$3T_{par}+7T_{mul}$	$5T_{par}+4T_{mul}$	$5kT_{par}+4kT_{mul}$
ECPP[52]	T_{mul}	$3T_{par}+11T_{mul}$	$3kT_{par}+11kT_{mul}$
DCS[68]	$2T_{mul}$	$5T_{par}+3T_{mul}$	$5T_{par}+3kT_{mul}$
PASS[50]	T_{mul}	$3T_{par}+4T_{mul}$	$3kT_{par}+4kT_{mul}$
LPA[65]	$3T_{mul}$	$4T_{par}+2T_{mul}$	$4kT_{par}+2kT_{mul}$
PAFB(proposed)	$3T_{mul}$	$3T_{par}+3T_{mul}$	$3T_{par}+3kT_{mul}$

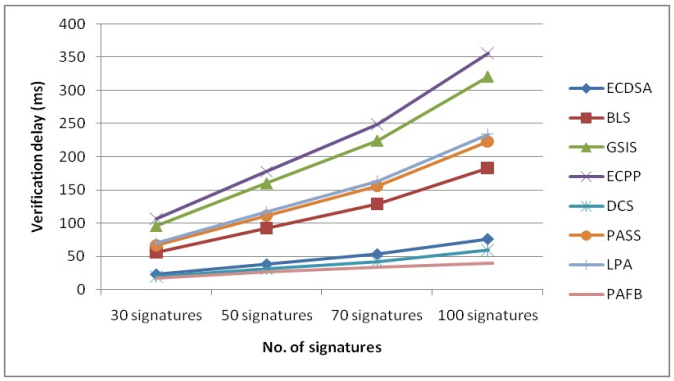

Figure 5.1: Comparison of proposed protocol with related protocols

probability) *i.e.* 0.064, 0.146, 0.20 under urban and rural scenarios. The parameters used for comparison are packet delivery ratio, network latency and computational delays in various scenarios. The two cases of bloom filters are also considered where two third of the received entries are verified in bloom filter BF_2 and other case where only half of the entries are verified.

The proposed scheme is compared with the other security schemes as shown in Table 5.4 which compares the message signing and verification procedures. The three basic operations used in the message signing and verification process are T_{mul}, T_{mtp} and T_{par} which are the times to compute scalar multiplication, map to point hash and pairing operations respectively. The times of these operations are calculated using MIRACL library. The time calculated to perform one T_{mul} is 0.19ms, T_{mtp} is 0.42ms and T_{par} is 0.49ms. ECDSA[49] signature scheme is the basic signature scheme which was adopted for VANETs which takes T_{mul} for

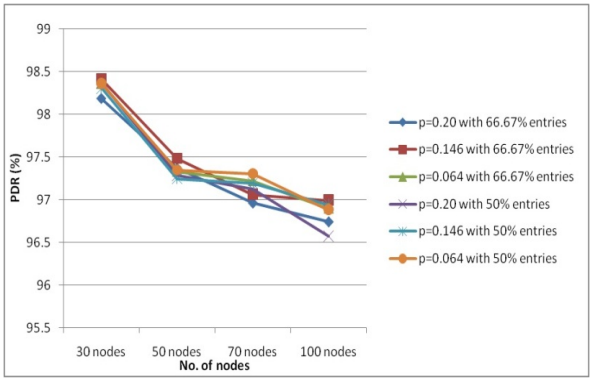

Figure 5.2: Packet delivery rate of proposed scheme with various error probabilities under urban scenario

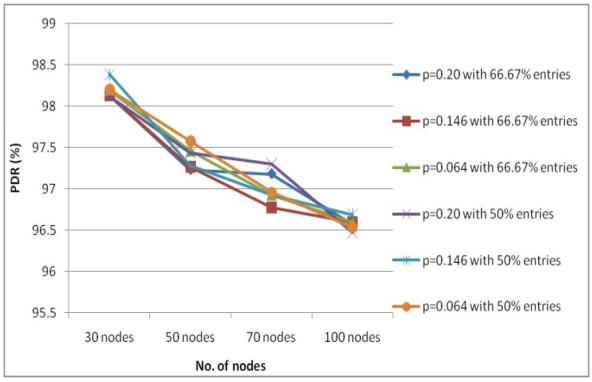

Figure 5.3: Packet delivery rate of proposed scheme with various error probabilities under rural scenario

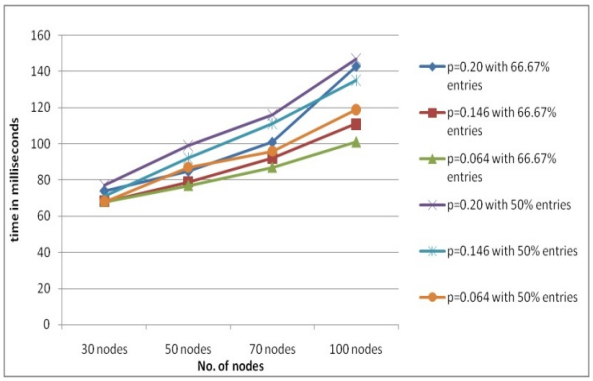

Figure 5.4: Network latency of proposed scheme with various error probabilities under urban scenario

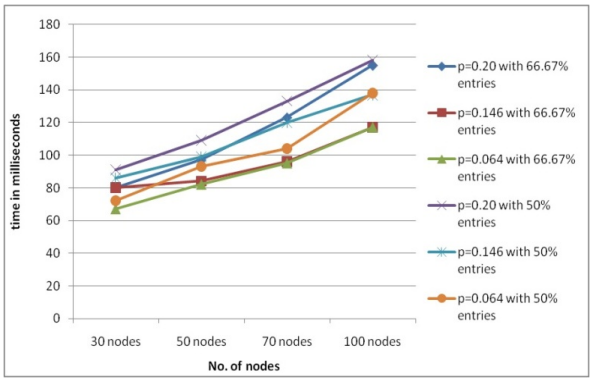

Figure 5.5: Network latency of proposed scheme with various error probabilities under rural scenario

signing the message and $4T_{mul}$ for verifying the single signature. The message signature time is comparable as the vehicle has to sign one message but verify multiple signatures. So the major aim is to reduce the signature verification time. The proposed PAFB scheme took $3T_{mul}$ operations which is comparable with LPA which is less than GSIS and BLS. ECDSA scheme needs only T_{mul} operations for verification which takes $4kT_{mul}$ operations for k signatures. The other schemes GSIS, ECPP, PASS and LPA considers the T_{par} operations for signature verification which increase linearly as the number of signatures increase. These schemes do not verify the signatures aggregately which increase the verification time linearly with the signatures. BLS, DCS and PAFB(ours) are the aggregate signature schemes which

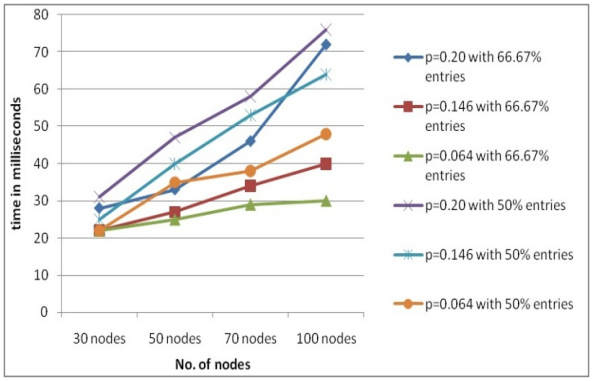

Figure 5.6: Computational delays of proposed scheme with various error probabilities under urban scenario

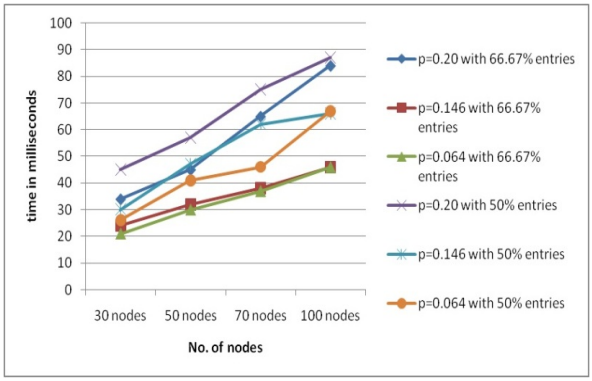

Figure 5.7: Computational delays of proposed scheme with various error probabilities under rural scenario

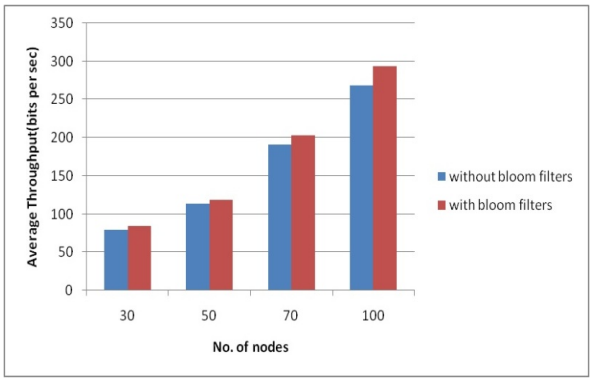

Figure 5.8: Average throughput of the simple aggregate scheme and proposed scheme

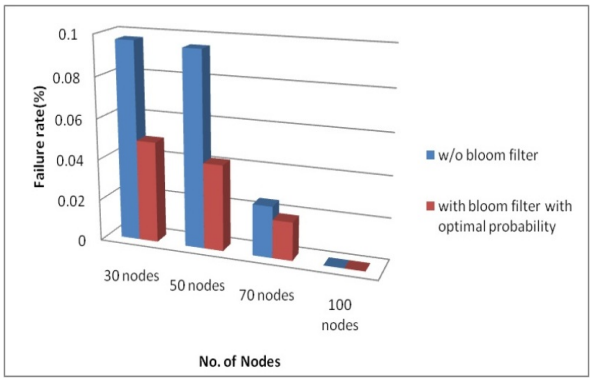

Figure 5.9: Failure rate of the simple aggregate scheme and proposed scheme

verify the signatures aggregately. PAFB took only $3T_{par} + 3kT_{mul}$ operations which is less than BLS and DCS which took $(2k+2)T_{par} + 2kT_{mtp}$ and $5T_{par} + 3kT_{ul}$ respectively. The signature verification time of PAFB is further reduced by employing the bloom filters which greatly increases the efficiency of the protocol. Figure 5.1 compares the verification delay of PAFB with the other related works which shows that the verification delay in our scheme PAFB is much lesser than the other schemes.

Figure 5.2 gives the Packet Delivery Rate (PDR) of the various cases under urban scenario and Figure 5.3 gives the same for rural scenario. PDR decreases as the error probabilities of the bloom filter increases under both urban and rural scenarios. Figure 5.4 and

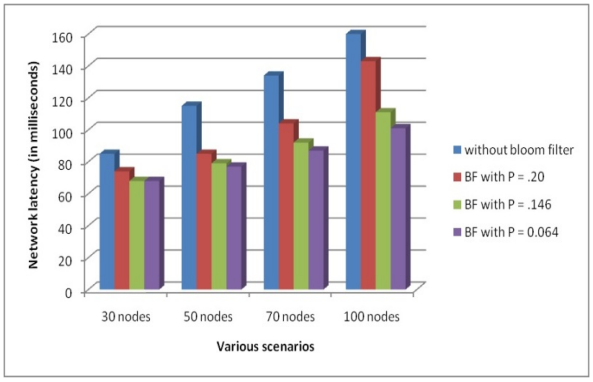

Figure 5.10: Network latency of the simple aggregate scheme and proposed scheme

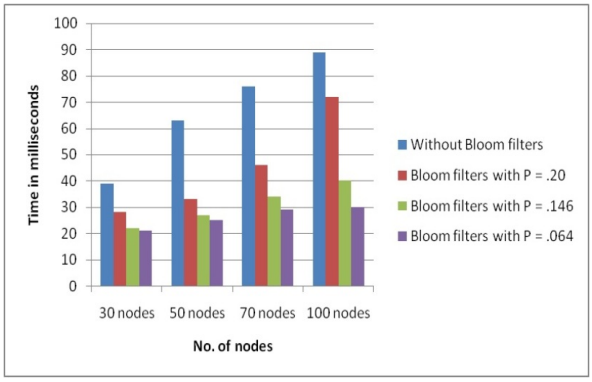

Figure 5.11: Computational delays of the simple aggregate scheme and proposed scheme

Figure 5.5 gives the network latency of the scheme under different error probabilities in urban and rural scenarios respectively. Similarly, Figure 5.6 and Figure 5.7 shows the computational delays in urban and rural respectively. The network latency and computational delays increases with the increase in error probabilities. The network latency and computational delays are more when $\frac{1}{2}$ of the received entries are matched compared to the case when $\frac{2}{3}$ entries are matched in BF_2. Moreover, the delays incurred are more in the rural area as compared to urban area under same conditions and probabilities. The bloom filters need to verify some already matched entries to incorporate the error probabilities and therefore, the error probability of the bloom filters should be less so that optimal number of entries are also verified apart from the unmatched new entries. Hence, the error probability need to be reduced but it should not be reduced to such a large extent that no matched entry is verified. So, the optimal value of the error probability needs to be selected. In these three cases, 0.146 can be considered as the optimal probability.

The average throughput increases by 7.3% with our proposed scheme as shown in Figure 5.8. Figure 5.9 gives the comparison of failure rate of the network where the failure rate of the network is reduced by 49.5% in our proposed scheme with bloom filter. Figure 5.10 represents the network latency of the proposed scheme with the highest latency in the sim-

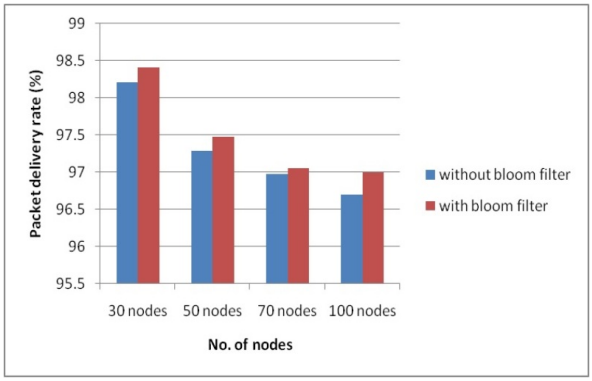

Figure 5.12: Packet delivery rate of the simple aggregate scheme and proposed scheme

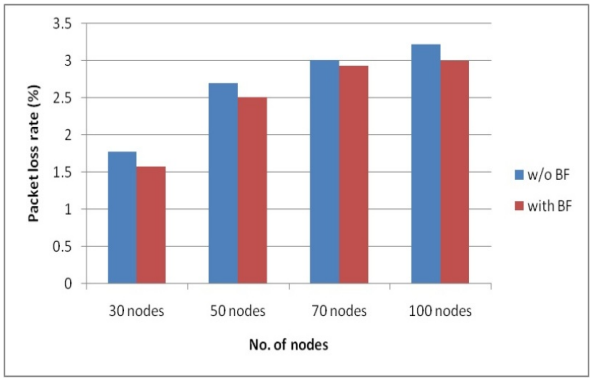

Figure 5.13: Packet loss rate of the simple aggregate scheme and proposed scheme

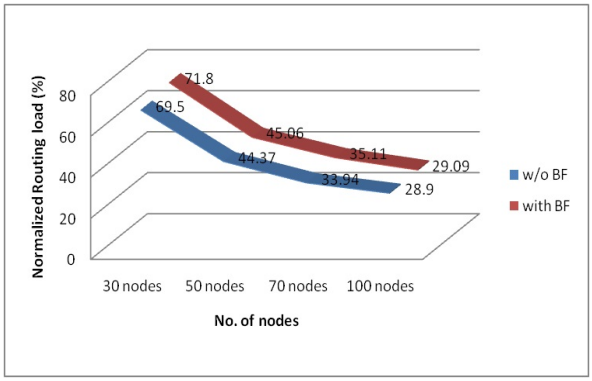

Figure 5.14: Normalized routing load of the simple aggregate scheme and proposed scheme

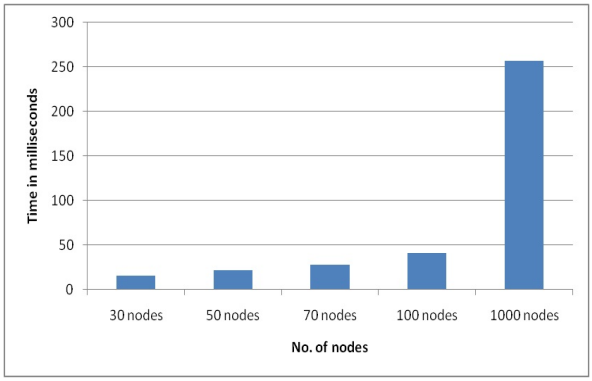

Figure 5.15: Computational delays of RSU

ple aggregate scheme and it gets reduced when bloom filter is used by 17.8% with $\mathbb{P}$ =0.2, 29.15% with $\mathbb{P}$ =0.146 and 32.38% with $\mathbb{P}$ = 0.064. Similarly, the computational delays are reduced by 32.9% with bloom filter with error probability $\mathbb{P}$ =.20, 53.93% with $\mathbb{P}$ = 0.146 and by 60.6% with $\mathbb{P}$ = 0.064 as in Figure 5.11, thus the proposed scheme with bloom filters has less computational delays. The packet delivery rate increases in the proposed scheme using bloom filter compared with the simple aggregate scheme as shown in Figure 5.12. The packet loss rate of the proposed and simple scheme is compared in Figure 5.13 where packet loss rate decreases by 6.4% with the help of bloom filters. The normalized routing load increases by 2.46% with application of the bloom filters as in Figure 5.14. Figure 5.15 gives

the average computational delays of road side infrastructure as the number of nodes in the network increases.

5.2 Conclusion

The results have shown that the proposed scheme is very efficient in terms of computation and communication overhead. So the bloom filters improve the efficacy of the aggregate scheme which is very useful in heavy traffic scenarios where vehicles need to verify a lot of messages from its neighbouring vehicles in small amount of time.

Chapter 6

Effective Vehicular Communications

The road vehicles were the territory of mechanical engineers until recently when the willingness of manufacturers for the road safety increased to provide the security of the road network. Nowadays, the vehicles are rather becoming "Network on Wheels" with mini computers installed on vehicles. These networks are aiming towards maintaining high level of security for the traffic security. The group of vehicles within short range of communication (100-300m) can communicate with each other regarding events, position information, *etc.* but the information shared among vehicles may be false as the malicious vehicle may transmit the wrong information. The broadcasting of false information in the network is one of the major concern of security.

6.1 Fuzzy Based Trust Prediction Model

The vehicle-to-vehicle communication systems are emerging with the crucial requirement to embellish the driver and road safety by imparting the up-to-date information regarding road traffic conditions. The message integrity in VANETs is ensured by the authentication approach but the limitation of such approach is that it only ensures legitimate sender and

Table 6.1: Comparison of existing trust based schemes with proposed scheme in VANETs

Trust Schemes	**Network Type**	**Fuzzy Inference Engine**	**Data Centric Approach**	**Relay Node Trust Computation**	**Sender Reputation**	**Third Party Involvement**	**Communication Overhead**	**Probabilistic Approach**	**Transmission Path Selection**
Raya *et al.* (2008) [153]	VANETs	×	×	×	✓	×	✓	✓	×
Minhas *et al.* (2011) [144]	VANETs	×	×	✓	✓	✓	✓	×	×
Gomez *et al.* (2012) [138]	VANETs	×	×	✓	×	×	×	×	×
Gazdar *et al.* (2012) [152]	VANETs	✓	×	✓	×	✓	✓	×	×
Anita *et al.* (2014) [161]	WSNs	✓	×	✓	✓	✓	×	×	×
Li *et al.* (2015) [160]	VANETs	✓	✓	×	✓	×	×	×	×
Proposed Scheme	VANETs	✓	✓	✓	✓	×	×	×	✓

cannot prevent it from broadcasting bogus and malicious information. Hence, it is mandatory to confirm the authenticity of the information received rather than the legitimacy of the corresponding sender. Thus, it is important to evaluate the trustworthiness of the information received to make effective decisions. The trust models are developed in a unique manner to give incentives to the vehicles to behave appropriately and to discourage the malicious activities of the self-centered vehicles. A fuzzy based trust model is proposed for vehicular ad hoc network which computes the relaying trust value and coordinating trust value that form an input to fuzzy engine in yielding the final trust value for each node. The data transmission path is selected based on the vehicles having higher computed trust values. The proposed trust model is integrated with the routing protocols to test its performance in a simulated network environment. Table 6.1 compares the existing trust based schemes with the proposed trust prediction scheme based on the various parameters to test the efficiency of the proposed scheme in comparison to other existing trust based schemes.

The trust models have been designed widely in the distributed environments such as

VANETs, where each vehicle is able to build the opinion regarding the rest of the vehicles in network in terms of trust value, by properly collecting the information of other vehicles in a timely manner. All the other works evaluate the trust of the received messages from the other nodes, but none of the scheme used the concept of relay selection for data transmission using fuzzy inference engine. The proposed model is used for the selection of data transmission path based on relaying nodes, and the relaying nodes are selected by each vehicle based on the calculated trust of other vehicles using the fuzzy inference engine.

6.1.1 Proposed Fuzzy Based Trust Model

Trust is the association between two nodes for the reliable packet forwarding technique. The proposed model calculates the trust level based on relaying trust value and the coordinating trust value where former predicts the trust value for the selection of relay nodes to forward the data packet and later for the selection of data transmission path. In vehicular ad-hoc networks, each source node forwards the data packet to the destination with the help of intermediate nodes known as relaying nodes. The number of relaying nodes does not have any impact on the model, but the selection of relay nodes to forward the packet has the impact. It is assumed that there is only one source and destination in the radio range of the source node. Further, it is assumed that each node has the knowledge of its location coordinates as well as of other nodes. Global Positioning System (GPS) installed onboard of the vehicle is used for the position verification mechanism by sending the location of the vehicle along with timestamp.

Relaying Trust Value

When the source needs to transmit the data to the destination, the selection of the reliable and trustworthy intermediate nodes is vital to assure the reliable transmission of the data

packet. Therefore, the trust value of the neighbouring nodes is calculated by each node and the node with highest trust value among the neighbours is used for the selection of relay node to forward the packet to next relay node and finally to destination. The relaying trust value is basically an actual set of nodes that can be used as input for relaying. $N = \{N_1, N_2, N_3, N_4 ..... N_n\}$ depicts the set of nodes in the zonal radio range of the source S. Let the source S wants to forward the packet to the node N_2, then the set of relay nodes can be defined as,

$$N_2^{'} = \{X, |d(X, N_1 \leq R), X, N_1 \in N, X \neq S, X \neq N_2\},$$

where $N_2^{'}$ depicts the set of relay nodes present in the path between source S and destination N_2 in the defined radio range. The relaying trust is computed based on the relaying distance factor, network density and trust inconsistency.

I Relaying Distance Factor:

The relaying distance factor computes the distance between the any two nodes which is used as an input parameter for the relaying trust computation. The relaying distance is further dependent on the three types of distances:

i Distance between relaying node and source (d_1)

ii Distance between relaying node and destination (d_2)

iii Inter-relaying distance (d_3)

The distances d_1 and d_2 are used for the selection of appropriate relay nodes which can be used for data transmission between source and destination. Inter-relaying distance is the distance between any two relay nodes which can be selected for the data packet forwarding path. The distance between any two nodes can be calculated based on the

distance formula as:

$$d(N_{(x1,y1)},N_{(x2,y2)}) = \sqrt{(x2-x1)^2+(y2-y1)^2}, \tag{6.1}$$

where (x1,y1) and (x2,y2) are the location coordinates of the two nodes N_1 and N_2 among which the distance is to be calculated. The distance relaying factor (DW) is calculated as:

$$DW(S_{(x1,y1)},R_{(x2,y2)}) = \beta_1(d_1)+\beta_2(d_2)+\beta_3(d_3) \begin{cases} 0 \leq \beta_1 \leq 1 \\ 0 \leq \beta_2 \leq \beta_1 \\ 0 \leq \beta_3 \leq \beta_2 \end{cases} \tag{6.2}$$

where $S_{(x1,y1)}$ is the source node, $R_{(x2,y2)}$ is the destination node, β_1, β_2, β_3 are the priority factors for the distances d_1, d_2 and d_3 respectively. The less is the distance relaying factor, more is the connectivity among the nodes.

II Network Density:

Network density is calculated by each node based on the zone-based density i.e. the network density is calculated based on the condition that the nodes N are within the range R. The network density is dependent on vehicular density, traffic density and average connectivity.

i Vehicular Density : The Vehicular Density (VD) is calculated in the time interval (Δt) as:

$$VD(\Delta t) = \frac{\sum x | x \in N, d(x1,x2) \leq R}{\sum N(\Delta t)}, \tag{6.3}$$

Where $\sum x$ is the total number of nodes which are in the zonal distance of R and $\sum N$ is the total number of vehicles in the given time interval Δt.

ii Traffic density: Traffic Density (TD) is measured in terms of packet data which is transmitted among the nodes which can be easily determined from the packet delivery ratio of the network. Traffic density is the ratio of the packets which need to be transmitted and the total number of packets.

$$TD(\Delta t) = \frac{\sum Rw.x | x \in N, d(S,x) \leq R}{Sw(S)} \tag{6.4}$$

Rw is the number of received packets by all the nodes x such that the x lies in the zonal distance of source S. Sw(S) is the total number of packets sent by the source S in the given time interval Δt.

iii Average connectivity : Average Connectivity (AC) is measured as ratio of the minimum number of vehicular connections that should always be present to sustain the network and the total available connections in the network.

$$AC(\Delta t) = \frac{c(min)}{c(avl)} \tag{6.5}$$

where c(min) is the minimum connections required to sustain the network and c(avl) is the total number of available connections in the network.

The network density can be calculated in the given time interval (Δt) as:

$$ND(\Delta t) = \alpha.VD + \delta.TD + \gamma.AC \tag{6.6}$$

where α denotes probabilistic connectivity with $0 \leq \alpha \leq 1$, α can be 0 as vehicular density can be zero. δ denotes probabilistic traffic density depending on vehicular connectivity such that $0 \leq \delta \leq \alpha$ and if $\alpha = 0$ which implies $\delta = 0$, thus traffic density can be 0. γ denotes rate of connectivity with $0 < \gamma \leq 1$, γ cannot be 0 as minimum connec-

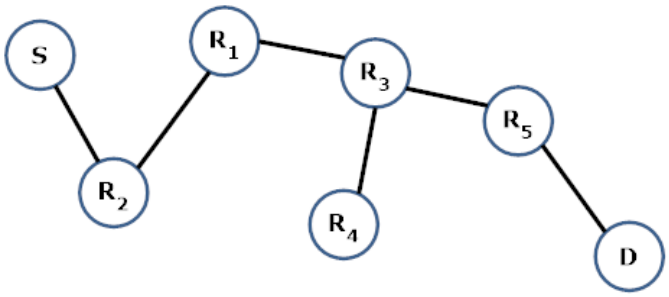

Figure 6.1: Network topology

tions cannot be nil as atleast c(min) connections should always be present to sustain the network.

III Trust Inconsistency:

Trust Inconsistency is defined as the minimum number of connections leading to more inconsistency in trust. The nodes with higher number of connections will have lower trust inconsistency as the node with maximum connections is highly trusted. In Figure 6.1 number of connections and the corresponding normalized values are given as:

$R_1 - \mathbf{2} \longleftarrow 0.5$

$R_2 - \mathbf{1} \longleftarrow 1$

$R_3 - \mathbf{3} \longleftarrow 0$

$R_4 - \mathbf{1} \longleftarrow 1$

$R_5 - \mathbf{1} \longleftarrow 1$

In this example (Figure 6.1), trust inconsistency of node R_3 is high as its normalized value is 0 and trust inconsistency of nodes R_2, R_4 and R_5 is low as these nodes have value 1. Therefore, the node with least number of connections will have high trust inconsistency

IV Fuzzy membership functions for relaying trust:

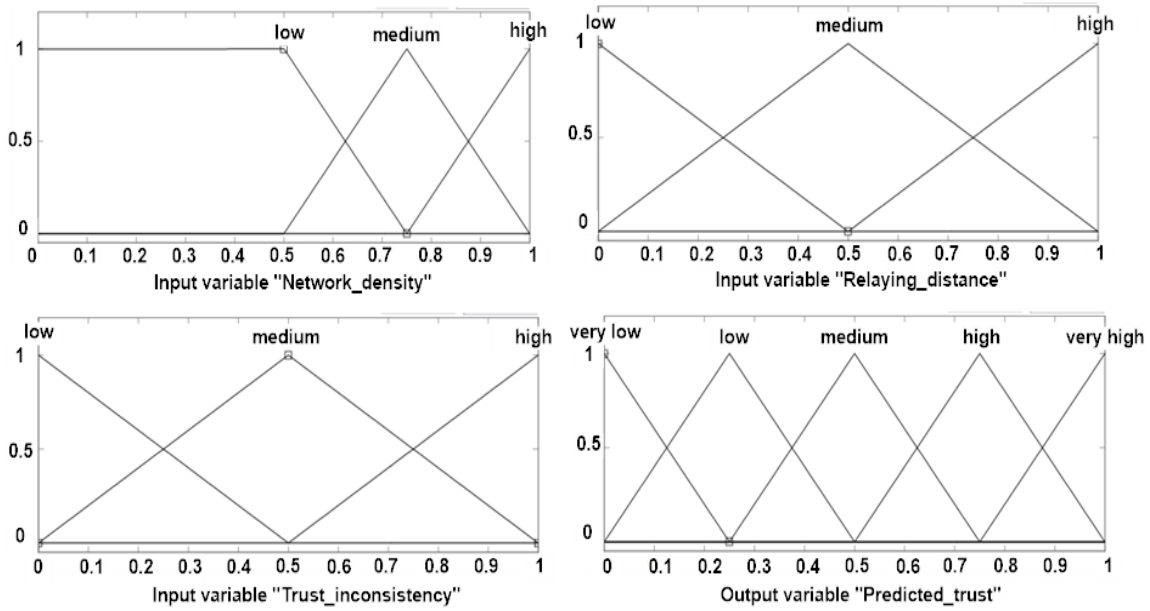

Figure 6.2: Fuzzy membership functions for the relaying trust value inputs and outputs

The relaying trust value is computed based on three inputs relaying distance factor DW($S_{(x1,y1)}$,$R_{(x2,y2)}$), network density ND(Δt) and trust inconsistency Ti($S_{(x1,y1)}$,$R_{(x2,y2)}$) resulting in one output, relaying trust value T_R. The fuzzy membership functions for the inputs and output are shown in Figure 6.2. The fuzzy membership functions for the distance relaying factor DW($S_{(x1,y1)}$,$R_{(x2,y2)}$) are low, medium and high denoted as Rdis_Low, Rdis_Medium and Rdis_High respectively. Similarly, fuzzy membership functions for network density ND(Δ t) are low, medium and high denoted as Net_Low, Net_Medium and Net_High respectively. The fuzzy membership functions for trust inconsistency Ti($S_{(x1,y1)}$,$R_{(x2,y2)}$) are low, medium and high denoted as T_Inc_Low, T_Inc_Medium and T_Inc_High respectively. The minimum value for fuzzy membership function, low, for network density ND(Δ t) is taken as 0.5 because it is assumed that half of network density ND(Δ t) should always be present to sustain the network. The fuzzy membership functions for the output relaying trust value T_R are very low, low, medium, high and very high denoted as RelT_Very_Low, RelT_Low, RelT_Medium, RelT_High and RelT_Very_High respectively. The values of the fuzzy

membership functions are chosen appropriately to obtain optimal output values. Based on the fuzzy values of relaying distance factor, network density and trust inconsistency, rules based on IF/THEN are defined to calculate the relaying trust value of the node. The rule base is defined in Table 6.2. The rule 1 in Table 6.2 can be expressed as: *"IF the network density is low and relaying distance factor is low and trust inconsistency is low, THEN relaying trust value is medium"*

Table 6.2: Rule base to calculate relaying trust value

RULE NO.	NETWORK DENSITY	RELAYING DISTNACE FACTOR	TRUST INCONSISTENCY	RELAYING TRUST VALUE
1	Net_Low	Rdis_Low	T_Inc_Low	RelT_Medium
2	Net_Low	Rdis_Low	T_Inc_Medium	RelT_Medium
3	Net_Low	Rdis_Low	T_Inc_High	RelT_Low
4	Net_Low	Rdis_Medium	T_Inc_Low	RelT_Medium
5	Net_Low	Rdis_Medium	T_Inc_Medium	RelT_Medium
6	Net_Low	Rdis_Medium	T_Inc_High	RelT_Low
7	Net_Low	Rdis_High	T_Inc_Low	RelT_Low
8	Net_Low	Rdis_High	T_Inc_Medium	RelT_Low
9	Net_Low	Rdis_High	T_Inc_High	RelT_Very_Low
10	Net_Medium	Rdis_Low	T_Inc_Low	RelT_High
11	Net_Medium	Rdis_Low	T_Inc_Medium	RelT_Medium
12	Net_Medium	Rdis_Low	T_Inc_High	RelT_Medium
13	Net_Medium	Rdis_Medium	T_Inc_Low	RelT_Medium
14	Net_Medium	Rdis_Medium	T_Inc_Medium	RelT_Medium
15	Net_Medium	Rdis_Medium	T_Inc_High	RelT_Low
16	Net_Medium	Rdis_High	T_Inc_Low	RelT_Medium
17	Net_Medium	Rdis_High	T_Inc_Medium	RelT_Low
18	Net_Medium	Rdis_High	T_Inc_High	RelT_Low
19	Net_High	Rdis_Low	T_Inc_Low	RelT_Very_High
20	Net_High	Rdis_Low	T_Inc_Medium	RelT_High
21	Net_High	Rdis_Low	T_Inc_High	RelT_Medium
22	Net_High	Rdis_Medium	T_Inc_Low	RelT_High
23	Net_High	Rdis_Medium	T_Inc_Medium	RelT_High
24	Net_High	Rdis_Medium	T_Inc_High	RelT_Low
25	Net_High	Rdis_High	T_Inc_Low	RelT_Medium
26	Net_High	Rdis_High	T_Inc_Medium	RelT_Low
27	Net_High	Rdis_High	T_Inc_High	RelT_Low

Coordinating Trust Value

The coordinating trust value T_C is calculated to select the data transmission path between the source node $S_{(x1,y1)}$ and destination node $R_{(x2,y2)}$. The coordinating trust value is calculated

from three factors,

i Relative Velocity

ii Degree of Connectivity

iii Connection Loss

I Relative velocity:

Relative velocity V_R is calculated between the source node $S_{(x1,y1)}$ and other neighbouring nodes moving in the same direction in its vicinity.

$$V_R = \frac{|V(S_{(x1,y1)}) - V(Ns_{(x1,y1)})|}{max(V(S_{(x1,y1)}), V(N_{(x1,y1)}))} \tag{6.7}$$

where $V(S_{(x1,y1)})$ is the velocity of the source node and $V(N_{(x1,y1)})$ is the velocity of the neighbouring node Ns such that Ns $\in$ N.

II Degree of Connectivity:

Degree of connectivity deg_n is the ratio of the number of connections a node is sharing with other neighboring nodes in the network and the total connections a node can establish with other nodes in the network in the time interval (Δt).

$$deg_n(\Delta t) = Ti(\Delta t)Tn(\Delta t) \tag{6.8}$$

where Ti(Δt) is the number of connections a node n has with its neighbours and Tn(Δt)is the total number of connections a node x can establish with its neighbours in the time interval (Δt).

III Connection Loss:

The connection loss L_C can be defined as the number of connections lost by the node in

the time interval (Δt). The connection loss $L_{C(Ni)}$ (Δt) by the node N_i in the time interval (Δt) can be defined as:

$$L_{C(Ni)}(\Delta t) = \frac{Ti(\Delta t) - (deg(\Delta t) - deg(\Delta t - 1))}{T(\Delta t)} \tag{6.9}$$

where Ti(Δt) is the total number of connections a node N_i has in time interval (Δt), deg(Δt)is the degree of connectivity of node N_i, deg((Δt)-1) is the degree of connectivity at time interval (Δt)-1 and T(Δt) is the total number of available connections in the network.

Coordinating Trust

The coordinating trust is used for the selection of the reliable path for the transmission of data. The coordinating trust value T_C can be calculated as:

$$T_C = \lambda_1(V_R) + \lambda_2(deg_n(\Delta t)) + \lambda_3(L_{C(Ni)}(\Delta t)) \begin{cases} 0 \leq \lambda_1 \leq 1 \\ \lambda_1 \leq \lambda_3 \leq \lambda_2 \\ 0 < \lambda_2 \leq 1 \end{cases} \tag{6.10}$$

where V_R is the relative velocity of node N_i, $deg_n(\Delta t)$ is degree of connectivity of node N_i, $L_{C(Ni)}$ (Δt) is the connection loss for node N_i and λ_1, λ_2 and λ_3 are the various probabilistic values for V_R, $deg_n(\Delta t)$ and $L_{C(Ni)}$ (Δt) respectively.

6.1.2 Final Trust Level

The final trust level is computed from the two inputs, relaying trust value and coordinating trust value. Figure 6.3 shows the fuzzy membership functions for relaying trust T_R, coordi-

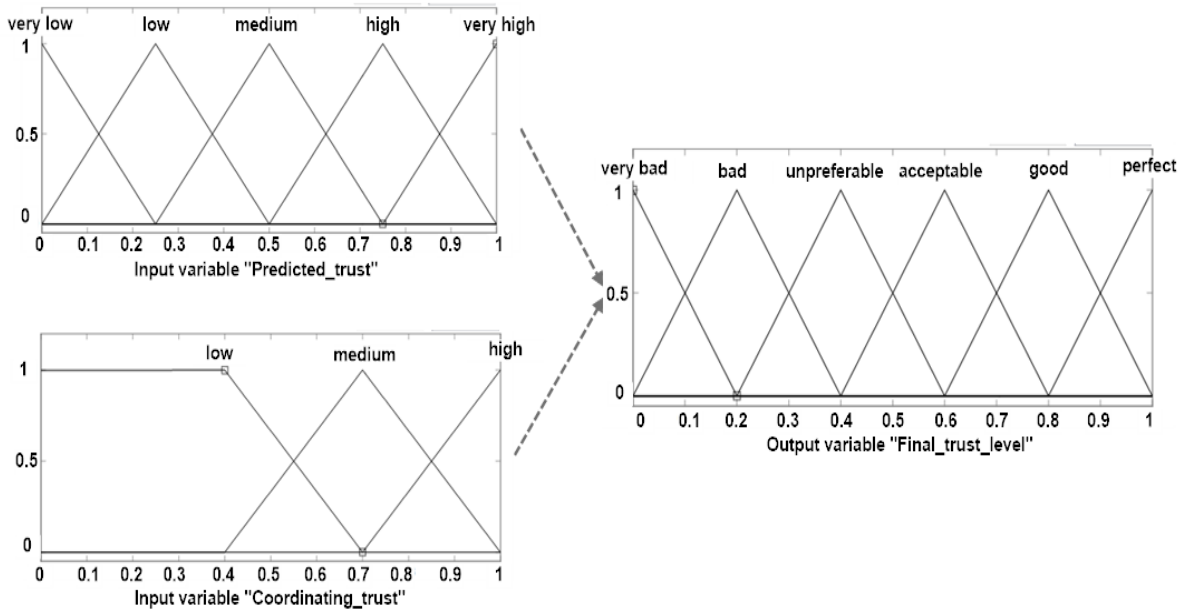

Figure 6.3: Fuzzy membership functions for the final trust value inputs and outputs

nating trust T_C and final trust level T_L. The fuzzy membership functions for relaying trust T_R are obtained from the previous calculations in section 3.3.4; the fuzzy membership functions for coordinating trust T_C are low, medium and high denoted as Cor_Low, Cor_Medium and Cor_High respectively. The fuzzy membership functions for the output final trust level T_L are Worst, Bad, Unpreferable, Acceptable, Good and Perfect. The IF/THEN rules considered for the calculation of final trust level T_L are provided in rule base in Table 6.3.

Fuzzy Updations

After each interval Δt, fuzzy inference engine is updated to find the next best possible combination of rules. The updations are provided over the final trust value computed using relaying trust value and coordinating trust value. Let $\eta^{'}$ be the updation rate defined as:

$$\eta^{'} = \frac{\eta T_R}{max(T_R, T_C)} \quad \eta \in (0,1) \tag{6.11}$$

According to updation rule, output equation for fuzzy inference iterations $F_{updations}$ is:

Table 6.3: Rule base to calculate final trust level

RULE NO.	RELAYING TRUST VALUE	COORDINATING TRUST VALUE	FINAL TRUST VALUE
1	RelT_Very_low	Cor_Low	Worst
2	RelT_Very_low	Cor_Medium	Bad
3	RelT_Very_low	Cor_High	Unpreferable
4	RelT_Low	Cor_Low	Bad
5	RelT_Low	Cor_Medium	Unpreferable
6	RelT_Low	Cor_High	Unpreferable
7	RelT_Medium	Cor_Low	Unpreferable
8	RelT_Medium	Cor_Medium	Acceptable
9	RelT_Medium	Cor_High	Acceptable
10	RelT_High	Cor_Low	Unpreferable
11	RelT_High	Cor_Medium	Acceptable
12	RelT_High	Cor_High	Good
13	RelT_Very_High	Cor_Low	Acceptable
14	RelT_Very_High	Cor_Medium	Good
15	RelT_Very_High	Cor_High	Perfect

Algorithm 6.1 Algorithm for fuzzy based trust calculation

Require: simulation_time
Ensure: nodes — nodes≥5 /*Minimum network size*/
configure(nodes) /*paramterized configurations of nodes*/
iteration_interval ⟵ Δt
initialize ⟵ η /*setinitial update rate*/
while $i <= simulation\_time$ **do**
$T_{R_t} = f(DW, ND, Ti)$ /*Relaying Trust Value*/
$T_{C_t} = f(V_R, deg_n, L_{C(Ni)})$ /*Coordinating Trust Value*/
$T_{L_t} = f(T_R, T_C)$ /*Final Trust Level*/
$\eta_t^{'} = \frac{\eta T_{R_t}}{mac(T_{R_t}, T_{C_t})}$
if $Node(i, T_L) \geq 0.5$ **then**
set relay ⟵ i /*setting realying nodes*/
relay_count=relay_count+1
end if
$i = i + \Delta t$
path ⟵ route(relay) /*finalizing path*/
Apply Fuzzy_update
transmit
end while

$$F_{updations} = \frac{\sqrt{T_{C_t}^2 + T_{R_t}^2}\ I^{'} + \eta_t^{'} T_{L_t}}{||T_{C_t} + \eta_t^{'} \sqrt{T_{C_t}^2 + T_{R_t}^2}||} \tag{6.12}$$

where $\sqrt{T_{C_t}^2 + T_{R_t}^2}$ is the weighing factor for updations and $I^{'}$ is the iteration level. T_{L_t} is the final trust level, T_{R_t} is the relaying trust value and T_{C_t} is the coordinating trust value at time t. The algorithm for control and selection of trusted path based on the final trusted value is given in algorithm 6.1.

6.1.3 Simulation Results and Discussion

The performance of the proposed fuzzy based trust model was evaluated using fuzzy based inference engine created over Matlab. The proposed approach was analyzed using network simulations configured over NS-2 and Matlab. The analysis were carried using a fuzzy based engine designed for implementation of the proposed model coded in Matlab and NS-2 was used to generate the traffic for the network. The standard IEEE 802.11p is used to evaluate the performance of the VANET scenario for the proposed trust model under various performance metrics. The simulation parameters configured are described in Table 6.4.

Table 6.4: Simulation parameters for trust prediction model

Parameter	Value	Description
Simulation time	100 seconds	The time for which simulation runs
Highway length	5000-15000m	The length of the road considered for simulation
Highway width	50m	The width of the road considered for simulation
No. of nodes	50-400	The number of vehicles
No. of Non-cooperating vehicles	5%	The vehicles refuse to participate in communication
Propagation radio Model	Two Ray Ground	Topological Model
Node placement	Random	Placement of nodes in network
Mobility Model	Random way point	Node movement model
Routing protocols	AODV,DSR,DSDV	The protocols for analysis
MAC protocol	IEEE 802.11p	IEEE standard for wireless communication
Transmission range	500m	Transmission range of vehicles
Base frequency	5.88GHz	Frequency used for simulation
Velocity range	10-30m/s	The velocity range of vehicles
Movement model	Dynamic	Node movement model
Traffic type	CBR(TCP)	Protocol for initiating communication
No. of simulation runs	10	Number of analysis runs

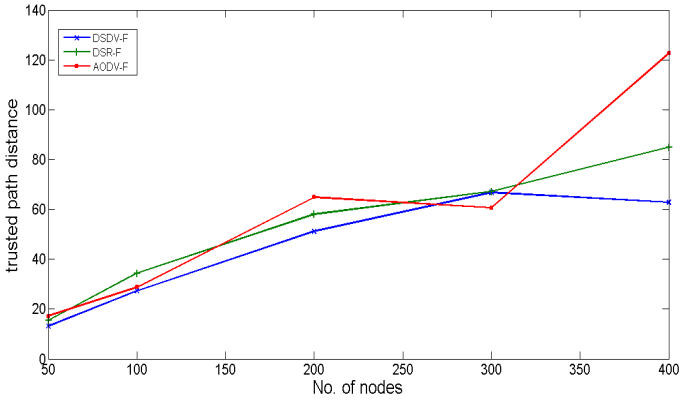

Figure 6.4: Trusted path distance vs. nodes

Trusted path is the path selected between source and destination which the nodes will follow for the data transmission and the path considered is more reliable with less non-cooperating nodes. Trusted path distance is the number of hops used for the data transmission on the trusted path between source and destination, calculated by the proposed scheme. The trusted path distance should be less for the protocol to be more efficient. The trusted path distance comparison for the three protocols is depicted in Figure 6.4 where DSDV-F performs better as compared to other protocols i.e. AODV-F and DSR-F. DSDV-F outperforms AODV-F by 32.89% and DSR-F by 17.4% in terms of trusted path distance. The time taken by the network to establish the connection between source and destination is the connectivity time. The connectivity time should be less for the protocol as lesser will be the connectivity time and more faster the nodes will establish the connection with other nodes for the efficient transmission of data in the network. Figure 6.5 shows the connectivity time for all the three protocols and DSDV-F has connectivity time lesser than AODV-F and DSR-F. DSDV-F performs 33.12% better than AODV-F and by 30.6% than DSR-F in terms of connectivity time. The number of paths which are not trusted and cannot be selected for the data transmission path are known as unreliable paths. The number of unreliable paths for all the protocols are calculated and plotted in Figure 6.6 where DSDV-F has maximum num-

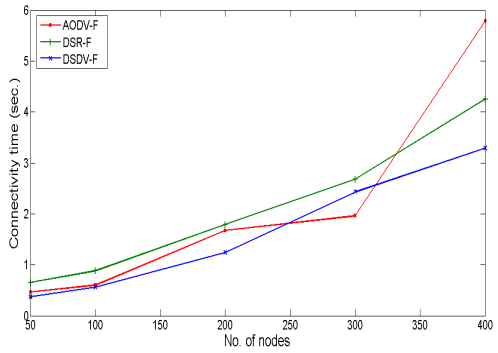

Figure 6.5: Connectivity time vs. nodes

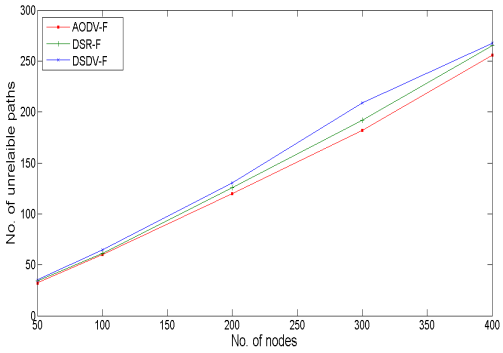

Figure 6.6: Unreliable paths count vs. number of nodes

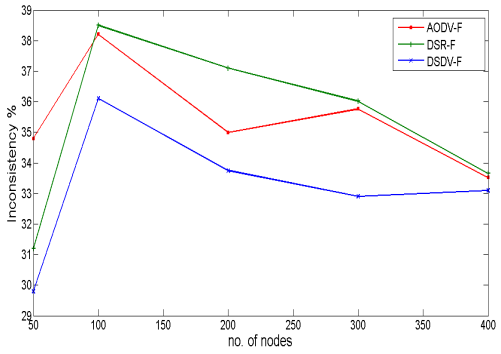

Figure 6.7: Inconsistency vs. number of nodes

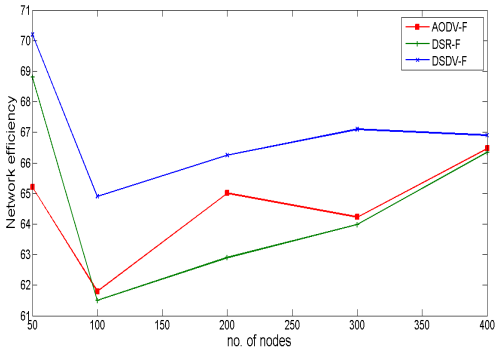

Figure 6.8: Network efficiency vs. number of nodes

ber of unreliable paths. The performance of the network can be observed from the number of unreliable paths. A protocol operating over network with less number of unreliable path offers high transmission rate. AODV-F has the better performance in terms of path selection as it has less number of unreliable paths than DSDV-F by 8.17% and DSR-F by 3.97%. The percentage of the nodes which are untrustworthy in the given network and should be least trusted for relaying is inconsistency. In order for the protocol to select the best path consideration in the network, the trust inconsistency should be less. The inconsistency in DSDV-F is lesser than AODV-F by 7% and from DSR-F by 6.5% as shown in Figure 6.7. The overall efficiency of the proposed trust model in the simulated network is the network efficiency. The network efficiency shows which protocol in integration with the proposed

model performs best. The protocol behaviour is considered best in term of each aspect if the network efficiency increases and thus, our proposed model is behaving best in integration of that protocol. Network efficiency of DSDV-F increases from AODV-F by 3.8% and from DSR-F by 3.5% plotted in Figure 6.8. The network efficiency of the DSDV-F is best when compared with other protocols indicating that our proposed protocol performs best with DSDV protocol.

The given proposed trust model performs better with DSDV protocol and the results of the various performance metrics have shown that DSDV-F is more effective than AODV-F and DSR-F. Therefore, the performance analysis of our proposed model integrated with three protocols has shown that the proposed fuzzy based trust model improves the performance of the DSDV protocol and it performs best in the considered testing parameters based on the proposed model when compared with AODV and DSR.

6.2 Misbehaviour Detection Module

There is possibility that due to the selfish motive of the driver, malicious vehicle may send the false information to its neighbours. The misbehaving vehicles may attempt to collect the private information of the drivers for its personal interest. So, there is urgent need for detecting the malicious vehicles in the network and correcting the false information which is broadcasted in the network. A new misbehaviour detection scheme is employed for VANETs which employs the design of Decision Inference System (DIS) for the detection of misbehaviour in network. DIS uses the XML based dependency tree formation for the collection of information from the vehicles as well as RSUs by CA (Certification Authority) for the final XML tree formation. The final XML tree built by CA by using DIS is transmitted to the RSUs as well as vehicles for the actual decision making by the network entities.

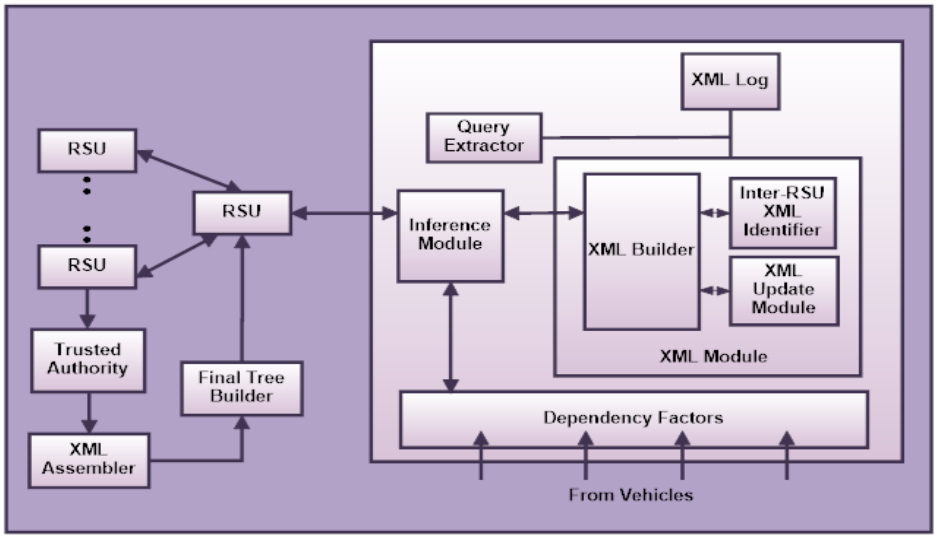

Figure 6.9: Decision inference system model

To prevent the legitimate nodes from being cheated by the illegitimate nodes, a new XML based model is proposed which will protect the message legitimacy. The DIS will help to filter the spurious messages from the legitimate messages. The decision inference system as shown in Figure 6.9 gives the detailed overview of the model that how the model actually works. Firstly, each vehicle sends its own information including its speed, acceleration, coordinates *etc.* in an XML file to the XML module located in the corresponding RSU in whose range the vehicle is currently travelling. The dependency module is used to collect information from the vehicles and other RSUs. The XML module in RSU validates the information received from the vehicles and builds a new XML tree according to the credentials verified by it. The inter-RSU XML identifier identifies the correctness of the information received from the the RSUs as well and if any information updation is required, it is updated by the XML update module and the new tree is build by the XML builder. The XML log is maintained by the RSU and if any information about any vehicle is required, it is derived by the query extractor from the XML log. The XML dependency tree is shared among all the RSUs to update the information as the vehicles travel from the region of one RSU to other RSU. Therefore, the updated XML tree should be uploaded on each RSU repeatedly to

avoid any bewilderment. The XML trees from RSUs are transmitted to the trusted authority which is the central repository for the information. The XML assembler module assembles all XML trees obtained from the RSUs and the final tree builder module in trusted authority builds the final XML tree after assembling all the information. The final XML tree by trusted authority is transmitted to all the RSUs for the actual decision making for the authenticity of the messages received.

6.3 V-Health Systems

Vehicular Ad-Hoc Network, an emerging network paradigm is considered as a low cost solution to the problem of connecting devices with each other to provide the end to end connectivity with medical professionals. The technology based ubiquitous patient monitoring is regarded as a viable solution for managing the chronic diseases and medical emergencies in order to economize the healthcare services. The new paradigm of patient monitoring using Vehicular Ad-Hoc Networks (VANETs) for optimization of healthcare services has recently been a popular mainstream for research in tremendous applications. The vital signs and signals of the patient include heart rate, pulse rate, breathing problems, balance disorder, dizziness, body temperature, blood pressure which are measured by the body sensors and transmitted as analog signals over the wireless media. A new wireless patient monitoring service called V-Health System is proposed which utilizes the patient health information collected by the body sensors to securely transmit it to the healthcare services via vehicular ad hoc network. The patient information collected by body sensors are transmitted by the vehicle in the form of XML data to the nearest road side infrastructure for the service selection of the healthcare centres and the information is transmitted to the healthcentres for the appropriate service reply. The XML dependency tree is used for the effective transmission

of patient and medical information in the vehicular ad hoc network. VANETs act as the middleware platform for medical service selection between the patient and the healthcare services for the mobile patients and vehicular users. Thus, the proposed V-Health system provides personalized healthcare services by employing the XML based dependency tree for information transmission. The general information flow and the components in V-Health system using VANETs is shown in Figure 6.10.

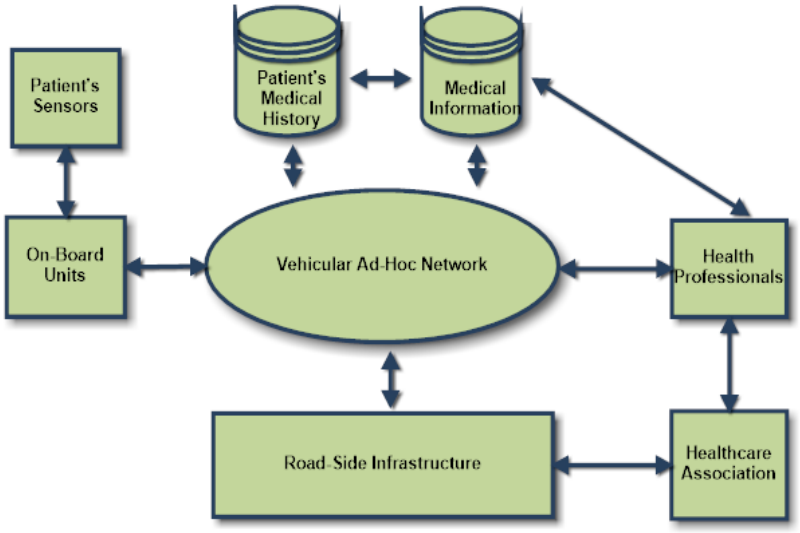

Figure 6.10: The general system model for V-Health system using VANETs

The V-Health system transmits the patient specific personal information from the body sensors to the medical professionals via vehicular ad hoc networks. The onboard unit of the vehicle collects the information from body sensors and transmits the health symptoms of the patient in the form of XML dependency tree. The XML file is generated for each patient by the vehicle and patient record is transmitted in the network to the nearest road side infrastructure. The RSU does the XML parsing of the patient XML and helps in selecting the type of service requested by the patient and the request for that medical service is generated by the road side infrastructure. Thus, the medical service requested is sent to the patient accordingly. The medical database stored at the central repository contains the database of all the patients' record history, patients' latest health statistics *etc.*

6.3.1 Secure Communication Process

The individual vehicle and user is registered with the trusted authority before starting any communication process. Each registered vehicle has identity $V = \{V_1, V_2, V_3....V_n\}$ and each registered user has identity $U = \{U_1, U_2, U_3....U_n\}$ where V and U are the set of registered vehicles and users respectively. The body sensors of the user transmit the information collected to the onboard unit of the vehicle by establishing a shared secret key between them. Let $a \in \mathbb{Z}_q^*$ be the secret key of body sensors and P_s = a.P be the public key of body sensors. Let $b \in \mathbb{Z}_q^*$ be the secret key of onboard unit of vehicle and P_v = b.P be the public key of vehicle. The shared secret key P_k is established by body sensors as $a.P_v$ and by vehicle as $b.P_s$ which can be justified as:

$a.P_v = a.b.P = b.a.P = b.P_s$

Thus, the data is transferred between the body sensors and the vehicle by establishing a shared secret key P_k between them. The shared key is only used between the body sensors and the vehicle. The rest communication in the network among the network entities on the road takes place by means of Public key Cryptography. The information from the body sensors is sent in encrypted form to the vehicle as $ENC_{P_k}(M, U_i) \rightarrow V_i$ which is decrypted by the vehicle as $DEC_k(M, U_i)$. After collecting the information from the body sensors, the vehicle transmits the information to the nearest vehicles and the roadside unit. The information transmitted by the vehicle is digitally signed with the private key of the vehicle and transmitted as $SIG(M, P_{i_{xml}}, V_i, U_i, loc; b) \rightarrow *$. The broadcasted information is authenticated by the vehicles and the nearest RSUs by using the public key of the vehicle. The information received by the RSU is authenticated and verified for the medical services requested by the user. The private key of RSU_i is $y_i \in \mathbb{Z}_q^*$ and the public key is computed as $P_{r_i} = y_i.P$. The RSU identifies the type of service and selects the nearest healthcare unit accordingly. The information is transmitted to the healthcare centre by encrypting it with

the public key of healthcare centre $P_{h_i} = x_i.P$ where x_i is the private key of the health centre H_i and x_i is randomly chosen from $\mathbb{Z}_q^*$. The message transmitted to the healthcare centre is $ENC_{P_h}(M, P_{i_{xml}}, S_{i_{xml}}, V_i, U_i, loc)$ which is analyzed by the health centres and in response to it, the medical response is created in the form of *medical_XML*. The *medical_XML* is sent to the respective RSU_i as $ENC_{P_{r_i}}(M, M_{i_{xml}}, V_i, U_i,$ loc) and the RSU_i after receiving the message decrypts the information and transmits it to the requesting vehicle by encrypting it with the public key of the vehicle. Thus, the secure end to end connectivity is maintained between the healthcare professionals and the mobile patients or users.

6.4 Conclusion

A new fuzzy based trust prediction model has been designed to effectively choose the relay nodes which can be used for routing in the first stage and to choose the appropriate data transmission path based on the trust levels computed for each of the relay nodes in the second stage. The proposed fuzzy based trust model behaves effectively in coordination with DSDV protocol indicating the efficiency and reliability of the proposed scheme. The misbehaviour detection model is proposed namely, DIS to prevent the sharing the false information by the entities in the Vehicular network. The V-health system is proposed for the online monitoring of mobile patients or the vehicular users by adapting the vehicular ad hoc network as the middleware platform. The V-Health system is effective application for VANETs to monitor the emergency events of vehicular users.

Chapter 7

Conclusions and Future Scope

7.1 Conclusions

The entire focus of this thesis has been on securing the vehicular communications in vehicular ad hoc networks. After having a thorough review of various approaches adopted for security of vehicular ad hoc networks, it was realized that the public key cryptography, symmetric key cryptography as well as identity based cryptography approaches had few limitations in securing the communications in vehicular entities. One of the available approaches for enhancing the security of vehicular ad hoc networks is certificateless cryptography. Certificateless cryptography has the advantage that it reduces the certificate overhead and certificate revocation problem of public key cryptography. Moreover, it also solves the key escrow problem of identity based cryptography.

A new efficient certificateless aggregate signature scheme is proposed for vehicular communications. The proposed signature scheme is proven existentially unforgeable against the chosen message attack under the assumption that CDH problem is intractable in the random oracle model. The proposed CLAS scheme is adduced specifically for securing vehicular communications in vehicular ad hoc networks by reducing the signature verification time

drastically and helps in verifying more messages in the specific stipulated time, thus increasing the efficiency of the network. The propounded scheme has much less computational cost in terms of verifying signatures when compared with the already proposed works. This scheme will work efficiently in networks which have limited bandwidth such as vehicular ad-hoc networks.

The proposed certificateless aggregate signature scheme is employed for designing a security framework for enhancing the communication process in vehicular ad hoc networks. The proposed security framework achieves the security requirements of authentication, privacy, non-repudiation and confidentiality. The privacy of the scheme is preserved by using the pseudonyms for communication in the network. The proposed certificateless digital signature scheme is employed for inter-vehicular communication allowing the vehicles to anonymously communicate with each other. The message verification process is improved by employing the bloom filters in the scheme. The analysis of the security scheme is done with various parameters and proposed scheme of bloom filters have major performance improvements compared to the simple aggregate verification scheme thus, assuring the accuracy of the proposed security system.

A new fuzzy based trust prediction model has been designed for vehicular ad hoc networks by employing the concept of choosing the relay nodes for the selection of data transmission path. The trust levels are computed for each of the relay nodes chosen for the selection of best possible data transmission path. The effectiveness of the proposed model has been shown by integrating it with the routing protocols and testing it with the help of various evaluation parameters indicating that DSDV-F performs much effectively compared to AODV-F and DSR-F.

The two XML based modules have been designed for vehicular ad hoc networks which are:

i) The decision inference system for the detection of misbehaving nodes which are transmitting the false information in the network.

ii) The V-health system is proposed by employing the XML dependency tree for the secure transmission of patient specific data to the nearest healthcare centres for the medical emergency.

The major contributions of the thesis are:

i) A privacy preserving authentication based security framework is designed for securing vehicular communications in vehicular ad hoc networks. The framework can be divided into two steps.

   a. A new certificateless aggregate signature scheme is proposed specifically for vehicular ad hoc networks and its security proof has been given in random oracle model.

   b. The security framework employs the use of pseudonyms for anonymity and proposed certificateless signature scheme for authentication purposes. It uses the bloom filters to enhance the signature verification process in vehicular communications.

ii) The proposed signature scheme has been implemented using Miracl library and the proposed security framework is implemented on a simulated environment with major performance improvements compared to other schemes.

iii) The trust prediction model has also been designed to secure vehicular communications along with two XML based modules for the secure VANETs.

7.2 Future Scope

In future, work can be extended on fully decentralized VANET authentication schemes while maintaining the applicable efficiency. The lightweight and efficient authentication scheme

can be designed based on decentralized regional transportation authorities in a particular region to further increase the communication reliability. The efficient position based schemes can also be explored to improve the proposed security framework. The impact of the velocity changes of the vehicles on simulation results can also be studied in the future.

The security framework can be further enhanced to incorporate the defense mechanism against various other attacks applicable in VANETs. An intrusion detection mechanism can be developed against various attacks applicable in VANETs to enhance the network security. The solution to inside attacks in the vehicular ad hoc network can also be given. Further, the proposed framework can also be implemented on real vehicles to obtain real time analysis of the results.

Bibliography

[1] "IEEE 802.11p, amendment to standard for information technology: Telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements, part 11: Wireless lan medium access control (MAC) and physical layer (PHY) specifications," 2010. Amendment 7: Wireless Access in Vehicular Environment, 802.11p, version 2010.

[2] "IEEE 1609.1, IEEE trial-use standard for wireless access in vehicular environments (WAVE): Resource manager," 2006. 1609.1, version 2006.

[3] "IEEE 1609.2, IEEE trial-use standard for wireless access in vehicular environments (WAVE): Security services for applications and management messages," 2006. 1609.2, version 2006.

[4] "IEEE 1609.3, IEEE trial-use standard for wireless access in vehicular environments (WAVE): Networking services," 2007. 1609.3, version 2007.

[5] "IEEE 1609.4, IEEE trial-use standard for wireless access in vehicular environments (WAVE): Multi-channel operation," 2006. 1609.4, version 2006.

[6] L. Zhang, "Research on security and privacy in vehicular ad hoc networks," 2010.

[7] S. Mahajan and A. Jindal, "Security and privacy in VANET to reduce authentication overhead for rapid roaming networks," *International Journal of Computer Applications*, vol. 1, no. 20, pp. 21–25, 2010.

[8] T. Leinmüller, R. K. Schmidt, E. Schoch, A. Held, and G. Schäfer, "Modeling roadside attacker behavior in vanets," in *IEEE GLOBECOM Workshops*, pp. 1–10, IEEE, 2008.

[9] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for VANETs," *Proc. 4th Wksp. Embedded Sec. in Cars*, pp. 15–22, 2006.

[10] P. Papadimitratos, V. Gligor, and J. P. Hubaux, "Securing vehicular communications-assumptions, requirements, and principles," in *Workshop on Embedded Security in Cars (ESCAR)*, no. LCA-CONF-2006-021, pp. 5–14, 2006.

[11] P. Papadimitratos, L. Buttyan, T. S. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[12] K. Plob and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," *Computer Standards and Interfaces*, vol. 30, no. 6, pp. 390–397, 2008.

[13] K. A. Kroh R. and K. F., "VANETs security requirements." http://www.sevecom.org/Pages/ProjectDocuments.html, September 2006. Technical report, Secure Vehicle Communication (Sevecom).

[14] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Privacy enhancing technologies*, pp. 197–209, Springer, 2006.

[15] C. Boyd and A. Mathuria, *Protocols for authentication and key establishment*. Springer Science & Business Media, 2013.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*, pp. 47–53, Springer, 1985.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[18] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Advances in Cryptology-ASIACRYPT*, pp. 514–532, Springer, 2001.

[19] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Cryptography and Coding*, pp. 360–363, Springer, 2001.

[20] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[21] D. R. Stinson, *Cryptography: theory and practice*. CRC press, 2005.

[22] L. C. Washington, *Elliptic curves: number theory and cryptography*. CRC press, 2008.

[23] J. H. Conway and R. Guy, *The book of numbers*. Springer Science & Business Media, 2012.

[24] J. Gallian, *Contemporary abstract algebra*. Cengage Learning, 2009.

[25] G. B. Arfken, *Mathematical methods for physicists*. Academic press, 2013.

[26] J. V. Armitage and W. F. Eberlein, *Elliptic functions*, vol. 67. Cambridge University Press, 2006.

[27] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-ASIACRYPT 2003*, pp. 452–473, Springer, 2003.

[28] J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," *Journal of cryptology*, vol. 20, no. 2, pp. 203–235, 2007.

[29] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*, pp. 47–53, Springer, 1985.

[30] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Advances in cryptology-EUROCRYPT*, pp. 416–432, Springer, 2003.

[31] A. Bagherzandi and S. Jarecki, "Identity-based aggregate and multi-signature schemes based on rsa," in *Public Key Cryptography–PKC 2010*, pp. 480–498, Springer, 2010.

[32] A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum, "Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 276–285, ACM, 2007.

[33] A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham, "Sequential aggregate signatures from trapdoor permutations," in *Advances in Cryptology-Eurocrypt 2004*, pp. 74–90, Springer, 2004.

[34] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Cryptology and Network Security*, pp. 13–25, Springer, 2005.

[35] D. H. Yum and P. J. Lee, "Generic construction of certificateless signature," in *Information Security and Privacy*, pp. 200–211, Springer, 2004.

[36] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Information Security and Privacy*, pp. 235–246, Springer, 2006.

[37] J. K. Liu, M. H. Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model," in *Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 273–283, ACM, 2007.

[38] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signature revisited," in *Information Security and Privacy*, pp. 308–322, Springer, 2007.

[39] K. Y. Choi, J. H. Park, J. Y. Hwang, and D. H. Lee, "Efficient certificateless signature schemes," in *Applied Cryptography and Network Security*, pp. 443–458, Springer, 2007.

[40] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 390–394, 2009.

[41] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Computer Communications*, vol. 32, no. 6, pp. 1079–1085, 2009.

[42] S. Miao, F. Zhang, S. Li, and Y. Mu, "On security of a certificateless signcryption scheme," *Information Sciences*, vol. 232, pp. 475–481, 2013.

[43] H. Xiong, F. Li, and Z. Qin, "Certificateless threshold signature secure in the standard model," *Information Sciences*, vol. 237, pp. 73–81, 2013.

[44] D. He, J. Chen, and J. Hu, "A pairing-free certificateless authenticated key agreement protocol," *International Journal of Communication Systems*, vol. 25, no. 2, pp. 221–230, 2012.

[45] C. Gandhi and M. Dave, "A review of security in mobile ad hoc networks," *IETE Technical review*, vol. 23, no. 6, pp. 335–344, 2006.

[46] J. W.-K. HONG, "Towards management of next generation networks," *IEICE transactions on communications*, vol. 90, no. 11, pp. 3004–3014, 2007.

[47] S.-S. Kim, M.-J. Choi, H.-T. Ju, M. Ejiri, and J. W.-K. Hong, "Towards management requirements of future internet," in *Challenges for Next Generation Network Operations and Service Management*, pp. 156–166, Springer, 2008.

[48] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, vol. 13, no. LCA-ARTICLE-2006-015, pp. 8–15, 2006.

[49] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[50] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[51] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[52] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *The 27th Conference on Computer Communications INFOCOM 2008*, IEEE, 2008.

[53] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. SECON'09.*, pp. 1–9, IEEE, 2009.

[54] Z. Li and C. Chigan, "On resource-aware message verification in VANETs," in *2010 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2010.

[55] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: a robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, 2009.

[56] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *The 27th Conference on Computer Communications. INFOCOM*, IEEE, 2008.

[57] J. H. Cheon and J. H. Yi, "Fast batch verification of multiple signatures," in *Public Key Cryptography–PKC 2007*, pp. 442–457, Springer, 2007.

[58] S.-H. Kim and I.-Y. Lee, "A secure and efficient vehicle-to-vehicle communication scheme using bloom filter in vanets," *International Journal of Security & Its Applications*, vol. 8, no. 2, 2014.

[59] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[60] C.-H. Yeh, M.-Y. Hsieh, and K.-C. Li, "A certificate enhanced group key framework for vehicular ad hoc networks," in *Ubiquitous Information Technologies and Applications*, pp. 215–222, Springer, 2013.

[61] A. A. Wagan and L. T. Jung, "Security framework for low latency vanet applications," in *International Conference on Computer and Information Sciences (ICCOINS)*, pp. 1–6, IEEE, 2014.

[62] H. Lu, J. Li, and M. Guizani, "A novel ID-based authentication framework with adaptive privacy preservation for VANETs," in *Computing, Communications and Applications Conference (ComComAp)*, pp. 345–350, IEEE, 2012.

[63] J. Li, H. Lu, and M. Guizani, "ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[64] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks," *Computer Standards & Interfaces*, vol. 36, no. 3, pp. 513–523, 2014.

[65] X. Xue and J. Ding, "LPA: a new location-based privacy-preserving authentication protocol in VANET," *Security and Communication Networks*, vol. 5, no. 1, pp. 69–78, 2012.

[66] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in wave-enabled vanets," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.

[67] J.-L. Tsai, "An improved cross-layer privacy-preserving authentication in wave-enabled VANETs," *IEEE Communications Letters*, vol. 18, no. 11, pp. 1931–1934, 2014.

[68] A. Wasef, Y. Jiang, and X. Shen, "DCS: an efficient distributed-certificate-service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 533–549, 2010.

[69] S. Bhushan, M. Dave, and R. Patel, "Reducing network overhead with common junction methodology," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 3, no. 3, pp. 51–61, 2011.

[70] N. Chand, R. C. Joshi, and M. Misra, "Cooperative caching in mobile ad hoc networks based on data utility," *Mobile Information Systems*, vol. 3, no. 1, pp. 19–37, 2007.

[71] M. B. Younes and A. Boukerche, "SCOOL: a secure traffic congestion control protocol for VANETs," in *IEEE Wireless Communications and Networking Conference (WCNC),*, pp. 1960–1965, IEEE, 2015.

[72] A. P. Isern-Deyà, L. Huguet-Rotger, M. M. Payeras-Capellà, and M. Mut-Puigserver, "On the practicability of using group signatures on mobile devices: implementation and performance analysis on the android platform," *International Journal of Information Security*, pp. 1–11, 2014.

[73] M.-C. Chuang and J.-F. Lee, "TEAM: trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2014.

[74] X. Zhu, Y. Lu, X. Zhu, and S. Qiu, "Lightweight and scalable secure communication in VANET," *International Journal of Electronics*, vol. 102, no. 5, pp. 765–780, 2015.

[75] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication," *Computing*, pp. 1–24, 2014.

[76] H. Xiong, Z. Qin, and F. Li, "Secure vehicle-to-roadside communication protocol using certificate-based cryptosystem," *IETE Technical Review*, vol. 27, no. 3, pp. 214–219, 2010.

[77] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT professional*, vol. 6, no. 1, pp. 24–29, 2004.

[78] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, no. 3, pp. 49–55, 2004.

[79] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms-ideal and real," in *IEEE 65th Vehicular Technology Conference, VTC2007-Spring.*, pp. 2521–2525, IEEE, 2007.

[80] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pp. 11–21, ACM, 2005.

[81] J. Luo and J.-P. Hubaux, "A survey of inter-vehicle communication," tech. rep., 2004.

[82] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *5th Swiss Transport Research Conference (STRC)*, no. LCA-CONF-2005-012, 2005.

[83] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in vanets," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 67–75, ACM, 2006.

[84] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," tech. rep., DTIC Document, 2005.

[85] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, vol. 13, no. LCA-ARTICLE-2006-015, pp. 8–15, 2006.

[86] S. Eichler, C. Schroth, and J. Eberspächer, "Car-to-car communication," in *VDE-Kongress 2006*, VDE VERLAG GmbH, 2006.

[87] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[88] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Workshop on hot topics in networks (HotNets-IV)*, pp. 1–6, 2005.

[89] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in *European Wireless*, vol. 2, 2002.

[90] L. Gollan and C. Meinel, "Digital signatures for automobiles," in *Proceedings of Systemics, Cybernetics and Informatics*, 2002.

[91] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch, "Security architecture for vehicular communication," in *Workshop on Intelligent Transportation*, 2007.

[92] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, *et al.*, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, 2008.

[93] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *7th International Conference on ITS Telecommunications, ITST'07.*, pp. 1–6, IEEE, 2007.

[94] J. Zhang, C. Chen, and R. Cohen, "A scalable and effective trust-based framework for vehicular ad-hoc networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 1, no. 4, pp. 3–15, 2010.

[95] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, 2005.

[96] "5.9 GHz DSRC." http://grouper.ieee.org/groups/scc32/dsrc/. [Online; accessed 20-August-2015].

[97] "The Network on Wheels (NOW) Project." http://www.network-on-wheels.de/. [Online; accessed June 2015].

[98] "Car 2 Car Communication Consortium." http://www.car-2-car.org/. [Online; accessed 20-August-2015].

[99] "The DSRC Consortium." http://grouper.ieee.org/groups/scc32/dsrc/. [Online; accessed June 2015].

[100] "SEVECOM project." http://www.sevecom.org/. [Online; accessed 20-August-2015].

[101] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in VANETs," in *IEEE International Conference on Wireless and Mobile Computing Networking and Communications. WIMOB'08*, pp. 508–513, IEEE, 2008.

[102] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pp. 79–87, ACM, 2005.

[103] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, *et al.*, "Mix-zones for location privacy in vehicular networks," 2007.

[104] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "MLAS: Multiple level authentication scheme for VANETs," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1445–1456, 2012.

[105] C. Hu, T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Efficient HMAC-based secure communication for VANETs," *Computer Networks*, vol. 56, no. 9, pp. 2292–2303, 2012.

[106] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *Communications Magazine*, vol. 46, no. 4, pp. 88–95, 2008.

[107] P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith, "Blacklistable anonymous credentials: blocking misbehaving users without ttps," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 72–81, ACM, 2007.

[108] J. Sun and Y. Fang, "A defense technique against misbehavior in vanets based on threshold authentication," in *Military Communications Conference MILCOM*, pp. 1–7, IEEE, 2008.

[109] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," in *Military Communications Conference MILCOM*, pp. 1–7, IEEE, 2007.

[110] J. Sun and Y. Fang, "Defense against misbehavior in anonymous vehicular ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1515–1525, 2009.

[111] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "EPA: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks," *Pervasive and Mobile Computing*, 2014.

[112] R. C. Merkle, "A certified digital signature," in *Advances in CryptologyCRYPTO89 Proceedings*, pp. 218–238, Springer, 1990.

[113] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings," in *Advances in cryptologyASIACRYPT 2002*, pp. 533–547, Springer, 2002.

[114] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *Securecomm and Workshops, 2006*, pp. 1–5, IEEE, 2006.

[115] X. Chen, F. Zhang, and K. Kim, "A New ID-based Group Signature Scheme from Bilinear Pairings," *IACR Cryptology ePrint Archive*, vol. 2003, p. 116, 2003.

[116] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[117] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pp. 94–95, ACM, 2006.

[118] N. I. Shuhaimi and T. Juhana, "Security in vehicular ad-hoc network with identity-based cryptography approach: A survey," in *7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, pp. 276–279, IEEE, 2012.

[119] J. Choi and S. Jung, "A security framework with strong non-repudiation and privacy in VANETs," in *6th Consumer Communications and Networking Conference, CCNC 2009.*, pp. 1–5, IEEE, 2009.

[120] M. Dikmak, Z. Sabra, A. Kayssi, and A. Chehab, "Optimized conditional privacy preservation in VANETs," in *19th International Conference on Telecommunications (ICT)*, pp. 1–6, IEEE, 2012.

[121] O. Gavril, "Security in vanet," tech. rep., Polytehnica University of Bucharest, 2009. Graduation project.

[122] Y. Park, K.-H. Rhee, and C. Sur, "A secure and location assurance protocol for location-aware services in VANETs," in *Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, pp. 456–461, IEEE, 2011.

[123] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security*, vol. 6, no. 4, pp. 213–241, 2007.

[124] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Advances in cryptologyASIACRYPT*, pp. 548–566, Springer, 2002.

[125] A. Bradai and H. Afifi, "A Framework Using IBC Achieving Non-Repudiation and Privacy in Vehicular Network," in *Conference on Network and Information Systems Security (SAR-SSI)*, pp. 1–6, IEEE, 2011.

[126] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "SPECS: secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 189–203, 2011.

[127] H. Liu, H. Li, and Z. Ma, "Efficient and secure authentication protocol for vanet," in *International Conference on Computational Intelligence and Security (CIS)*, pp. 523–527, IEEE, 2010.

[128] R. N. Salma, N. A. Balaji, and R. Sukumar, "A framework for authentication in vehicular ad-hoc network using identity based approach," *IOSR Journal of Engineering*, vol. 3, no. 7, pp. 15–19, 2013.

[129] A. Chaudhuri, S. DasGupta, and S. Saha, "Identity based secure algorithm for VANET," *Procedia Engineering*, vol. 38, pp. 165–171, 2012.

[130] Y.-H. Lee, H. Kim, B. Chung, J. Lee, and H. Yoon, "On-demand secure routing protocol for ad hoc network using id based cryptosystem," in *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.*, pp. 211–215, IEEE, 2003.

[131] D. Huang, S. Misra, M. Verma, and G. Xue, "Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[132] S. Mohanty and D. H. S. Panigrahy, "A secure RSU-Aided aggregation and batch-verification scheme for vehicular networks," in *International Conference on Soft Computing and its Applications (ICSCA2012)*, pp. 174–178, 2012.

[133] S. Taha and X. Shen, "A link-layer authentication and key agreement scheme for mobile public hotspots in NEMO based VANET," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 1004–1009, IEEE, 2012.

[134] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.

[135] S. S. D. Selvi, S. S. Vivek, V. K. Pradhan, and C. P. Rangan, "Efficient certificateless online/offline signature with tight security," *Journal of Internet Services and Information Security (JISIS)*, vol. 3, no. 1, p. 2, 2013.

[136] W. XIONG, "Certificate-less based private querying in vanets," pp. 53–62, 2013.

[137] H.-R. Tseng, R.-H. Jan, W. Yang, and E. Jou, "A secure aggregated message authentication scheme for vehicular ad-hoc networks," in *18th World congress on Intelligent Transportation systems*, pp. 1–14, 2011.

[138] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[139] N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 9, 2009.

[140] T. Yang, W. Xin, L. Yu, Y. Yang, J. Hu, and Z. Chen, "MisDis: An Efficent Misbehavior Discovering Method Based on Accountability and State Machine in VANET," in *Web Technologies and Applications*, pp. 583–594, Springer, 2013.

[141] L.-S. Shao, L. Zhou, J.-F. Zhao, B. Xie, and H. Mei, "Web service QoS prediction approach," *Journal of Software*, vol. 20, no. 8, pp. 2062–2073, 2009.

[142] E. Keogh and S. Kasetty, "On the need for time series data mining benchmarks: a survey and empirical demonstration," *Data Mining and knowledge discovery*, vol. 7, no. 4, pp. 349–371, 2003.

[143] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for vanets," in *IEEE 10th International Conference on Computer and Information Technology (CIT)*, pp. 832–837, IEEE, 2010.

[144] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 41, no. 3, pp. 407–420, 2011.

[145] R. S. Bali, N. Kumar, and J. J. Rodrigues, "An efficient energy-aware predictive clustering approach for vehicular ad hoc networks," *International Journal of Communication Systems*, 2015.

[146] J. Zhang and Y. Xu, "Privacy-preserving authentication protocols with efficient verification in VANETs," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 3676–3692, 2014.

[147] A. K. Malhi and S. Batra, "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks," *Discrete Mathematics & Theoretical Computer Science*, vol. 17, no. 1, pp. 317–338, 2015.

[148] M. A. Alawi, R. Saeed, A. A. Hassan, R. A. Alsaqour, *et al.*, "Simplified gateway selection scheme for multihop relay in vehicular ad hoc network," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 3855–3873, 2014.

[149] K.-L. Wang, T.-P. Wang, and C.-C. Tseng, "Reducing wireless multi-hop delay via RSU re-routing in vehicular wireless networks," *International Journal of Communication Systems*, 2014.

[150] S. Nepal, W. Sherchan, J. Hunklinger, and A. Bouguettaya, "A fuzzy trust management framework for service web," in *IEEE International Conference on Web Services*, pp. 321–328, IEEE, 2010.

[151] A. A. Pouyan and M. Yadollahzadeh Tabari, "FPN-SAODV: using fuzzy petri nets for securing AODV routing protocol in mobile Ad hoc network," *International Journal of Communication Systems*, 2015.

[152] T. Gazdar, A. Benslimane, A. Rachedi, and A. Belghith, "A trust-based architecture for managing certificates in vehicular ad hoc networks," in *International Conference on Communications and Information Technology (ICCIT)*, pp. 180–185, IEEE, 2012.

[153] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *The 27th Conference on Computer Communications, INFOCOM*, IEEE, 2008.

[154] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, 2013.

[155] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications*, vol. 7, no. 3, pp. 229–242, 2014.

[156] D. Easley and J. Kleinberg, *Networks, crowds, and markets: Reasoning about a highly connected world*. Cambridge University Press, 2010.

[157] D. Acemoglu, M. A. Dahleh, I. Lobel, and A. Ozdaglar, "Bayesian learning in social networks," *The Review of Economic Studies*, vol. 78, no. 4, pp. 1201–1236, 2011.

[158] R. H. Khokhar, R. M. Noor, K. Z. Ghafoor, C.-H. Ke, and M. A. Ngadi, "Fuzzy-assisted social-based routing for urban vehicular environments," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, pp. 1–15, 2011.

[159] S. Jain, M. Chawla, V. N. Soares, and J. J. Rodrigues, "Enhanced fuzzy logic-based spray and wait routing protocol for delay tolerant networks," *International Journal of Communication Systems*, 2014.

[160] G. Li, M. Ma, C. Liu, and Y. Shu, "Adaptive fuzzy multiple attribute decision routing in VANETs," *International Journal of Communication Systems*, 2015.

[161] X. Anita, M. Bhagyaveni, and J. Manickam, "Fuzzy-based trust prediction model for routing in WSNs," *The Scientific World Journal*, vol. 2014, 2014.

[162] I. AlShawi, L. Yan, W. Pan, and B. Luo, "Fuzzy chessboard clustering and artificial bee colony routing method for energy-efficient heterogeneous wireless sensor networks," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 3581–3599, 2014.

[163] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An efficient biometric authentication protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[164] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems*, 2015.

[165] M. Gerlach, "Trust for vehicular applications," in *Eighth International Symposium on Autonomous Decentralized Systems, 2007. ISADS'07*, pp. 295–304, IEEE, 2007.

[166] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad-hoc networks," *International Journal of Computational Intelligence Theory and Practice*, vol. 5.

[167] A. Tajeddine, A. Kayssi, and A. Chehab, "A privacy-preserving trust model for vanets," in *10th International Conference on Computer and Information Technology (CIT)*, pp. 832–837, IEEE, 2010.

[168] A. A. Wagan, B. M. Mughal, and H. Hasbullah, "Vanet security framework for trusted grouping using tpm hardware," in *Second International Conference on Communication Software and Networks, 2010. ICCSN'10.*, pp. 309–312, IEEE, 2010.

[169] Q. Wu, J. Domingo-Ferrer, and Ù. González-Nicolá, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 559–573, 2010.

[170] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *The 27th Conference on Computer Communications INFOCOM 2008*, IEEE, 2008.

[171] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pp. 29–37, ACM, 2004.

[172] C. Chen, J. Zhang, R. Cohen, and P.-H. Ho, "A trust modeling framework for message propagation and evaluation in VANETs," in *2nd International Conference on Information Technology Convergence and Services (ITCS)*, pp. 1–8, IEEE, 2010.

[173] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pp. 1–8, IEEE, 2006.

[174] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Computer Networks*, vol. 54, no. 14, pp. 2482–2491, 2010.

[175] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*, pp. 251–260, Springer, 2002.

[176] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259–268, ACM, 2004.

[177] G. Yan, S. Olariu, and M. C. Weigle, "Providing vanet security through active position detection," *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, 2008.

[178] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting sybil attacks in vanets," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, 2013.

[179] N. El Zoghby, V. Cherfaoui, B. Ducourthial, and T. Denoeux, "Distributed data fusion for detecting sybil attacks in VANETs," in *Belief Functions: Theory and Applications*, pp. 351–358, Springer, 2012.

[180] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 1–8, ACM, 2006.

[181] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *IEEE Military Communications Conference. MILCOM*, pp. 1–7, IEEE, 2009.

[182] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban vanets," in *29th IEEE International Conference on Distributed Computing Systems Workshops, ICDCS Workshops' 09*, pp. 270–276, IEEE, 2009.

[183] G. Guette and B. Ducourthial, "On the sybil attack detection in VANET," in *IEEE International Conference on Mobile Adhoc and Sensor Systems, MASS 2007*, pp. 1–6, IEEE, 2007.

[184] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within VANET," *IJ Network Security*, vol. 9, no. 1, pp. 22–33, 2009.

[185] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAPsybil attacks detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, 2011.

[186] N.-W. Lo and H.-C. Tsai, "Illusion attack on vanet applications-a message plausibility problem," in *IEEE Globecom Workshops*, pp. 1–8, IEEE, 2007.

[187] M. Elsa Mathew, M. tech and A. Raj Kumar P, "Truc: Towards trusted communication for emergency scenarios in vehicular adhoc networks (vanets) against illusion attack," in *Qatar Foundation Annual Research Conference*, no. 1, p. ITPP1109, 2014.

[188] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications INFOCOM*, vol. 3, pp. 1976–1986, IEEE, 2003.

[189] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET," in *First Asian Himalayas International Conference on Internet. AH-ICI*, pp. 1–6, IEEE, 2009.

[190] H. S. Chiu and K.-S. Lui, "DelPHI: wormhole detection mechanism for ad hoc wireless networks," in *2006 1st international symposium on Wireless pervasive computing*, pp. 6–11, IEEE, 2006.

[191] A. Chinnasamy, S. Prakash, and P. Selvakumari, "Enhance trust based routing techniques against sinkhole attack in AODV based VANET," *International Journal of Computer Applications Volume (0975–8887)*, pp. 22–28, 2013.

[192] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 22–28, 2010.

[193] A. Khan, "Minimization of denial of services attacks in vehicular adhoc networking by applying different constraints," *International Journal of Academic Research in Business and Social Sciences*, vol. 3, no. 7, p. 662, 2013.

[194] S. Biswas, J. Misic, and V. B. Misic, "DDoS attack on WAVE-enabled VANET through synchronization," in *IEEE Global Communications Conference (GLOBECOM)*, pp. 1079–1084, IEEE, 2012.

[195] N. Alsharif, A. Wasef, and X. S. Shen, "Mitigating the effects of position-based routing attacks in vehicular ad hoc networks," in *IEEE International Conference on Communications (ICC)*, pp. 1–5, IEEE, 2011.

[196] V. M. Igure and R. D. Williams, "Taxonomies of attacks and vulnerabilities in computer systems," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 1, pp. 6–19, 2008.

[197] A. Tomandl, K.-P. Fuchs, and H. Federrath, "REST-Net: A dynamic rule-based IDS for VANETs," in *7th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 1–8, IEEE, 2014.

[198] H. Sedjelmaci and S. M. Senouci, "A new intrusion detection framework for vehicular networks," in *IEEE International Conference on Communications (ICC)*, pp. 538–543, IEEE, 2014.

[199] R. Coussement, B. Amar Bensaber, and I. Biskri, "Decision support protocol for intrusion detection in VANETs," in *Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications*, pp. 31–38, ACM, 2013.

[200] N. Deb, M. Chakraborty, and N. Chaki, "CORIDS: a cluster-oriented reward-based intrusion detection system for wireless mesh networks," *Security and Communication Networks*, vol. 7, no. 3, pp. 532–543, 2014.

[201] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1–23, 2014.

[202] N. Bißmeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in *IEEE Vehicular Networking Conference (VNC)*, pp. 166–173, IEEE, 2010.

[203] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014.

[204] S. Ruj, M. Cavenaghi, Z. Huang, A. Nayak, I. Stojmenovic, *et al.*, "On data-centric misbehavior detection in VANETs," in *IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, IEEE, 2011.

[205] S. Misra, P. V. Krishna, and K. I. Abraham, "A stochastic learning automata-based solution for intrusion detection in vehicular ad hoc networks," *Security and Communication Networks*, vol. 4, no. 6, pp. 666–677, 2011.

[206] K. Verma, H. Hasbullah, and A. Kumar, "Prevention of DoS attacks in VANET," *Wireless personal communications*, vol. 73, no. 1, pp. 95–126, 2013.

[207] K. Verma and H. Hasbullah, "Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET," *Security and Communication Networks*, vol. 8, no. 5, pp. 864–878, 2015.

[208] S. Sanyal, D. Gada, R. Gogri, P. Rathod, Z. Dedhia, and N. Mody, "Security scheme for distributed dos in mobile ad hoc networks," *arXiv preprint arXiv:1005.0109*, 2010.

[209] S. K. Harit, G. Singh, and N. Tyagi, "Fox-hole model for data-centric misbehaviour detection in VANETs," in *Third International Conference on Computer and Communication Technology (ICCCT)*, pp. 271–277, IEEE, 2012.

[210] N. Bissmeyer, K. H. Schroder, J. Petit, S. Mauthofer, and K. M. Bayarou, "Short paper: Experimental analysis of misbehavior detection and prevention in VANETs," in *IEEE Vehicular Networking Conference (VNC)*, pp. 198–201, IEEE, 2013.

[211] S. Dietzel, J. Petit, G. Heijenk, and F. Kargl, "Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1505–1518, 2013.

[212] J. Zhang, L. Huang, H. Xu, M. Xiao, and W. Guo, "An incremental bp neural network based spurious message filter for VANET," in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 360–367, IEEE, 2012.

[213] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of Intelligent Transportation Systems Research*, vol. 10, no. 1, pp. 11–21, 2012.

[214] G. Welch and G. Bishop, "An introduction to the kalman filter. 2006," *University of North Carolina: Chapel Hill, North Carolina, US*, 2006.

[215] R. Hussain, S. Kim, and H. Oh, "Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice," in *Information Security Applications*, pp. 296–311, Springer, 2012.

[216] M. A. Razzaque, F. A. Ghaleb, and A. Zainal, "Mobility pattern based misbehavior detection to avoid collision in vehicular ad hoc networks," in *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*, pp. 300–303, Springer, 2014.

[217] R. Kumar, M. Misra, and A. K. Sarje, "A simplified analytical model for end-to-end delay analysis in manet," *IJCA Special Issue on Mobile Ad-hoc Networks MANETs*, pp. 195–199, 2010.

[218] C. Baru, N. Botts, T. Horan, K. Patrick, and S. S. Feldman, "A seeded cloud approach to health cyberinfrastructure: Preliminary architecture design and case applications," in *45th Hawaii International Conference on System Science (HICSS)*, pp. 2727–2734, IEEE, 2012.

[219] H. Abid, L. T. T. Phuong, J. Wang, S. Lee, and S. Qaisar, "V-cloud: vehicular cyber-physical systems and cloud computing," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, p. 165, ACM, 2011.

[220] J. Barrachina, P. Garrido, M. Fogue, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "VEACON: a vehicular accident ontology designed to improve safety on the roads," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1891–1900, 2012.

[221] G. Anogianakis, S. Maglavera, and A. Pomportsis, "Relief for maritime medical emergencies through telematics," *IEEE Transactions on Information Technology in Biomedicine*, vol. 2, no. 4, pp. 254–260, 1998.

[222] K. Hung and Y.-T. Zhang, "Implementation of a WAP-based telemedicine system for patient monitoring," *IEEE Transactions on Information Technology in Biomedicine*, vol. 7, no. 2, pp. 101–107, 2003.

[223] C. Pattichis, E. Kyriacou, S. Voskaride, M. Pattichis, R. Istepanian, and C. N. Schizas, "Wireless telemedicine systems: an overview," *Antennas and Propagation Magazine*, vol. 44, no. 2, pp. 143–153, 2002.

[224] S. Pavlopoulos, E. Kyriacou, A. Berler, S. Dembeyiotis, and D. Koutsouris, "A novel emergency telemedicine system based on wireless communication technology-ambulance," *IEEE Transactions on Information Technology in Biomedicine*, vol. 2, no. 4, pp. 261–267, 1998.

[225] R.-G. Lee, H.-S. Chen, C.-C. Lin, K.-C. Chang, and J.-H. Chen, "Home telecare system using cable television plants-an experimental field trial," *IEEE Transactions on Information Technology in Biomedicine*, vol. 4, no. 1, pp. 37–44, 2000.

[226] S. Khoor, J. Nieberl, K. Fügedi, and E. Kail, "Telemedicine ECG-telemetry with Bluetooth technology," in *Computers in Cardiology*, pp. 585–588, IEEE, 2001.

[227] B. Pandey and R. Mishra, "An integrated intelligent computing method for the detection and interpretation of ECG based cardiac diseases," *International Journal of Knowledge Engineering and Soft Data Paradigms*, vol. 2, no. 2, pp. 182–203, 2010.

[228] M. Modarreszadeh and R. N. Schmidt, "Wireless, 32-channel, EEG and epilepsy monitoring system," in *Proceedings of the 19th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, vol. 3, pp. 1157–1160, IEEE, 1997.

[229] J. Pollard, S. Rohman, and M. Fry, "A web-based mobile medical monitoring system," in *International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pp. 32–35, IEEE, 2001.

[230] G. Mendoza and B. Tran, "In-home wireless monitoring of physiological data for heart failure patients," in *Proceedings of the Second Joint Engineering in medicine and biology, 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society EMBS/BMES Conference*, vol. 3, pp. 1849–1850, IEEE, 2002.

[231] O. Boric-Lubeke and V. M. Lubecke, "Wireless house calls: using communications technology for health care and monitoring," *IEEE Microwave Magazine*, vol. 3, no. 3, pp. 43–48, 2002.

[232] K. J. Cho and H. H. Asada, "Wireless, battery-less stethoscope for wearable health monitoring," in *Proceedings of the IEEE 28th Annual Northeast Bioengineering Conference*, pp. 187–188, IEEE, 2002.

[233] S. Rhee, B.-H. Yang, K. Chang, and H. H. Asada, "The ring sensor: a new ambulatory wearable sensor for twenty-four hour patient monitoring," in *Proceedings of the 20th Annual International Conference of the Engineering in Medicine and Biology Society*, vol. 4, pp. 1906–1909, IEEE, 1998.

[234] E. Jovanov, A. O. Donnel, A. Morgan, B. Priddy, and R. Hormigo, "Prolonged telemetric monitoring of heart rate variability using wireless intelligent sensors and a mobile gateway," in *Proceedings of the Second Joint Engineering in Medicine and Biology, 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society EMBS/BMES Conference*, vol. 3, pp. 1875–1876, IEEE, 2002.

[235] E. Jovanov, A. O. Lords, D. Raskovic, P. G. Cox, R. Adhami, and F. Andrasik, "Stress monitoring using a distributed wireless intelligent sensor system," *IEEE Engineering in Medicine and Biology Magazine*, vol. 22, no. 3, pp. 49–55, 2003.

[236] C. Bielza, J. A. F. del Pozo, and P. J. Lucas, "Explaining clinical decisions by extracting regularity patterns," *Decision Support Systems*, vol. 44, no. 2, pp. 397–408, 2008.

[237] S. Brahnam, C.-F. Chuang, R. S. Sexton, and F. Y. Shih, "Machine assessment of neonatal facial expressions of acute pain," *Decision Support Systems*, vol. 43, no. 4, pp. 1242–1254, 2007.

[238] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Certificateless signature: a new security model and an improved generic construction," *Designs, Codes and Cryptography*, vol. 42, no. 2, pp. 109–126, 2007.

[239] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic, and S. Khan, "Timestamp authentication protocol for remote monitoring in ehealth," in *Second International Conference on Pervasive Computing Technologies for Healthcare, 2008. Pervasive-Health*, pp. 73–76, IEEE, 2008.

[240] D. Niyato, E. Hossain, and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 412–423, 2009.

[241] X. Hu, X. Li, E. C. Ngai, J. Zhao, V. Leung, and P. Nasiopoulos, "Health drive: Mobile healthcare onboard vehicles to promote safe driving," in *48th Hawaii International Conference on System Sciences (HICSS)*, pp. 3074–3083, IEEE, 2015.

[242] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365–378, 2009.

[243] R. Lu, X. Lin, and X. Shen, "SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614–624, 2013.

[244] M. Masi, R. Pugliese, and F. Tiezzi, "A standard-driven communication protocol for disconnected clinics in rural areas," in *13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom)*, pp. 304–311, IEEE, 2011.

[245] S. Sneha and U. Varshney, "Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges," *Decision Support Systems*, vol. 46, no. 3, pp. 606–619, 2009.

[246] S. Sneha and U. Varshney, "A framework for enabling patient monitoring via mobile ad hoc network," *Decision Support Systems*, vol. 55, no. 1, pp. 218–234, 2013.

[247] A. Z. Doorenbos, A. Kundu, L. H. Eaton, G. Demiris, E. A. Haozous, C. Towle, and D. Buchwald, "Enhancing access to cancer education for rural healthcare providers via telehealth," *Journal of Cancer Education*, vol. 26, no. 4, pp. 682–686, 2011.

[248] M. Barua, X. Liang, R. Lu, and X. S. Shen, "RCare: Extending Secure Health Care to Rural Area Using VANETs," *Mobile Networks and Applications*, vol. 19, no. 3, pp. 318–330, 2014.

[249] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM conference on Computer and communications security*, pp. 62–73, ACM, 1993.

[250] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in cryptology*, pp. 10–18, Springer, 1985.

[251] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[252] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology - CRYPTO 2001*, pp. 213–229, Springer, 2001.

[253] S. K. Pal, P. Sardana, and K. Yadav, "Efficient multilingual keyword search using bloom filter for cloud computing applications," in *Fourth International Conference on Advanced Computing (ICoAC)*, pp. 1–7, IEEE, 2012.

[254] A. Papadimitriou, F. Le Fessant, A. C. Viana, and C. Sengul, "Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks," in *5th IEEE Workshop on Secure Network Protocols, NPSec*, pp. 43–48, IEEE, 2009.

[255] N. Alam, A. Tabatabaei Balaei, and A. G. Dempster, "Relative positioning enhancement in VANETs: A tight integration approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 47–55, 2013.

[256] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," in *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD*, vol. 3, pp. 188–193, IEEE, 2007.

[257] "Shamus Software. MIRACL library." http://www.certivox.com. [Online; accessed 20-August-2015].

List of Publications

Refereed Journals

1) Avleen Kaur Malhi and Shalini Batra, "An Efficient Certificateless Aggregate Signature Scheme for Vehicular Ad-Hoc Networks", Discrete Mathematics and Theoretical Computer Science- SCIE Indexed, Volume 17, no. 1, 2015, pp. 317-338. (IF:0.324)

2) Avleen Kaur Malhi and Shalini Batra, "Privacy-preserving authentication framework using bloom filter for secure vehicular communications." International Journal of Information Security- SCIE Indexed, 2015, pp. 1-21.(IF:0.963)

3) Avleen Kaur Malhi and Shalini Batra, "Fuzzy Based Trust Prediction for Effective Coordination in Vehicular Ad-Hoc Networks", International Journal of Communication Systems, Wiley- SCIE Indexed, 2016.(IF:1.106)

Conferences

4) Avleen Kaur Malhi and Shalini Batra, "A survey of approaches to secure Vehicular Networks with Identity based Cryptography", in: *Proceedings of IEEE International Conference on Emerging Trends in Engineering and Applied Sciences*, 27-28 December, 2013, Jaipur, India.

5) Avleen Kaur Malhi and Shalini Batra, "Decision Inference System for Misbehaviour Detection in VANETs", in: *Proceedings of 2nd IEEE International Conference on Electronics and Communication Systems*, 26-27 February, 2015, Coimbatore, India, pp. 1557-1562.

6) Avleen Kaur Malhi and Shalini Batra, "XML based Wireless Patient Monitoring System using Vehicular Ad-Hoc Networks", in: *Proceedings of 14th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2015)*, 26-28 October, 2015, Liverpool, UK, pp. 1087-1094.

Posters

7) Avleen Kaur Malhi and Shalini Batra, "A Framework for Secure Vehicular Communication Systems", Poster presented at Grace Hopper Conference on 2-4 December, 2015 at Bangalore, India.[Best Poster Award]

8) Avleen Kaur Malhi and Shalini Batra, "Certificateless Aggregate Signature Scheme for VANETs", Poster presented at TCS Innovation Labs, Bangalore, India on 17 July, 2015.

9) Avleen Kaur Malhi and Shalini Batra, "Misbehaviour Detection in Vehicular Ad-Hoc Networks", Poster presented at 3rd ACM Security and Privacy Symposium 2015 on 13-14 February, 2015 at IIIT Delhi, India.

10) Avleen Kaur Malhi and Shalini Batra, "A Security Framework for Vehicular Communication", Poster presented at TCS annual meet, SANGAM-2014 on 12-13 December, 2014 at Bangalore, India.