STATUS OF THESIS

Title of thesis | VANET SECURITY FRAMEWORK FOR LOW LATENCY SAFETY APPLICATIONS

I ASIF ALI WAGAN

hereby allow my thesis to be placed at the information Resource Center (IRC) of Universiti Teknologi PETRONAS (UTP) with the following conditions:

1. The thesis becomes the property of UTP
2. The IRC of UTP may make copies of the thesis for academic purposes only.
3. This thesis is classified as

☐ Confidential

☑ Non-confidential

If the thesis is confidential, please state the reason:

_____
_____
_____

The contents of the thesis will remain confidential for _____years.
Remarks on disclosure:

_____
_____
_____

Endorsed by

_____ _____

Signature of Author
Permanent Address:
House No D 103/104 New Quest
Colony Nawabshah, Sindh.
Date: _____

Signature of Supervisor
Name of Supervisor
Dr. Halabi Bin Hasbullah.

Date: _____

UNIVERSITI TEKNOLOGI PETRONAS

VANET SECURITY FRAMEWORK FOR LOW LATENCY SAFETY APPLICATIONS

by

ASIF ALI WAGAN

The undersigned certify that they have read, and recommend to the Postgraduate Studies Program for acceptance of this thesis for the fulfillment of the requirements for the degree stated.

Signature: _____

Main Supervisor: Dr. Halabi Bin Hasbullah

Signature: _____

Head of Department: Assoc.Prof. Mohd Fadzil Bin Hassan

Date: _____

VANET SECURITY FRAMEWORK FOR LOW LATENCY SAFETY APPLICATIONS

by

ASIF ALI WAGAN

A Thesis

Submitted to the Postgraduate Studies Programme

as a Requirement for the Degree of

MASTER OF SCIENCE

INFORMATION TECHNOLOGY

UNIVERSITI TEKNOLOGI PETRONAS

BANDAR SERI ISKANDAR,

PERAK, MALAYSIA

FEBRUARY 2012

DECLARATION OF THESIS

Title of thesis | VANET SECURITY FRAMEWORK FOR LOW LATENCY SAFETY APPLICATIONS

I ASIF ALI WAGAN

hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTP or other institutions.

Witnessed by

_____ _____

Signature of Author

Permanent Address: House No D.104/105,Quest Colony, Airport Road, Nawabshah, Pakistan.

Signature of Supervisor

Name of Supervisor

Dr. Halabi Bin Hasbullah

Date: _____ Date: _____

DEDICATION

I would like to dedicate this master dissertation to my beloved Father Imdad Ali Wagan, and Mother Ruqiya Imdad.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Almighty Allah for giving me the patience, ingenuity and environment to complete this research work. I would like to thank my supervisor, Dr. Halabi Hasbullah for his help and guidance, which he has provided with great patience and diligence. I would also like to thank Mr. Bilal Munir Mughal, my good friend, for his moral and practical support throughout the degree.

At the same time, I would like to thank my dear friends Mr. Aamir Amin, Mr. Asif Iqbal, Mr. Asim Qureshi, Mr. Aamir Malik, Ms. Goay Xuan Hui, Mr. Jahanzeb Anwer, Mr. Muhammad Imran Khan, Mr. Haseeb Dilshad, Mr. Mubasshir Rehman, Mr. Nazabat Hussain, Mr. Sohail Safdar, Mr. Ahsan Abro, Mr. Sohail Memon and Mr. Usman Khalid. They have been a source of love and moral support during my studies at Universiti Teknologi PETRONAS (UTP). At last, I owe a deep debt of gratitude to Universiti Teknologi PETRONAS (UTP) for providing me the monetary resources and infrastructure to complete this research work.

ABSTRACT

Vehicular Ad hoc Network (VANET) is a communication network for vehicles on the road. The concept of VANET is to create communication between vehicles, such as one vehicle is able to inform another vehicle about the road conditions. Communication is possible by vehicle to vehicle (V2V) and vehicle to road side unit (V2R). Presently, VANET technology is surrounded with security challenges and it is essentially important for VANET to successfully implement a security measure according to the safety applications requirements. Many researchers have proposed a number of solutions to counter security attacks and also to improve certain aspects of security i.e. authentication, privacy, and non-repudiation. The current most suitable security scheme for VANET is an Elliptic Curve Digital Signature Algorithm (ECDSA) asymmetric security mechanism. ECDSA is small in key size but it provides the same level of security as the large key sized scheme. However ECDSA is associated with high computational cost, thus lacking applicability in life-critical safety messaging. Due to that reason, alternative security schemes have been proposed, such as symmetric methods which provide faster communication, but at the expense of reduced security. Hence, hybrid and hardware based solutions have been proposed by researchers to mitigate the issue. However, these solutions still do not satisfy the existing safety applications standard or have larger message size due to increased message drop ratio.

In this thesis, a security framework is presented; one that uses both standard asymmetric PKI and symmetric cryptography for faster and secured safety message exchange. The proposed framework is expected to improve the security mechanism in VANET by developing trust relationship among the neighboring nodes, hence forming trusted groups. The trust is established via Trusted Platform Module (TPM) and group communication.

In this study, the proposed framework methods are simulated using two propagation models, i.e. two ray ground model and Nakagami model for VANET environment (802.11p). In this simulation, two traffic scenarios such as highway and urban are established. The outcome of both simulation scenarios is analyzed to identify the performance of the proposed methods in terms of latency (End-to-End Delay and Processing Delay). Also, the proposed V2V protocol for a framework is validated using a software in order to establish trust among vehicles.

ABSTRAK

Rangkaian Ad hoc kenderaan (VANET) ialah satu rangkaian komunikasi untuk kenderaan di jalanraya. Konsep VANET ialah untuk mengwujudkan komunikasi antara kenderaan, supaya sebuah kenderaan boleh memaklumkan keadaan jalan kepada sebuah kenderaan lain. Komunikasi boleh berlaku antara kenderaan ke kenderaan (V2V) atau kenderaan ke unit tepi jalan (V2R). Buat masa ini, teknologi VANET dikelilingi dengan cabaran keselamatan dan adalah amat penting untuk VANET berjaya melaksanakan sebuah rangka keselamatan yang menepati keperluan penggunaan keselamatan. Ramai penyelidik telah mencadangkan beberapa penyelesaian untuk menangani serangan keselamatan ini dan juga untuk meningkatkan beberapa aspek keselamatan seperti pengesasihan, privasi dan tanpa sangkalan. Skema keselamatan terkini yang paling sesuai untuk VANET ialah mekanisma keselamatan asimetri ECDSA. ECDSA mempunyai saiz kekunci yang kecil tetapi ia mempunyai tahap keselamatan yang sama seperti skema berkekunci besar. Tetapi ECDSA dikaitkan dengan kos pengkomputeran yang tinggi, maka ia kurang mendapat aplikasi dalam penyampaian mesej keselamatan genting hayat. Oleh sebab tersebut, skema keselamatan alternatif telah dikemukakan, seperti kaedah simetri yang memberi komunikasi lebih cepat tetapi menjejaskan faktor keselamatan. Justeru, penyelasaian berdasarkan hibrid dan perkakasan telah dicadangkan oleh para penyelidik untuk mengurangkan masalah tersebut. Namun, penyelesaian tersebut masih belum dapat memenuhi piawaian keselamatan sedia ada atau mempunyai mesej bersaiz besar yang disebabkan oleh peningkatan dalam nisbah turunan mesej.

Di dalam tesis ini, sebuah rangka kerja keselamatan dikemukakan; sebuah rangka kerja yang menggunakan kedua-dua PKI asimetri dan kriptografi simetri untuk pertukaran mesej yang lebih cepat dan terjamin selamat. Rangka kerja yang dicadangkan ini dijangka berupaya meningkatkan mekanisma keselamatan di dalam VANET dengan membina hubungan amanah di kalangan nod-nod berjiranan,

sekaligus membentuk kumpulan amanah. Amanah ini diwujudkan melalui Modul Pelantar Terpercaya (TPM) dan komunikasi berkumpulan.

Di dalam kajian ini, kaedah-kaedah rangka kerja yang dicadangkan disimulasikan menggunakan dua model rambatan iaitu model asas dua sinar dan model Nakagami untuk persekitaran VANET (802.11p). Di dalam simulasi ini, dua senario trafik seperti lebuhraya dan bandar diwujudkan. Hasil simulasi kedua-dua senario dianalisa untuk mengenalpasti prestasi kaedah yang dicadangkan dari segi kependaman. Protokol V2V yang dicadangkan untuk rangka kerja ini juga disahkan bagi mengwujudkan kepercayaan di kalangan kenderaan.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

This chapter provides an overview on Vehicular Ad-hoc Network (VANET). The overview contains introduction to VANET technology, application, standards, and its security. Next, security requirements and security attacks are defined in this chapter to develop the problem statement and research questions. Following that, the scope, limitation and contributions of this research work are also highlighted.

1.1 Introduction to Vehicular ad hoc Network (VANET)

Vehicular Ad-hoc Network (VANET) is one of the fastest growing technologies in the area of communication technologies. It is a specific branch of the Mobile Ad-hoc Network (MANET) and is considered as the first real world global application among the existing ad-hoc networks. The main idea that gives birth to VANET technology is based on communication among motor vehicles on roads. It is also known as a Vehicle-to-Vehicle (V2V) communication [1]. Communication can also be made to roadside infrastructure, which is known as Vehicle-to-Roadside Unit (V2R) communication as shown in Figure 1.1.

VANET has different distinguishing characteristics, i.e. vehicles moving at high speeds, rapidly changing topology, and has short interaction time between nodes; all of these make it different from the other types of ad-hoc networks. In one aspect, the increasing rate of motor vehicles on the roads keeps human beings mobile, going from one place to another; this process contributes to the development of the economy of a nation. Considering another aspect, with the increasing rate of these vehicles, it is reasonable to think that it will lead to high chance of road accidents [2]. Now, keeping in mind that the aim is to introduce the concept of VANET technology; therefore by using VANET technology, one vehicle can broadcast a message to neighboring vehicles, and that message may contain information regarding the vehicle’s speed,

position, and road situations. For example, considering the road situation only, if there is a traffic accident/incident, then the vehicle can notify its driver to divert or maneuver along the track accordingly. Additionally, this message can also be transmitted to nearby vehicles so that the other drivers are able to manage the situations according to the received information.

The implementation of VANET technology does not only help drivers to avoid fatal road accidents, but it can also provide the experience of smooth driving and many different types of entertainment. For instance, the driver or passengers can be accommodated with internet connection while on the highway. They can pay bills, play games, and be informed about the different service announcements conveniently and effectively [1].

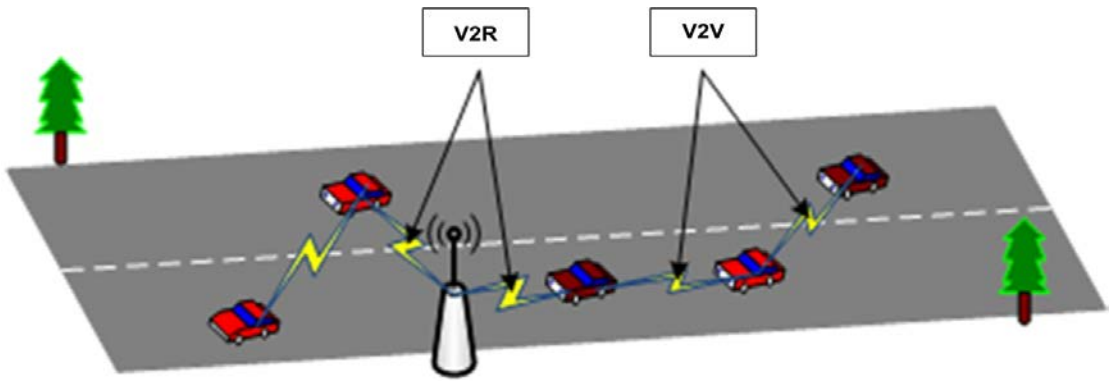

Figure 1.1: VANET Communication: Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside unit (V2R)

The infrastructure of VANET consists of many computing tools in order to make it fully functional. One of the most popular piece of equipment named On Board Unit (OBU) is installed in every vehicle. It is composed of different types of sensors and devices (e.g. GPS, Parking directions, and Warning alarms) that enable VANET to work accordingly. The OBU works as an intermediate device between two OBUs or an OBU to road side unit infrastructure.

1.2 VANET Applications

As discussed in the previous section, VANET technology has various features that can be used extensively to avoid road accidents involving motor vehicles, which in some cases could be fatal. In this respect, the VANET technology that has a wide range of applications in the domain of communication technologies of vehicle-to-vehicle and vehicle-to-infrastructure has the potential to provide solutions to the problem. VANET applications are classified into two categories, i.e. safety and non-safety applications. Sometimes a non-safety application is also called a commercial application. In order to have a clearer understanding, the safety and non-safety applications are discussed in the following sub-sections.

1.2.1 Safety Applications:

In VANET, the term safety itself determines the security of the passengers in the moving vehicles and off the road. In this respect, the safety application plays an important role in providing security to passengers in many ways. It is further classified into two categories according to its functional specifications. This study focuses on safety application that requires minimum delay in communication about 100 milliseconds (ms) denoted as low latency safety application.

a) Periodic Message: The periodic message is a special type of message which is broadcasted by every vehicle in the communication range of 100 to 1000 meters and every message should be broadcasted in 100 to 500 milliseconds. This message contains the information related to road conditions, and vehicle speed and position. The main purpose of broadcasting these messages are to periodically convey suitable road information to other vehicles. Most of the common examples of periodic safety message applications are slow/stop vehicle advisor, Road Hazard Control Notification (RHCN), Cooperative Collision Warning (CCW), Congested Road Notification, Parking Availability Notification, and Toll Collection [3][4][5].

b) Event Driven Message: This is another type of message that is usually broadcasted by vehicles in emergency cases that occurs on roads. An example

of this is when a vehicle brake is suddenly applied by a driver due to nearby crash of a vehicle or existence of hazards on the road. This makes VANET a very useful technology for avoiding road accidents. However, it has a low latency due to its natural behavior and it covers only areas of short range communication. In the domain of VANET, these two types of safety applications play an important role in providing security with distinguishing features. For example, periodic messages are usually broadcasted within a defined/fixed time interval, whereas event driven messages are broadcasted based on an incident that happens on the road. Popular examples of these applications are Emergency Message Dissemination (EDM), Emergency Electronic Break Light (EEBL), and Post-crash notifications [4].

1.2.2 Non-Safety Applications

Using VANET, users may access some commercial applications in order to perform various tasks. Assuming that a user wants to access the internet while on the highway, it can be facilitated by internet service providers through VANET technology for obtaining different services. These services can be pre-paid or post-paid. Additionally, some companies want to advertise their goods and services (e.g. hotels) to vehicles entering into their communication range. These types of applications are named Service Announcement (SA), Remote Vehicle Personalization/Diagnostic (RVP/D), Content Map Database Download (CMDD), and real time video relay [4], [5].

1.3 VANET Standards

There are two standards that are described as Dedicate Short Range Communication (DSRC) and Wireless Access in Vehicular Environment (WAVE). DSRC/802.11p works at lower layers (Phy and MAC); it is an extended version of 802.11a. The IEEE 1609 is a suite of standards for WAVE; the WAVE suite is divided into four classes 1609.1 to 1609.4, each has its own functionality. The details of these standards are described below [6].

1.3.1 Dedicated Short Range Communication (DSRC)

In order to communicate accurately, the Federal Communication Commission (FCC) has allocated a specific frequency, i.e. 5.9 GHz (5.850-5.925) for Dedicated Short Range Communication (DSRC) scheme. It consists of 7 channels and each of them contains 10 MHz out of 75MHz. DSRC can be used for both safety and non-safety applications accordingly, of which, channel 172 has been allocated for safety applications, whereas channels 174, 176, 180, and 182 have been allocated for non-safety applications (e.g. service channels). In addition, channel 178 has been used for controlled communication channels and channel 184 is used for high power and long distance transmission. The DSRC channels are listed according to their functionality in Table 1.1 [7].

Table 1.1: DSRC Channels, Frequencies and Function

Channel	Frequency	Function
Channel 172	5.855 to 5.865	Accident avoidance safety of life
Channel 174	5.865 to 5.875	Service channel
Channel 176	5.875 to 5.885	Service channel
Channel 178	5.885 to 5.895	Control Channel
Channel 180	5.895 to 5.905	Service channel
Channel 182	5.905 to 5.915	Service channel
Channel 184	5.915 to 5.925	High Power, Long Range

1.3.2 Wireless Access in Vehicular Environment (WAVE)

For testing the functionality of VANET, an IEEE trail layer architecture named the Wireless Access in Vehicular Environment (WAVE) has been proposed. It is composed of IEEE 1609.x and 802.11p (an 802.11a variant for VANET) protocols. This architecture has been used in the DSCR for obtaining multi-channel communication to perform different tasks. The WAVE architecture is divided into four classes as illustrated in Table 1.2 [8][9]. It supports the WAVE short message (WSM) and WAVE short message protocol (WSMP) in order to provide different

services at Network and Transport layers for safety applications. In this architecture, two distinguishing standards, of 1609.3 and 1609.2 have been implemented in VANET that work under Network and Transport layers. The IEEE 1609.3 is a networking service standard scheme, which is responsible for describing a message and IEEE 1609.2 Standard defines the security service schemes to provide authentication and encryption [8][9].

Table 1.2: Wireless Access for Vehicular Environments (WAVE) Suite

WAVE	Application Name	Function
1609.1	Resource Manager	Message data formats, Services, and Interfaces.
1609.2	Security	Secure message format , processing, and exchanging
1609.3	Routing and Transport Services	Defines Protocol stack, and provides an alternative IPv6.
1609.4	Multiple Channel	Specification of the multiple channels in DRSC standard.

1.4 VANET Security

In order to achieve secure and reliable communication, security has remained to be one of the more challenging issues in wired and wireless networks. There is always the possibility of external and internal attacks on these networks during communication. These attacks create various obstacles during message transmission from a source to a destination on the network. In this respect, users demand the highest security which must meet their requirements such as authentication, non-repudiation, privacy, availability, and reliability. Keeping these factors in mind, accordingly security has been considered as one of the most important requirement for implementing VANET. In order to achieve security, three main methods, i.e. the symmetric cryptography, asymmetric cryptography, and trusted platform module are proposed. These methods could be implemented in VANET based on hardware and software schemes. These methods contribute in achieving the required security measure but introduce different merits and demerits according to their functionality. The detailed description of these methods is given in the following sub-sections [10].

1.4.1 Symmetric Cryptography

The symmetric cryptographic is an important method in which only one key is used for encryption and decryption of a message. If nodes *A* and *B* at a network share a secret key to each other, then both nodes can read each other's message. The transmitted message is meaningless for other nodes until and unless that secret key is shared accordingly. Using the symmetric method, secret key sharing is important between two nodes for proper communication. The symmetric method is further divided into sub-methods, i.e. block cipher and stream cipher. The block cipher method is capable of encrypting a bulk of data at a time, whereas the stream cipher is capable of encrypting the data bit by bit. It has been found through various studies that symmetric methods are faster than asymmetric methods. However, these methods do not provide protection against the non-repudiation issue during communication [10]. The well known symmetric methods in the area of VANET are as follows.

- Advanced Encryption Standard (AES).
- Data Encryption Standard.
- Data Encryption Standard III.
- Time Efficient Stream Loss-tolerant Authentication (TESLA).

1.4.2 Asymmetric Cryptography

In order to ensure security, another type of cryptography technique named the asymmetric cryptography method has been introduced. In this method, the concept of two keys, i.e. public and private has been used for encryption and decryption of the message during communication. In this connection, the Public Key (PK) is opened for all nodes and it is always used for encrypting the message, whereas the private key is kept secret from other nodes and it is usually used for decrypting the message at receiver accordingly. Both types of keys are generated automatically by an asymmetric algorithm in order to perform their function during communication. These

keys are mathematically related to each other, thus it is hard to break or derive the private key from the public key [10].

In order to enforce security measure, a digital signature scheme has also been implemented in VANET using asymmetric algorithms. This scheme provides a signature of the source that is a unique symbol, which verifies the source of a message. A source sends a message with its signature which will be computed by the receiver. If the signature is valid, then the message will be accepted by the receiver; otherwise it will be discarded. This mechanism ensures security and solves many other issues, such as non-repudiation and exchange of keys during communication. These asymmetric cryptography based schemes contribute in achieving security, but introduce high computational cost and complexity [3]. Some of the well known asymmetric cryptography methods are given as follows.

- Rivest, Shamir, and Adleman (RSA).
- Elliptic Curve Digital Signature Algorithm (ECDSA).
- NTRUEncrypt Public Key Cryptosystem.
- The ID based scheme.

1.4.3 Trusted Platform Module (TPM)

The Trusted Platform Module is a hardware chip, which is designed and implemented On-Board-Unit (OBU) to provide security in VANET. TPM consists of different modules, i.e. asymmetric module used for RSA/ECC, symmetric module used for AES/SMS, HASH module, which defines (SHA1), and the random number generator [11]. These modules have been designed and implemented in VANET for obtaining security during communication. Another feature of TPM is to validate every component in a node and maintain their functionality. It is capable of producing the encryption, decryption, hashes, and random number generator for reliable data communication. This hardware approach assists in the following.

- Asymmetric module used for RSA/ECC.
- Symmetric module use AES/SMS.
- HASH module define (SHA1).
- Random Number Generator.

1.4.4 Vehicle Grouping Scheme

Taking the advantage of Global Positioning System (GPS) and navigation map installed in vehicles. It is possible to create a group of vehicles; the vehicle can form a group by adjacent vehicles. There are two approaches to create group of vehicles in VANET. The first approach is dynamically forming a group of vehicle according communication range. The second approach is dividing the highway into small cells and vehicle creates a group according to cell. In this approach some of vehicles are allowed to join two groups at the same time, that vehicle considered as relay node. Furthermore there are different techniques are applied on second approach to improve the performance[12].

1.5 VANET Security Requirement

In order to implement VANET successfully, some well known security implementation is required i.e. authentication, privacy, non-repudiation, reliability, and availability. These requirements are described in the following sub-sections and need to be fulfilled accordingly [3], [11], [13–15].

a) Authentication: This is a specific process that is used for identifying the source vehicle as the source vehicle broadcasts an encrypted message with a unique identity/signature. On the receiver side, an algorithm is run that verifies the source identity to validate the vehicle, otherwise that message is discarded. There are two techniques that provide the authentication mechanism, one is asymmetric and the second is a digital signature. In VANET, the digital

signature algorithm is used. It uses a private key as a unique signature and that signature is placed in a message, so the receiver is able to authenticate the source vehicle [15].

b) Privacy: As demonstrated in [9], privacy is directly related to the information which should be kept secret from any unauthorized node. There are many kinds of information in VANET which should be kept protected from being disclosed. Depending on a particular situation, the most sensitive data are identity and location. If the identity of a vehicle has been disclosed, then it may be easy for an attacker to use that identity for their own benefit; it is the same in the case of the location being revealed [11] [15].

c) Non-Repudiation: This is a specific security process and a requirement for VANET, which needs to be implemented for the purpose of identifying a user. In many situations, if a bogus message is sent by a sender to a receiver, and the real user denies that the message has been originated by him/her, then the non-repudiation security process provides a mechanism to track the source of the broadcasted message. In this situation, the sender cannot deny sending the message due to the availability of exact evidence inside the sent message using VANET [16].

d) Reliability: In order to establish trust among the vehicles, reliability is one of the important factors that must be maintained during communication. When a message is sent by a nearby vehicle (source), it should be trustworthy for the recipient (destination) vehicle. This is information is useful for a recipient to take immediate and appropriate actions without measuring or waiting for further confirmation [16].

e) Availability: This is also an important requirement for VANET security in which vehicles are able to communicate with each other in any situation. However, sometimes it happens that the message cannot be received by a recipient due to a jam of services or busy channels [3].

f) Efficiency: All vehicles broadcasts safety message in every 100 to 300 millisecond, in order to convey the information about road condition for upcoming vehicles. Considering this practice when the numbers of vehicles are increased, it creates a problem for vehicles to verify large number of messages within such short time (100 ms). For that reason verification scheme should be fast enough to verify all incoming message within time[12], [17], [18].

1.6 Challenges and Issues of Using VANET

To successfully implement VANET technology, various challenges and issues have been identified by researchers. The major challenging issue is security attack, i.e. bogus information, personal information tracing, Sybil attack, vehicle impersonation, and denial of service. In order to solve this challenging issue, different studies have been undertaken in which it has been identified that there exist external and internal security attacks on the networks. The external attacks come from invalid vehicles whereas internal attacks come from valid vehicles. These attacks can be active or passive in nature as described below.

a) Bogus information: It is reported in literature [19] that sometimes bogus/fake messages are broadcasted by a malicious vehicle to other vehicles for its own advantage. For example, an attacker vehicle wants to either clear or jam traffic on the road, so a fake message is sent to other vehicles. This scenario introduces the possibility of fatal accidents and wastage of time for everyone. In order to avoid these situations, an integrity mechanism has been proposed. It assists in tackling fake information during communication using VANET.

b) Personal Information Tracing: This is a privacy attack which is directly related to personal information of a vehicle, such as identity and location. In this situation, the malicious vehicle may use the private information for financial benefits or to claim the identity. In order to overcome this issue, a mechanism named anonymity/pseudonym has been proposed that helps in keeping the information secured [16].

c) Sybil attack: It has been identified through different studies that an attacker vehicle broadcasts many messages that are associated with fake identities. In addition, it also broadcasts bogus information related to its position and location to create an illusion for neighbor vehicles on the road. These situations introduce the Sybil attack in a VANET environment. It has been reported in different studies that this attack is possible in a network, if there is no centralized authority. In this attack, an attempt is made to create a scenario which diverts the other vehicles to another route. It may lead to the risk of life and many other issues [13].

d) Vehicle impersonation: As defined in [15], in this situation, bogus information is spread into a network, and eventually an accident occurs between vehicles in the network. The authority can easily track down the vehicle, which is responsible for broadcasting that message. VANET uses a mechanism to detect vehicle identity by using the unique given identity of a vehicle, or the position estimate of a vehicle and its related plate number of the user's original identity.

e) Denial of Service (DoS): The denial of service occurs when attackers attempt to broadcast too many messages through a jammed channel on a network. The basic purpose of this service is to make service unresponsive, which means users are not able to communicate. There is also another type of denial service named the Distributed Denial of Service (DDoS) in which one or more attackers can broadcast messages on a network [16].

1.7 Problem Statement and Motivation

VANET is an emerging technology in the field of computer networks. The concept of VANET technology comes into reality due to the increasing rate of vehicles accidents on highways. These accidents increase the death rate and countless injuries yearly of human beings in the metropolitan cities and on highways. These accidents are also the reason for severe damage to vehicles and roads. In regards to this, the cost of repairing vehicles and roads is increasing day by day [20],[14]. However, vehicles are

needed to provide convenience for people to move from one place to another for business and other daily activities. Considering these factors, VANETs have gained greater attention in academic and industrial research to provide solutions to the problems. Several studies have also been conducted to provide security and services for users to ensure comfort and satisfaction.

Despite that, improving security remains as the most essential challenge for VANET technology. The current security schemes are inefficient in terms of verification process. If there are hundred vehicles in the communication range, then every vehicle has to verify all incoming messages within a short time (100 ms). It is noticed in literature review, the current security schemes are not considered as efficient as they cannot perform verification within the short time. However significant improvement done by researcher but there is still gap identified in these studies typically for low latency safety application [10], [16], [18–22]. Trust is another issue between vehicles, It is notice that there is strong authentication mechanism is required to build trust among vehicles, especially when symmetric scheme is used for safety application [3] [11]. This study has been conducted with the aim of overcoming these issues. There is another issue during communication using VANET.

1.8 Research Questions

Related literature has been reviewed and analyzed in which the problem statement and gaps have been identified. Based on that, some research questions are formulated as given below. This study attempts to answer the followings.

a) How to reduce latency during message transmission for safety applications?

b) How to build a trust among the neighboring vehicles using the symmetric cryptographic scheme?

1.9 Research Objective

Considering the research questions of this study, the following objectives are described that assist in overcoming the issues.

a) The primary objective is to propose a security framework to reduce latency for safety applications using Trusted Platform Module (TPM) and vehicle grouping.

b) The secondary objective is to provide a strong authentication mechanism to build a trust between neighboring vehicles using the symmetric cryptographic scheme.

1.10 Methodology

In order to address a problem statement and answering to the research questions of this study, a research methodology is proposed in the form of a security framework. It consists of different components and is divided into two parts, i.e. internal and external. These parts work to together in a VANET environment. The internal part is related to the message construction and trusted platform modules whereas the external part deals with group designing and communication protocols.

1.11 Scope and Limitation

VANET is a growing mobile wireless communication technology, which is challenging to implement according to its security requirements. Currently VANET technology has many issues and security is one of the most important issues. Thus, it is important to address the need to have sufficiently tight security for successful deployment of VANET. This work is focused on two major parts of security: encryption/decryption efficiency and trust between vehicles. The proposed security framework utilizes many components of security and cryptography to provide efficiency and trustworthiness for message related applications in VANET.

Part of the proposed security framework has been designed based on hardware chip called Trusted Platform Module (TPM). Owing to the nature of this study and in-line with the objective, it is sufficient to provide evidence based on simulation. In order to meet this requirement, simulations are conducted based on the message size that is already known from the results of other research works.

1.12 Contribution

This study contributes toward a body of knowledge in VANET technology, particularly in the aspect of security. This study proposes a framework which provides a solution of problem statement/research question. Hence, the overall contribution in this study is highlighted in five main points as given below.

a) The proposed framework is a combination of the trusted platform module and the vehicle grouping scheme, which assists in satisfying the safety requirement applications of VANET.

b) The second contribution of this study is the utilization of both asymmetric and symmetric cryptographic methods to achieve secure and fast communication for safety applications.

c) This study contributes in building the trust among group of vehicles by vehicle-to-vehicle protocol (V2V). The V2V protocol is used mutual authentication mechanism to build trust between vehicles.

d) In addition, a new vehicle grouping scheme is designed for the proposed framework that reduces the extra burden from the group leader and provides a fast way for new vehicles to join any particular group.

e) This study compares four security schemes message sizes to examine the proposed framework and its functional scheme through simulation under 802.11p in the domain of the highway and urban scenarios.

1.13 Thesis Organization

This thesis begins with an introduction to VANET technology, its importance, and related issues. In Chapter 2, related literatures are reviewed in which VANET security schemes that are suggested for safety applications are focused. In order to address the specific issues a research methodology is defined in Chapter 3. This chapter defines and discusses the proposed framework which consists of two different parts, i.e. internal and external. Furthermore two software and their basic settings are defined; these software are used to get results. In Chapter 4, the results are analyzed and discussed in the context of the problem statement identified earlier. In addition, the proposed protocol is validated and discussed. Finally, in Chapter 5 the conclusion, contribution, and recommendations of this study are provided.

CHAPTER 2

LITERATURE REVIEW

This chapter discusses the different security schemes in detail that have been proposed for VANET environments. This chapter is divided into three parts. The first part discusses TPM architecture in order to understand the basic functionality of TPM. The second part defines the existing security schemes and frameworks that are associated with cryptographic, vehicle grouping, roadside unit and TPM. In third part a comparison tables are developed, in which early proposed works contributions, drawbacks and limitations are defined. Finally, the safety applications are defined, which are required minimum delay in communication, security scheme standards (1609.2), and safety message sizes.

2.1 Trusted Platform Module

The Trusted Platform Module (TPM) is an integrated chip that exists in hardware form. It contains the different cryptographic methods that assist in providing a variety of security features using VANET. The TPM chip is responsible for providing a reliable platform/system for vehicles through the Core Root of the Trusted for Measurement (CRTM) procedure.

The CRTM stores certain values during the booting process. In this procedure, all the records of the integrated components are stored accordingly for verification. The TPM performs operations under a secure environment and it stores all the cryptographic elements in a protected location. Meanwhile, the TPM defines an integrity procedure, which saves the measured digest in a protected location of the system, and these digests are used to ensure the system's performance in a trusted environment.

The TPM chip contains three main entities, namely: the cryptography modules, keys and registers/logs as illustrated in Figure 2.1. In addition, it is also associated with processes that perform different functionalities. In order to achieve trust among vehicles in VANET, the TPM is responsible for defining the set of processes named as the core root of the trust measurement and the key storage hierarchy. These processes ensure that the components of the running vehicles exist in a trusted environment, which has built trust among those vehicles [24].

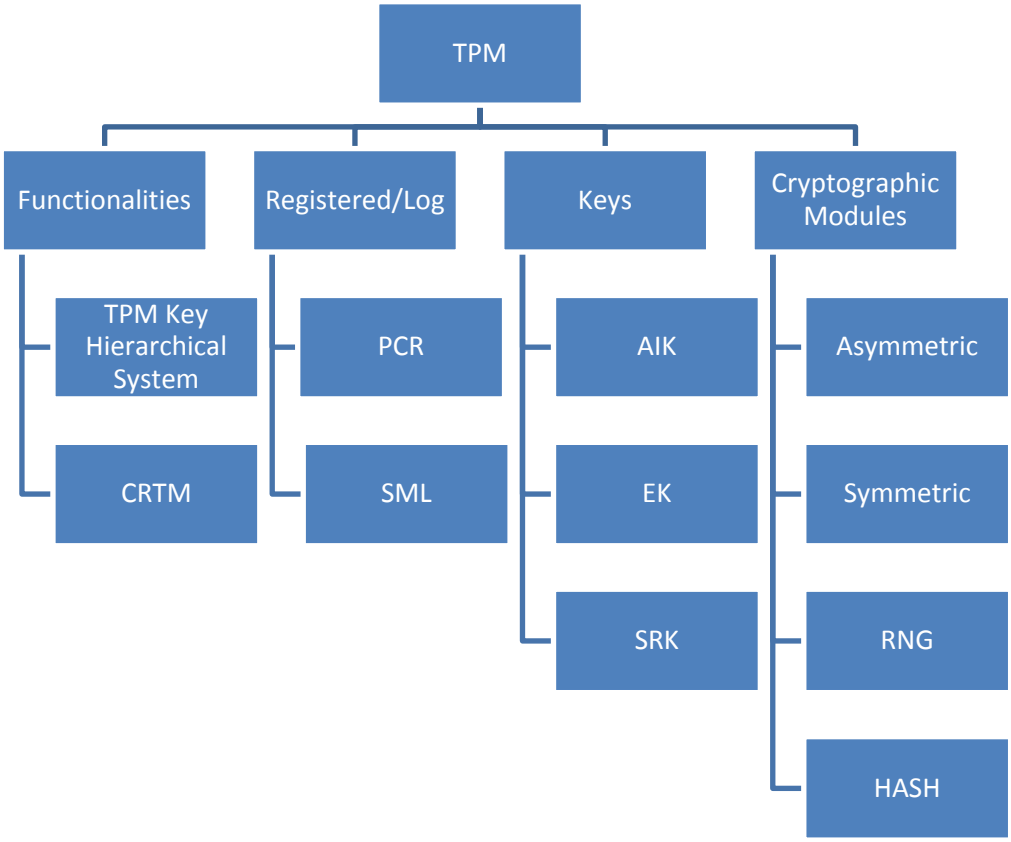

Figure 2.1: TPM basic Block Diagram [24]

The main entities of TPM, i.e. the cryptographic modules, keys, and registers that have been illustrated in Figure 2.1 provide specific functionalities needed to obtain the security requirement of VANET. Considering, the cryptographic modules, i.e. Asymmetric, Random Number Generator (RNG), and Hash. Certain keys are used in the TPM that also play an important role in providing security. These keys are named

as the Endorsement Key (EK), Attestation Identity Key (AIK), and Storage Root Key (SRK). In addition, the Registers, i.e. the Platform Configuration Registered (PCR) and, a log named the Stored Measurement Log (SML) also play an important role in achieving security for VANET. All these are further discussed in detail according to their functional specifications in the following sub-sections.

2.1.1 Cryptography Modules

Trusted Platform Module, the cryptographic module is associated with the three security engines as illustrated in Figure 2.1. Each engine plays an important role in achieving the security of VANET.

a. Asymmetric Module: The TPM uses the asymmetric module which consists Rivest, Shamir, & Adleman (RSA). These methods are responsible for generating the two keys which are public and private keys. In early studies, the TPM was implemented with the RSA method for providing security at VANET [24].

b. Random Number Generator: The Random Number Generator (RNG) generates the seed numbers. It can generate the hash string by accepting function. Primarily, it generates random a seed and then applies an appropriate function to get a resultant sequence number accordingly [24].

c. Hash Module: The hash function that helps in receiving the data and converting it into a fixed size of digest. It is also called string. The hash module uses the Secure Hash Algorithm1 (SHA1) method which is responsible for converting the data into the hash form/cipher text form. The basic function of this method is to provide message reliability in terms of identifying the unaltered message/unchanged message [24].

2.1.2 Trusted Platform Module (TPM) Keys

In order to encrypt and decrypt the messages and keys, the TPM uses three kinds of keys, i.e. the endorsement key, attestation identity key and storage root key. These keys are also identified as permanent or temporary according to their functionalities. Considering the functionalities of these keys, some are responsible for encrypting/signature and decrypting/verification the messages; while storage root key is responsible to encrypts keys that are stored outside the TPM.

a. Endorsement Key (EK): The endorsement key is a permanent key which is embedded in the trusted platform module during the manufacturing process. It consists of two segments named public and private; EK segments are generated by the asymmetric module. The private segment of the endorsement key is never revealed outside of the TPM. This private segment is kept secret and it is used for the purpose signatures or is responsible for decrypting a small piece of data in order to provide security. Considering the concept of trusted computing, if the private key is being kept secret then the digital signature can be ensured trustworthy. However, the public segment of the endorsement key is distributed, accordingly among the authorized parties. Basically, this segment is responsible for identifying the original TPM, for encrypting the data, and verifying the signed small pieces of the data, accordingly. If it is decrypted properly by the public segment, it ensures that the data was encrypted by an authorized party of the private segment [24].

b. Attestation Identity Key (AIK): These keys are temporary and created for providing authentication using the attesting process. AIK keys are used for different tasks; they can be used for signature/verification of data or they can assure that the current TPM is trustworthy. AIK also generates other key sets for attestation like the endorsement key. The AIK key pair is also generated by the asymmetric module; it can generate an ECDSA or ECDH key pair [24].

c. Storage Root Keys (SRK): The SRK is used to encrypt the keys which are stored on a secondary storage drive or any other drives. The SRK is an

symmetric key and it can be renewed when a new user takes ownership of the TPM [24].

2.1.3 Trusted Platform Module's Registers and Log

a. Platform Configuration Registers (PCRs): These are registers fabricated in the TPM that are used to store certain values during initial booting and in various software component(s) of the system. The TPM uses the Secure Hash Algorithm1 (SHA1) to store PCR values in digest form to avoid its modification. The TPM chip consists of 24 registers in which the PCR#0 is used for bios and the PCR#1 is used for booting the loader, respectively. The rest of the registers are responsible for storing component values at different levels using the TPM system [24].

b. Stored Measurement Log (SML): The SML is used to store the measured values of different software components. It digests each measured value, appends, rehashes, and stores them accordingly in a common measured digest [24].

2.1.4 Trusted Platform Module's Key Hierarchical System

In this system, many keys are involved during the TPM's operations and there is not sufficient memory to store the keys within the TPM chip. This is why the TPM provides the key hierarchical system that is illustrated in Figure 2.2. It provides an overview of how this particular hierarchy works. There are many keys which are stored in a secondary drive/hard drive. These keys are encrypted by the Secret Key (SK). After that, the SK is further encrypted through the Storage Root Key (SRK), which is stored in the TPM chip. The SRK key remains inside the TPM which is never used for any other process or entities such as software and components. This process is sometimes called binding a key and the SRK is sometimes called wrapping a key. This whole process introduces the nested key encryption concept as illustrated in Figure 2.2 [24].

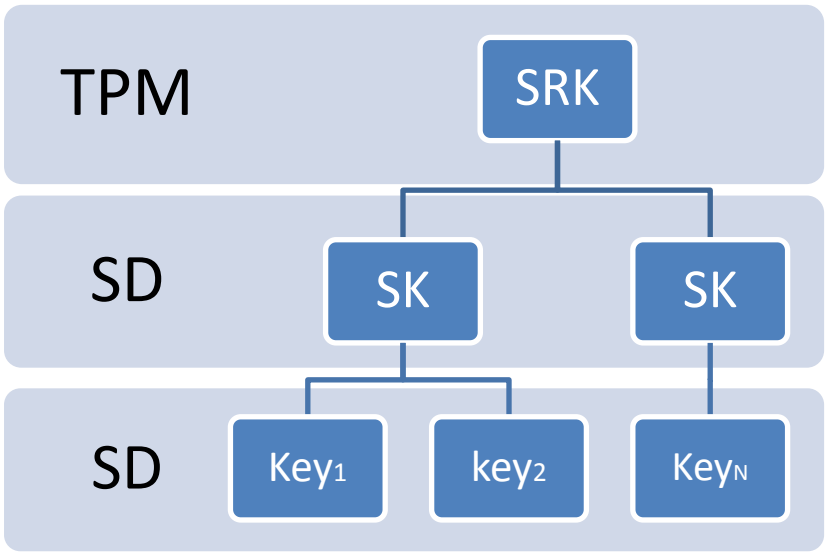

Figure 2.2: TPM key hierarchies [24]

2.1.5 Core Root of Trust for Measurement

The Core Root of Trust for Measurement (CRTM) is an advance programming code in the TPM. It provides the reliability of running components of the system. The CRTM starts functioning in the initial phase then the Basic Input/Output System (BIOS) tends to the workings accordingly as illustrated in the Figure 2.3.

The CRTM is capable of measuring the BIOS routines and then saving the valuable information in the PCR registers. After this process, the CRTM transfers control to the BIOS. The BIOS checks the hardware components. It passes the control to the boot-loader routines and it saves that information in the PCR. After that, control is transferred to the boot loader to assess the routines of the Operating System's (OS) kernel. Before transferring control to the OS, the boot loader saves the assessed information in the PCR. In this manner, all components are measured step by step so that one can verify from the PCR saved values that the current system is functioning in a trustworthy environment [24].

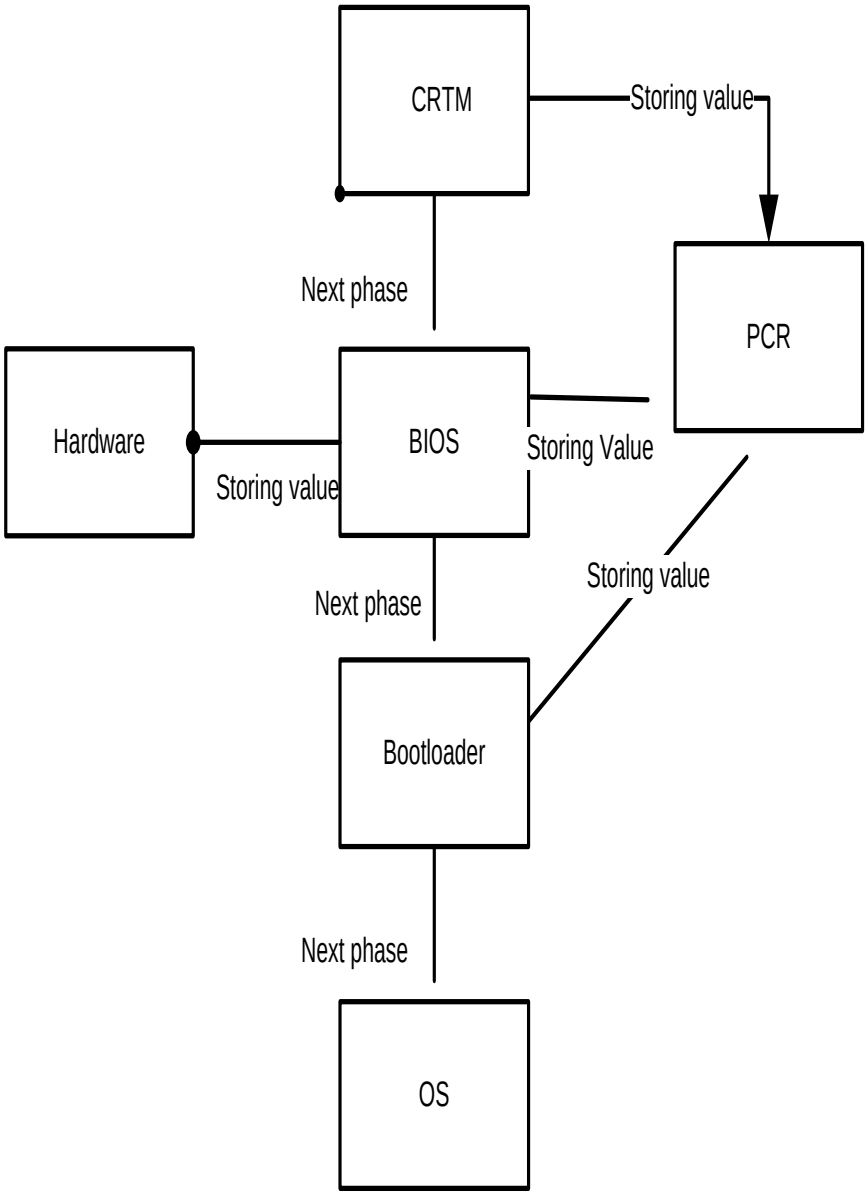

Figure 2.3: Core Root of Trusted for Measurement [24]

2.2 Security Schemes and Frameworks

In order to understand the early proposed security schemes and frameworks in VANET, the extensive literature reviewed is made in this chapter. Each of them plays an important role in providing security and also has some of limitations. These schemes and frameworks are divided into seven categories as illustrated in Figure 2.4 discussed as follows.

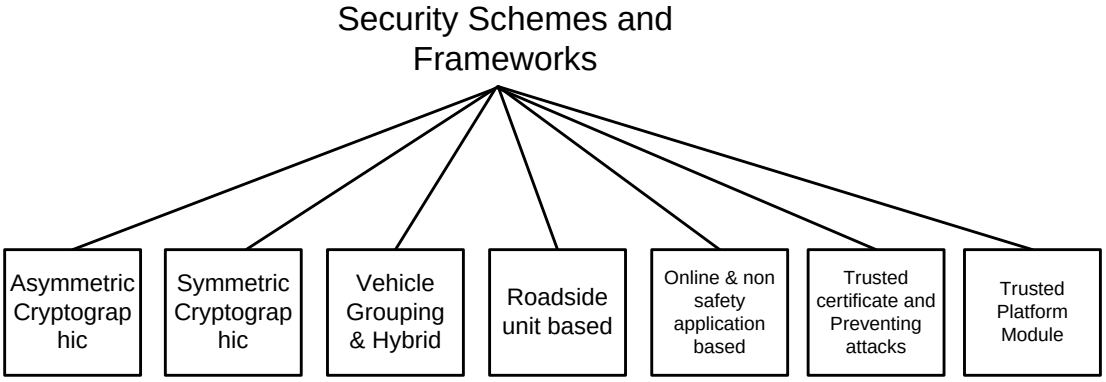

Figure 2.4: Early proposed schemes and frameworks

2.2.1 Asymmetric Cryptographic based Schemes and Frameworks

The asymmetric method comes with two different mechanisms; one is the Public Key Infrastructure (PKI) and the other is the digital signature. The digital signature scheme is used in safety application for VANET, the Elliptic Curve Digital Signature Algorithm (ECDSA) is most suitable scheme considered [16]. It has been used as the default security scheme in many different areas. ECDSA is used for protection against messages from malicious nodes in a VANET network. It is generally considered in the cryptographic world that large security key size algorithms are difficult to break. However, ECDSA comes with small key sizes but provides the same level of security as RSA. The ECDSA scheme uses two keys; one key is used as a signing key, it is known as a private key whereas, the other key is called a public key and is used to verify the data. The basic idea is that the private key should always be kept secret from other nodes and the public key should be made available to other authorized nodes. The ECDSA scheme is more secure in certain aspects of security. However, ECDSA is very slow in verifying signatures as illustrated in Figure 2.4 which makes it unsuitable for many in VANET; furthermore, due to the slow signature verification process, ECDSA can be memory DOS attacked, as well.

ECDSA was first proposed by Scott Vanstone in 1992, ECDSA is described in FIPS 186-2 [25] as a standard for government digital signatures, and is explained in ANSI X9.62. The Elliptic Curve Diffie-Hellman (ECDH) is an asymmetric

cryptographic scheme. ECDH is a variant of ECDSA and it is used for share keys between two nodes. ECDH allows two entities to establish a secure communication on an insecure channel. Due to the asymmetric nature it provides a high level of security like that of a large key size scheme [26]. The processing delay is considerably higher than RSA schemes. The ECDH scheme takes 2.82ms (milliseconds) for key agreement, whereas RSA scheme takes 6.24ms [27].

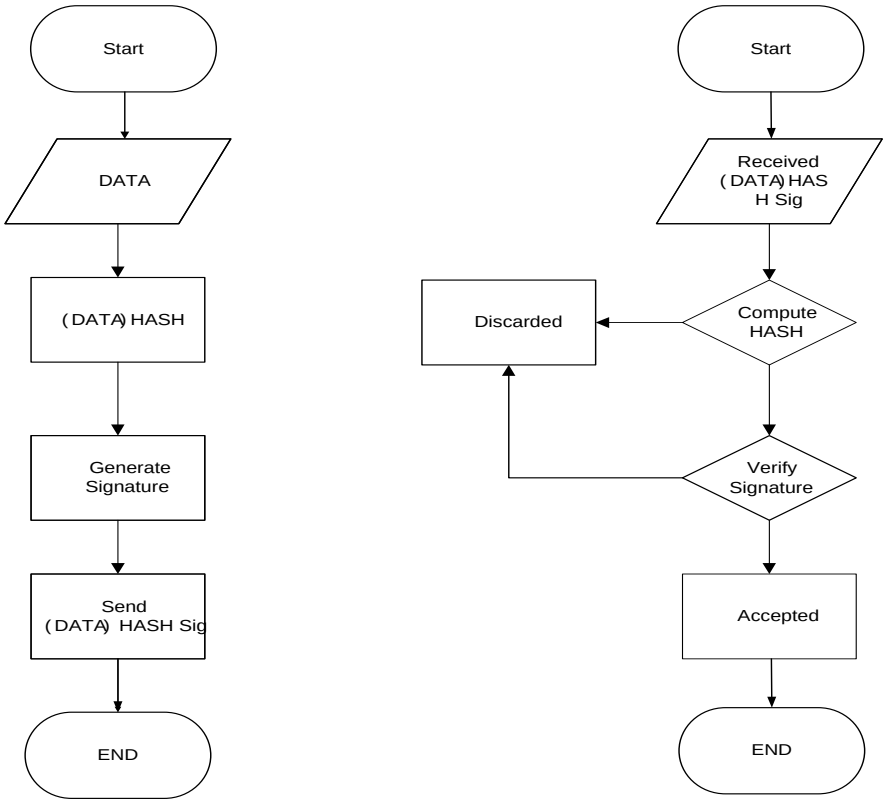

Figure 2.5: ECDSA Signature Generation and Verification Diagram

Rivest, Shamir and Adleman [28] is very popular algorithm in asymmetric cryptography, but due to its size and complexity it is not suitable for VANET applications. RSA has a nine times larger key size as compared to ECDSA; however it is very fast in verification. In the case of a VANET environment, where each vehicle broadcasts a message in 100 to 300 milliseconds, as RSA is a large key size, the scheme message drop ratio can be higher and it is also possible to jam signals by broadcasting many messages at the same time (DoS). RSA is suggested with TPM

chips also, which is defined in the TPM hardware section. RSA is based on the integer factorization of a prime problem. It is extremely difficult to find its prime factorization from a given positive integer n, where n is an extremely large number.

Considering large key and slow verification a new cryptographic scheme is proposed namely NTRUEncrypt. Its key size is smaller than RSA and larger than ECDSA; however NTRU is quite fast in verification. In [16] the authors give details of VANET's threats, possible security requirements and its solutions. This study also compares the default PKI mechanism with the NTRUEncrypt mechanism; this study reported that the ECDSA mechanism is slow in verification and NTRU is fast in verification but large in key size. NTRU may not be appropriate for VANET's environment due to the scarce bandwidth and is likely to result in longer transmission delays.

To focus privacy issue a scheme is introduced in VANET technology called ID based scheme, basic concept of an ID based scheme is described in [29][30]. It uses a type of technique such as where a user's address is used instead of a real identity name such as email address, date etc. One advantage of this technique is to protect the user's identity and compose the message more securely. The ID based scheme also solves the certification problem as it saves the certificate bandwidth. This scheme is used in for vehicle to vehicle communication. There are three basic phases of this scheme.

- System setup phase: This phase depends on the Trusted Authority (TA) which is used to select public keys and compute the corresponding private key.

- User registration phase: This is the joining phase. TA computes the secret key of the user. This communication is done by creating a protected tunnel (secret channel) for communication. After this process, TA generates a private key by computing the secret key where public information is disclosed (public key).

    - Authentication phase: In this phase, the user verifies another user's identity in order to join the network.

In order to avoid and traceability the Group Signature (GS) scheme is proposed in [31], [32]. In GS vehicles find a group and there is only one key to verify the message (public key) whereas all group members contain their own private keys. The idea of the group signature is that any vehicle within a group can sign a message by using its private key and the receiving vehicle can verify it. However, the receiving vehicle is not able to track back to which vehicle actually sent the message. This GS scheme provides unlink-ability and is untraceable. However, GS is a very complex scheme and is as large in size as the RSA scheme which makes it not suitable for VANET technology.

In [33],[30], the authors give the concept of a blind signature scheme utilizing it for vehicle to roadside infrastructure. In this algorithm, the vehicle sends a message to the roadside infrastructure. The message is blind so RSU does not know what the actual data inside the message is. RSU signs the message with his private key and sends it back to the source node. After that, the source vehicle will un-blind the message and broadcast it among the vehicles. The blind signature scheme is a very complicated algorithm and is used in specific applications. Blind signature provides anonymity; however it significantly increases the time due to the two parties' having to first blind and then signature the message, respectively, before it is broadcast

2.2.2 Symmetric Cryptographic based Schemes and Frameworks

The AES is a block cipher (converts a bulk of data at one time). AES is a very well known scheme and is used in many encryption/decryption techniques. AES has different key sizes, AES (64,128,256 bites), and variant combinations such as AES-ECB AES-CCM. The 1609.2 suggested AES CCM 128 for VANET. AES-CCM is used for both encryption and message authentication. AES- CCM just takes 5 micro seconds; whereas ECDSA takes 6 milliseconds, it is clear that AES is a thousand times faster than ECDSA [10].

In [34][22], a symmetric cryptography mechanism, Time Efficient Stream Loss-tolerant Authentication (TESLA), is introduced. TESLA is a fast cryptography mechanism due to its symmetric nature but lacks the non-repudiation property. In this

scheme, the receiver has to store the message and Message Authentication Code (MAC) until the sender discloses the key (delay key disclosure). TESLA may lead to vulnerability against possible memory attacks. VANET Authentication using Signatures and TESLA++ (VAST) is a hybrid framework [16], which is the combination of TESLA and ECDSA. VAST carries both signatures, ECDSA and TESLA, in case of emergency, where non-repudiation requires ECDSA signature verification. However, due to carrying both signatures, it will increase the size of the packet significantly.

In [35], the author gives the idea of the secure message aggregation. Two methods are defined; one is known as the concatenated signature. In this technique, a sender broadcasts a message and the receiver appends its signature and rebroadcasts the message; this process continues as the receiver has no need to verify other signatures. In the second scheme known as the onion signature scheme [35], a receiver signs over the message and then rebroadcasts it as a new message. It contains both the old signature and the signature of the last receiver so the next hop verifies the last signature; if the signature is an invalid signature, it will be discarded and the process starts again. This algorithm has an overall computation overhead.

The many researchers provide different PKI cryptographic schemes which are quite strong in terms of security. In [36], the author proposed a strong authentication scheme, which is based on lightweight TESLA and PKI to achieve privacy and reduce security material overhead. The author introduced the concept of a long chain of keys. In this scheme, a dispatcher produces a long chain of keys; every key is utilized for a short period of time and then discarded from list. A combination of two schemes (traditional digital scheme and lightweight broadcast scheme) is suggested in this study. The vehicle is embedded with two keys; one is a short term signing key and the other is a long term key, which is a public key. It has a certificate and each vehicle is time synchronized by GPS.

2.2.3 Vehicle Grouping and Hybrid Methods Schemes

In this paper [37], a hybrid scheme is proposed which is based on two schemes, namely the pseudonym and the group signature. In the hybrid scheme, every vehicle (node) contains a group signing key and a group public key. A vehicle also generates its own set of pseudonym certificates. Every vehicle generates a pseudonym certificate and self certifies that certificate on the fly. The certificate authority works to validate that generated certificate and verify that it belongs to the registered vehicle (node). The verifier upon receiving a message validates the message using a group signature public key and revocation list. After successful verification by the verifier, that message is accepted. Due to the pseudonym scheme, the user is unable to identify the source node (untraceable) and cannot link to which two certificates were used by the same party (unable to link). But, the hybrid scheme increases the size of the message (298 bytes security overhead).

In order to over efficiency and privacy issues, a framework is proposed in [12]. The proposed framework also described a secure and privacy preservation protocol, this protocol is the combination of group signature and identity based signature called GSIS. The proposed protocol designing goals are conditional privacy, traceability and efficiency. The system architecture considered three types of network entities. Tracing Manager (TM): TM is responsible to trace the real id in the case, if anyone broadcast a bogus message broadcast. Membership Manager (MM): Every vehicle on road need to be registered form MM and preloaded with public and private keys. On-board unit (OBUs): All moving vehicles are installed with OBUs. It is noticed that proposed protocol is not efficient in computation cost, because as revoked vehicles increased every vehicle need spend time on message verification and message drop ratio is very high. Furthermore RSU installed after every 500 meters, which significantly increased cost.

In order to reduce message size a framework is proposed in [17] namely TSVC is combination of two methods TESLA and SVC. TESLA method is use to reduce the size of packet and as well use a short MAC tag for fast verification. SVC is used for privacy protection; SV is utilizing a short certificate that has no real identity to keep the privacy of driver. However authorities can link that anonymous certificate with

real identity of driver. Furthermore this scheme also forms a dynamically group of vehicles. TSVC combines all these schemes to achieve privacy, data authentication and traceability. It is reported that TSVC method having higher message delay than required time. However message drop ratio decreased.

In [38] architecture is proposed that is based on layer 2 multi-hop authentication and credential delivery; this scheme works between vehicles and the network operator. The proposed scheme works for both safety and non safety applications. Furthermore, the author suggested some guidelines to perform better under different situations of density. The architecture consists of OBU/vehicle, APs/RSUs and AAA. OBUs are source nodes and relay as well as provide connection to other vehicles, which are not currently under any AP.

Authentication Authorization and Accounting servers (AAA) are responsible for linking with other parties such as the Certification Authority (CA). The Public Transportation Authority (PTA) is implemented as an authority to give certificates to valid nodes and network operators. The Network Operator's role is to handover different kinds of certificates to each vehicle; there are three kinds of certificates. The first is the long term certificate; it is an off line certificate given to the drivers to get non ITS services. The second certificate will be online and is temporarily valid for ITS and non ITS services. These certificate are used in the authentication process (vehicle to AS).There are two protocols used in this study; the first is the Authentication and Credential Delivery (AUCRED) protocol and the second is the EAP Geographic and Positioning Encapsulation for Multi-hop transport (EGEMO). AUCRED is a mutual authentication protocol among AS and vehicles; AUCRED is a temporary certificate which uses a stateless cookies mechanism for handling DoS attacks. EGEMO is designed to provide a multi-hop communication; EGEMO works with EAP at layer 2.

In [35],[39] the system group formation is computed by dividing the geographical area in a small size called a cell (cell size depends on the transmission range). If any vehicle enters into a cell, the cell will automatically know from which group it has joined this cell. The group leader is a vehicle which is nearest to the cell centre. If

there are many vehicles close to the cell centre, then selection of a group leader is done by the lowest id. However, this will cause a frequent change of group leaders.

Study [40] gives a concept of two techniques for getting the appropriate location of the vehicles. The first technique is the Convoy Member Authentication (CMA) and the second technique is the Vehicle Sequence Authentication (VSA). CMA and VSA are used to verify the actual position of a vehicle by using a formula and a GPS system. CMA checks whether a vehicle is on the same direction, whereas VSA is concerned about the vehicle's sequence. The proposed scheme also handles attacks such as Sybil and position cheating.

An efficient group creation scheme presents in [41], [42] denoted as Secure Group Communication (SeGCom), the highway is divided into small segments and each segment is monitored by an RSU. Each segment is divided into equal sizes and each RSU is placed in such a way that they overlap each other. Each vehicle forms a group by location and time interval. Furthermore, RSU segments are divided into splits. Each split has its own unique key for communication. If any vehicle between two segments split; it acts as a relay node; however, installing RSUs along the entire road is not feasible in a VANET environment as it can increase the deployment cost significantly

In [43], the author tries to mitigate the issues like certification distribution, revocation and weak tamper proof devices. An RSU is placed on a highway to maintain and manage a group of vehicles. A decentralized group authentication mechanism utilizes the group signature. Whenever a vehicle enters in a group, it is verified by the next vehicle; any bogus message is triggered while verification of that vehicle ID is discarded by the third party. The proposed scheme uses two methods. One is signcryption and the other is group signature. The signcryption is used to communicate with an RSU and gets the member key securely, and for vehicle to vehicle communication group signature is used. The proposed scheme divides roads into small cells which are controlled by the RSU.

This study describes a scalable and robust protocol, which has five phases (system setup, re-key issuance, key issuance, tracing and batch verification). The system setup

involves generating parameters and keys; three entities generate public and private keys: the tracing manager, vehicle and RSU. The re-key phase role is to update the vehicle certificate and the public and private keys in case the key is disclosed. The key issuance phase distributes secret keys among members by utilizing RSUs.The signing phase will use the group signature to sign a message; finally, when a message is received by a recipient he/she runs the batch verification process to ensure the message is valid or not. The total size of this scheme is around 474 bytes (2 group id+ 100 data+364 signature+4timestamp). Another issue with this scheme is installing the RSUs along the whole highway which is very costly

In [44], a scheme was proposed, which uses both asymmetric and symmetric methods; furthermore, the tamper resistant hardware is also implemented in this scheme. This study mainly focuses on two areas, one is reducing computational cost and the other is to protect the privacy of the user. There are different components used in this architecture. The tamper resistant hardware used to store the certificate, the governmental transportation authority provided vehicle related identity and the geographically distributed trusted third party is responsible for message encryption and authenticating pseudonyms. In the Asymmetric key scheme, the vehicle will be embedded with Vehicle Related Identities (VRI) and a certificate. VRI is a private key for each vehicle and is associated with a certificate from the central authority. Every country has a central authority and a Governmental Transportation Authority (GTA), which provide certificates to vehicles. Tamper Resistant Hardware (THR) is used to protect keys, the Geographically Distributed Trusted Third Parties (GTTPs) are installed region by region and it is responsible for providing pseudonym participation and the symmetric keys in VANET. The symmetric key is used for message encryption and message authentication, GTTP can also compare VRI and pseudonyms.

In [18], [45], they proposed an authentication protocol, which is implemented based on the Key Insulated Signature (KIS) scheme; it is an efficient anonymous authentication protocol. The paper also proposed a model which depends on three entities, namely the Transportation Authority (TA), Road Side Unit (RSU) and On Board Unit (OBU). TA is responsible for registration of RSU and to install OBU

equipment in vehicles. RSU is required to issue short time anonymous certificates and OBUs are used to communicate with others vehicles. KIS uses a method, where there is only one public key and that key is used for signature verification. The RSU can have a secret key to issue a certificate. The proposed scheme is used to achieve privacy protection, trace the vehicle and reduce computation cost

2.2.4 Roadside Unit based Schemes

RAISE [23], [46] is implemented with collaboration of a Road Side Unit (RSU) and an On Board Unit (OBU). It is especially used in metropolitan areas where an RSU is placed everywhere in infrastructure. The idea of RAISE is to work together with RSUs to reduce computational burden (fast verification). In RAISE systems, every vehicle initially contacts an RSU to get the shared symmetric key. Before getting a symmetric key, there is a mutual authentication process between the RSU and the vehicle(s). After receiving the shared key, the RSU also sends a pseudo ID to the vehicle, because if any misinformation happens then the RSU should be able to trace back to the vehicle for that RSU. The RSU maintains a table in its local database.

Cooperative Message Authentication Scheme (COMET) [46] was introduced as a supplementary scheme in the RAISE technique. It is used where RSUs are not installed. COMET is designed to verify signatures according to vehicle capacity. If there are n vehicles, a few of them will verify signatures and if the signature is valid that vehicle will notify other vehicles and if any vehicle finds an invalid signature, it will notify other vehicles to discard that message. It is review that in both paper simulations performed in IEEE 802.11a to check real impact of these schemes, it is necessary to perform simulation in VANET environment/802.11p. In addition it is also noted that these schemes are not suitable for low latency safety application.

In [47], the author gives the concept of a cellular network which is feasible for a VANET environment. The proposed scheme describes two ideas, one for vehicle to infrastructure and the second for vehicle to vehicle communication. The authors proposed a high level communication architecture in which the area is divided into logical zones; each zone has its own Peer-to-Peer (P2P) communication groups. When

a vehicle is moving from one zone to another this process is called roaming and the vehicle position can be obtained from a Global Positioning System (GPS). A group server is used to maintain data of the vehicles in each zone. There are also environment servers to alert of events in a particular zone.

2.2.5 Online and Non-safety Application Based Schemes

Keeping in view the importance of security, another study has been conducted in which architecture is proposed for both safety and commercial applications such as internet and service announcements [48]. They proposed two schemes named EAP-Kerberos and EAP-TLS [49]. These schemes provide Authentication, Authorization and Accounting (AAA). EAP-Kerberos is a scheme that mutually authenticates user to user or access point or service provider at the initial level. It can be suitable for some commercial applications. However, due to its on-line real-time security requirements, it may not be suitable for VANET safety applications. This is due to possible on-line system disconnections and delays, which may possibly lead to a network wide breakdown

In [50], a framework was proposed for commercial applications and it used a tamper proof device for security. The core idea is to purchase a file from an ongoing highway. Three entities are used (1) a broker (authorized agency) (2) a buyer (user) (3) a seller (RSU). Every vehicle has to register with a broker and after registration, the broker provides an ID to the user which is used later between the user and the RSU because the broker is reliable. However, the user and RSU both do not trust each other. If the file is large, than the other vehicle will work as a relay node and send pieces of the file to the user. After verification, they share a symmetric key between each other for the file transfer. The tamper proof device has three modules which are an authentication module, a decryption module and a digital fingerprint module.

An authentication module is responsible for verifying the signature of the seller and compares the identities of the receiving message and saves them in the tamper proof device. If both are successful, then it moves to the next phase. The decryption module using a symmetric algorithm decrypts the file and computes the hash values;

if the hash values are equal, it moves to the next and last phase, which is the digital fingerprint generation. This module creates a unique copy of the file by utilizing the user's real identity. If anyone redistributes the file it can be traced down by the authority.

2.2.6 Trusted Certificate and Preventing Attacks Based Schemes

In [51], the authors give a concept to reduce the computational overhead by leaving a certificate or sending a message without a signature or, by skipping the verification process for the received message. If a vehicle sends a message the first time, it is always attached with a certificate and stored. The next time the same vehicle sends a message without a certificate it only verifies by the key and compares it with the previous message certificate. It reduces the size of the message significantly. The second approach is not normally used in critical scenarios because every beacon sends signatures only when a vehicle senses any critical situation. When this happens, it then starts to send a beacon. This method is called situation based signature omission.

In [52], the authors presented a survey of security attacks that have been studied so far in VANET studies. After reporting such incidents, the authors presented a security solution which deals with anonymity key management, privacy and location. In this study, the proposed scheme is for geocast security. On the basis of the attacker model, this study proposed a geocast security protocol. The proposed scheme is lightweight and scalable. Another study [56], discussed challenges and issues in the VANET security environment. Two methods were proposed; one is for storing the certificate list in a Tamper Proof Device (TPD) where there is no need to validate the certificate.

The idea is to store the certificate of messages that are coming for the first time in the list. This will validate and save them in TPD. After 10 minutes, the certificate will be removed and the message will be checked again. However, during these 10 minutes there is no need to verify certificates in the message. The other method is that emergency messages should not be verified and there should be a special certificate (1 minute lifetime) that can be used in emergency cases.

Many studies tried to tackle Sybil attacks in different assumptions and techniques that are defined in [13], [53][54–56]. In Sybil attack, an attacker broadcasts several messages with bogus positions and identities. Many studies proposed possible ways to handle Sybil attacks such as public key infrastructure, resource testing, propagation models, secure positioning and distinguish ability. The distinguish solution depends on four propositions. The proposed model receives the data and reports similar data. A large number of received data will be accepted.

The proposed model is based on the secure positioning model. This study utilizes directional antennas (signal strength) and node cooperation for trustworthiness of the position of the vehicles. The author gives the position method. The paper proposed a model that uses the distance bounding scheme and infrastructure. In this model, it calculates the node's next position by putting the received signal strength into the propagation model. If the vehicle position is not within the limits of the estimated position, that vehicle is considered as a malicious node. Another proposed solution is to verify vehicle computational resources.

2.2.7 TPM based Schemes and Frameworks

The Trusted Platform Module (TPM) is a hardware chip introduced to be implemented in a VANET environment [11]. This study suggested several specific properties. First a VANET vehicle must have a Unique Identifier (UD); that UD is linked with pseudonyms and the authority involved to track the source vehicle. The second property is message integrity, which must be proven by an authentic message hash and the trustfulness of the message inside must be certifiable. The system configuration provides certain types of guarantees that the system parameter readings are correct. It has been noticed that TPM can bring a reliability factor to VANET technology. However, TPM has to be designed according to the requirements of VANET applications because VANET safety applications are time critical and compact in message size. Currently TPM is being suggested in one study as cooperative with the RSA method which is faster in verification but at the same time RSA has a larger key size.

A TPM based security architecture is proposed in [57], the basic concept is that every vehicle is embedded with TPM and vehicles are preloaded with a set number of cryptography keys to provide anonymity. That pair of cryptography keys is used for a short time to create a pseudonym. On a need basis, memory sticks can be used to create new key pairs. Furthermore, this study gives a brief overview of two schemes which are the Privacy Certificate Authority (PCA) and the Direct Anonymous Attestation (DAA) for anonymous attestation. The PCA focuses more on revoking the anonymity by using an authorized trusted entity, and for scalability, the DAA scheme is suggested with some adjustment. The revocation mechanism is used for revoking keys EK and AIK. The PCA is responsible for informing the compromised EK and AIK. When EK is taken away, then all the list of AIK revoked is linked with that EK; however, if AIK is compromised the revocation list will be updated by using the memory stick.

An TPM identity based concept present in [58], basically an identity based scheme for VANETs to cover security and privacy. The Trusted Third Party (TTP) is used to generate private keys for users after an authentication task is completed. TTP does not contain any record for binding keys. After authentication, the user gets a key. That key can be used for further operations such as encryption, decryption, signing and verification. This scheme is not utilized for the Certificate Authority (CA) or Key Distribution Center (KDC). Four levels are proposed in the scheme the first level is the setup (initializes all system parameters and computes all public and private keys). The second level is extraction (private key is computed). The third level is encryption. In this level data is encrypted by using the blowfish algorithm. The last level is decryption. In this level, data is decrypted by the same blowfish algorithm.

In study [59], a scheme is proposed that is based on the rough set theory. This study also introduces the Mobile Trusted Module (MTM). MTM is divided into the Mobile Local-owner Trusted Module (MLTM) and the Mobile Remote Owner Trusted Module (MRTM). MLTM works the same way as TPM. MLTM users can use the nearest local device and perform activities. MRTM cannot access directly any local device like the MLTM. MRTM performs all activities to restart in safe boot and certifies that all engines are able to perform in the right manner.

2.2.8 Implementation of ECC based Trusted Platform Module

In [60], the author implemented the Elliptic curve cryptography scheme based on TPM, which performs several operations including encryption, decryption, signature and verification. This study also compared ECC and RSA characteristics of a cryptosystem with TPM. ECC has many advantages over RSA. It can be seen that ECC is much more efficient in space than RSA. Moreover, ECC hardware implementation can bring much significant contributions towards technology.

It is shown in [61], that the ECC hardware chip is faster than software implemented cryptographic schemes. Table 2.1 shows that RSA takes more gate count than ECDSA; therefore ECDSA significantly saves space and money (more gates increase the cost). ECC takes 3260 gates, whereas RSA takes 34000 gates and after being optimized for space, ECC takes 48,400 and RSA 150,000.

There are two kinds of key agreements available: the ECDSA and the well know scheme Elliptic Curve Diffie Hellman (ECDH); ECDH provides a secret path between two parties to share a key. The author used a TPM based emulator [62] to verify the behavior of the ECDSA and ECDH schemes. According to the TPM specification, it describes four classes of data protection, namely: Binding, Sealing (sealed-Binding), Signing and Sealed-Signing.

Table 2.1: RSA and ECC Gate Counts [60]

Algorithm	Optimization	Time (ms)	Gate Count
RSA-1024	Space-optimized	4.90	34,000
ECC-163	Space-optimized	0.66	3,260
RSA-1024	Speed-optimized	2.60	150,000
ECC-163	Speed-optimized	0.35	48,400
RSA-3072	Space-optimized	184	50,000
ECC-283	Space-optimized	29ms	6,660
RSA-3072	Speed-optimized	110ms	189,200
ECC-283	Speed-optimized	1.3ms	80,100

2.2.9 TPM chip J3210

In [63], the authors designed and implemented a TPM high performance chip j3210 that was built into several modules of RSA/ECC, a cryptographic engine, a hash engine, a symmetric engine, a random number and some peripheral interfaces. The complete architecture is defined with internal and external buses. The asymmetric module contains two schemes RSA and ECC. Table 2.2 defines RSA and ECDSA cryptographic schemes by their signature sizes, verification and key generation time comparison. Furthermore, for symmetric module J3210 a 128-bit block cipher engine is used.

The SMS4 algorithm is integrated in the symmetric module which can produce a cipher text about 150 Mbps. The Random Number Generator (RNG) built into this chip is to generate an arbitrary seed for the Pseudo Random Number Generator (PRNG).

Table 2.2: Performance of Asymmetric Acceleration Engine [63]

Schemes	Signature Time (ms)	Verification Time (ms)	Key Generation Time (ms)
RSA-2048	59.54	0.67	<7000
RSA-1024	10.10	0.28	<900
ECC192	15.25	30.69	5.04
ECC224	17.79	35.28	5.85
ECC256	20.23	40.71	6.72
ECC384	39.01	78.27	12.84

Then PRNG can produce a random seed automatically or manually. Finally, a HASH module engine is integrated with the Secure Hash Algorithm (SHA1) which can perform hash with an output width of 20 bytes.

2.3 Comparison Between Well Know Schemes and Frameworks

After an extensive literature reviewed of early proposed work along with their categories. In the following section three tables are developed in order to explain the early work contribution and limitation. The Table 2.3 and 2.4 discusses advantages

and disadvantage of early proposed work, where Table 2.5 defines security characteristics.

Table 2.3: VANET Security Schemes

Scheme	Work	Advantage	Disadvantage
ECDSA	Asymmetric (PKI) 192 (bytes),224(bytes)	Small in size Fast in key generation	Computation Costly Slow in generation and Verification
AES	Symmetric key size 128(bytes),256(bytes)	Small in key size Fast in encryption/decryption	Lack of non-repudiation
ECDH	Asymmetric key size 28(bytes),32(bytes)	Fast in processing Key exchange algorithm	Limited applications
RSA	Asymmetric (PKI) 1024 (bits), 2048 (bits)	Fast in verification	Very large in size Slow in key generation
NTRU	Asymmetric (PKI) Size 197(bytes)	Fast in generation and verification then ECDSA	Large in size but not as much RSA
TESLA	Symmetric 80 (bytes)	Provide source authentication	TESLA uses delay key disclosure. TESLA vulnerable against memory attack. Lack of non-repudiation
Group Signature	Asymmetric (PKI) Privacy preservation , size 260 (bytes)	One key is used for group of vehicles Vehicles can traceable in event of forge message	Very high computational burden Key size is large
Blind Signature	Asymmetric Privacy preserving	No need of certificate	Magnitude is higher than ECDSA

Table 2.4: VANET Security Framework

Scheme	Work	Advantage	Disadvantage
VAST	Framework Combination of TESLSA/ECDSA	VAST contain both signature ECDSA and TESLA	Large in size Not proactive approach, Delay in key discloser not suitable for low latency application
EAP-Kerberos	Online token base	Mutual Authentication Safety and commercial application	Not suitable for VANET environment specially for V2V communication If not able to connect online then whole network will survive
Pseudonym Scheme	Asymmetric Privacy	Chain of small certificates	Increased certificate management.
Hybrid Scheme	Combination of pseudonym and group signature schemes	Untraceable Unlikable	Difficult to manage Increase size of message.
GSIS	Combination of group signature and identity based cryptograph	Short in massage size, traceable in event of bogus message ,privacy	Delay in Key broadcast not good for low latency applications, message drop ratio high.
TVSC	Combination of TESLA and SVC (TSVC)	Small in overhead, less message drops	Latency is quite high.

Table 2.5: Security Characteristics in Security Schemes and Frameworks

Schemes	Authentication	Integrity	Privacy	Non Repudiation	Platform Authentication	Efficiency	Reliability	Availability	Cost
RSA	✓	✓	×	✓	×	✓	✓	×	L
NTRU	✓	✓	×	✓	×	✓	✓	×	L
ECDSA	✓	✓	×	✓	×	×	✓	✓	L
Group Signature	✓	✓	✓	✓	×	×	✓	×	L
TESLA	✓	✓	×	×	×	✓	×	✓	L
ID based	✓	✓	✓	✓	×	NA	NA	×	L
Online	✓	✓	×	✓	×	NA	×	×	H
TPM based-RSA	✓	✓	✓	✓	✓	✓	✓✓	×	L
GSIS	✓	×	✓	✓	×	×	✓	✓	L
Raise	✓	✓	✓	✓	×	✓	✓	✓	H
TVSC	✓	✓	✓	✓	×	×	✓	✓	L
VAST	✓	✓	✓	✓	×	×	✓	✓	L

✓ Strong ✓✓ Very Strong × Weak H Costly L Not Costly NA Not Available ↑↑ Very High

2.4 High Priory Safety Applications

Table 2.6 defines safety applications that are high priority applications described by the US National Highway Traffic Safety Administration (NHTSA) and Vehicle Safety Communications Consortium (VSCC) [64]. There are applications which are Point to Multipoint (P2M), Infrastructure to Vehicle (I2V), Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). It can be noticed in Table 2.6 that all applications' communication ranges are between 50 - 300 meters and the data transmitted within these applications can be "position, direction, velocity and heading". Similar kinds of data can be handled efficiently by the Message Dispatcher (MD) [20].

Table 2.6: Safety Application [65]

Application	Communication Type	Frequency	Latency (ms)	Range (meters)	Data Transmitted
Traffic Signal Violation	I2V One way P2M	10Hz	100	250	Signal Status, Timing, Surface Heading, Light Position ,Weather,
Curve Speed Warning	I2V One way P2M	1Hz	1000	200	Curve Location, Curvature, Speed Limit, Bank, Surface
Emergency Brake Lights	V2V Two way, P2P	10Hz	100	200	Position, Deceleration Heading, Velocity
Pre-Crash Sensing	V2V Two way, P2P	50Hz	20	50	Vehicle Type, Yaw Rate, Position, Heading, Acceleration.
Collision Warning	V2V one way, P2P	10Hz	100	150	Vehicle Type, Position, Heading Velocity, Acceleration, Yaw Rate
Left Turn Assist	I2V and V2I One way P2M	10Hz	100	300	Signal Status, Timing, Position. Direction, Road Geom., Vel. Heading

Lane Chang Warning	V2V one way, P2P	10Hz	100	150	Position, Heading, Velocity Acceleration, Turn Signal Status,
Stop Sign Assist	I2V and V2I One way P2M	10Hz	100	300	Position, Velocity Heading, Warning.

MD is discussed in detail in the next chapter. Table 2.6 also highlights the latency, it is noticed that most of the safety applications are required 100 milliseconds latency, it's due to nature of application. This study focuses on the safety applications that are required 100 milliseconds latency.

2.5 WAVE IEEE 1609.3 and IEEE 1609.2

The IEEE 1609.3 standard [9] is described as transport and network layers (layer 3). The WAVE is defined as the new protocol wave short message protocol (WSMP). The WSMP is an efficient protocol defined by this standard. The safety applications operating on WSMP are composite according to 1609.2 secure message formations. The IEEE 1609.2 standards [8] describe the formation of secure messages for the required applications and the cryptographic principle is defined to achieve a certain level of security in the message. The format of the message is described in this standard as illustrated in Figure 2.6 and the cryptographic services are defined as follows.

<table>
<tr><th>Length (octets)</th><th colspan="4">Field</th></tr>
<tr><td>1</td><td>protocol version</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>1</td><td>type = signed</td></tr>
<tr><td>1</td><td rowspan="15">signed message</td><td rowspan="2">signer</td><td>type=certificate</td><td></td></tr>
<tr><td>125</td><td>certificate</td><td></td></tr>
<tr><td>1</td><td rowspan="13">unsigned message</td><td rowspan="3">Application</td><td>ACID</td></tr>
<tr><td>1</td><td>length of ACM</td></tr>
<tr><td>10</td><td>ACM</td></tr>
<tr><td>2</td><td>message flags</td><td></td></tr>
<tr><td>2</td><td>length of application data</td><td></td></tr>
<tr><td>32</td><td>application data</td><td></td></tr>
<tr><td>8</td><td>message generation time</td><td></td></tr>
<tr><td>4</td><td rowspan="3">location of message transmission</td><td>latitude</td></tr>
<tr><td>4</td><td>longitude</td></tr>
<tr><td>3</td><td>elevation and confidence</td></tr>
<tr><td>28</td><td rowspan="2">signature</td><td rowspan="2">edsa signature</td><td>r</td></tr>
<tr><td>28</td><td>s</td></tr>
</table>

Figure 2.6: Secure message format in IEEE 1609.2 [8]

The 1609.2 defined the asymmetric cryptographic scheme as a default trial and that scheme's name is ECDSA, as defined above in this chapter. Furthermore, this standard also explains that every broadcast message should be hashed, encrypted (signed), and embedded with a certificate issued by the Central Authority (CA). There are two sizes of keys described in this standard; one is a 224 bit and the other is a 256 bit. It is reported in many studies that the ECDSA processing capability is slow when there are 100 to 200 signatures to be authenticated.

2.6 Schemes Size

Table 2.7 defines security schemes and their cryptographic signature sizes, which are used so far in a VANET environment. The format of the message in VANET is already illustrated in Figure 2.5. Table 2.7 contains payload, certificate, and public. The payload size contains 180 bytes where as the message type and version are 1 byte long and the certificate size is 125 bytes as described in 1609.2 [8]. It is noticed that

mostly early studies only considered one application payload, in this studies considered an average payload size which is 180 bytes.

Table 2.7: VANET Security Schemes

Schemes	Scheme Size (Bytes)	Certificate (Bytes)	Payload (Bytes)	Total Size (Bytes)
RSA	512	125	180	817
NTRU	394	125	180	699
ECDSA	64	125	180	369
Group Signature	520	125	180	825
TESLA	80	-	180	260
AES	32	-	180	212

2.7 Summary

This chapter surveys the earlier suggested schemes on the focus area, beginning by presenting classification schemes based on the software and TPM based schemes and frameworks.

A high computational cost is incurred by the asymmetric Public Key Infrastructure (PKI) scheme. In order to reduce it, alternative schemes have been proposed, which are covered in this chapter. However, most of these schemes incurred tradeoffs with regards to processing overhead, such as large message size, communication delay and higher bandwidth utilization. Considering these issues, a symmetric cryptographic technique is proposed that provides less overhead and a fast verification process. However, it may consider less security measure than the PKI schemes. It is also noticed that many proposed work are simulated in IEEE 802.11a standard, which is not standard for VANET technology.

In addition these security schemes lack in providing the minimum delay for the low latency safety applications. It is also reviewed that mostly scheme broadcast interval higher than application requirement. Furthermore all early proposed studies are considering small payload, which is only suitable for one application data. It is

reported in many studies; that is possibility more than one applications running on vehicle simultaneously.

CHAPTER 3

PROPOSED SECURITY FRAMEWROK

This chapter is divided in three parts. In first part of this chapter, a research methodology defines that to be taken in this work to address the security issues in VANET. To overcome these issues a security framework which consists of internal and external parts is proposed. The internal part describes components that are related to the message construction and cryptographic schemes. The external part, which is further divided into two sub parts of group entities and group communication, discusses entities and protocols, which are required to construct a group.

Next, in second part of this chapter, a formal validation software called *"Automated Validation of Internet Security Protocols and Applications (AVISPA)"* is introduced. In order to understand the functionality of AVISPA, its architecture, and components are discussed. Following this designing parameters of V2V protocol are discussed. In the third part of this chapter, a "*Network Simulator 2 (NS2)*" is defined that helps in understanding the basic concept and flow of tool. Also the basic sets of properties of 802.11p protocol are described including its propagation models, and the performance matrices are studied in detail.

3.1 The Proposed Framework

It has been identified through literature review that the safety applications are mainly brought into practice for providing security. Few studies have also been conducted related to non-safety applications. However, this research work is focused only on safety applications of VANET due to its importance for life saving.

Security is one of the key requirements for successful implementation of VANET technology. In this respect, designing a suitable security framework using VANET is

important in order to avoid time delay in safety application that directly affects human lives. It is essential for VANET to provide fast and secure communication in real time manner. In this regard, a framework is proposed as depicted in Figure 3.1.

This proposed security framework concept taken from [11], [41] [12], [17], this framework assists in providing fast and secure schemes to overcome some critical issues in the safety applications. The proposed framework deals with low latency safety applications like emergency brake, lane changing warning, and pre-collision sense among others.

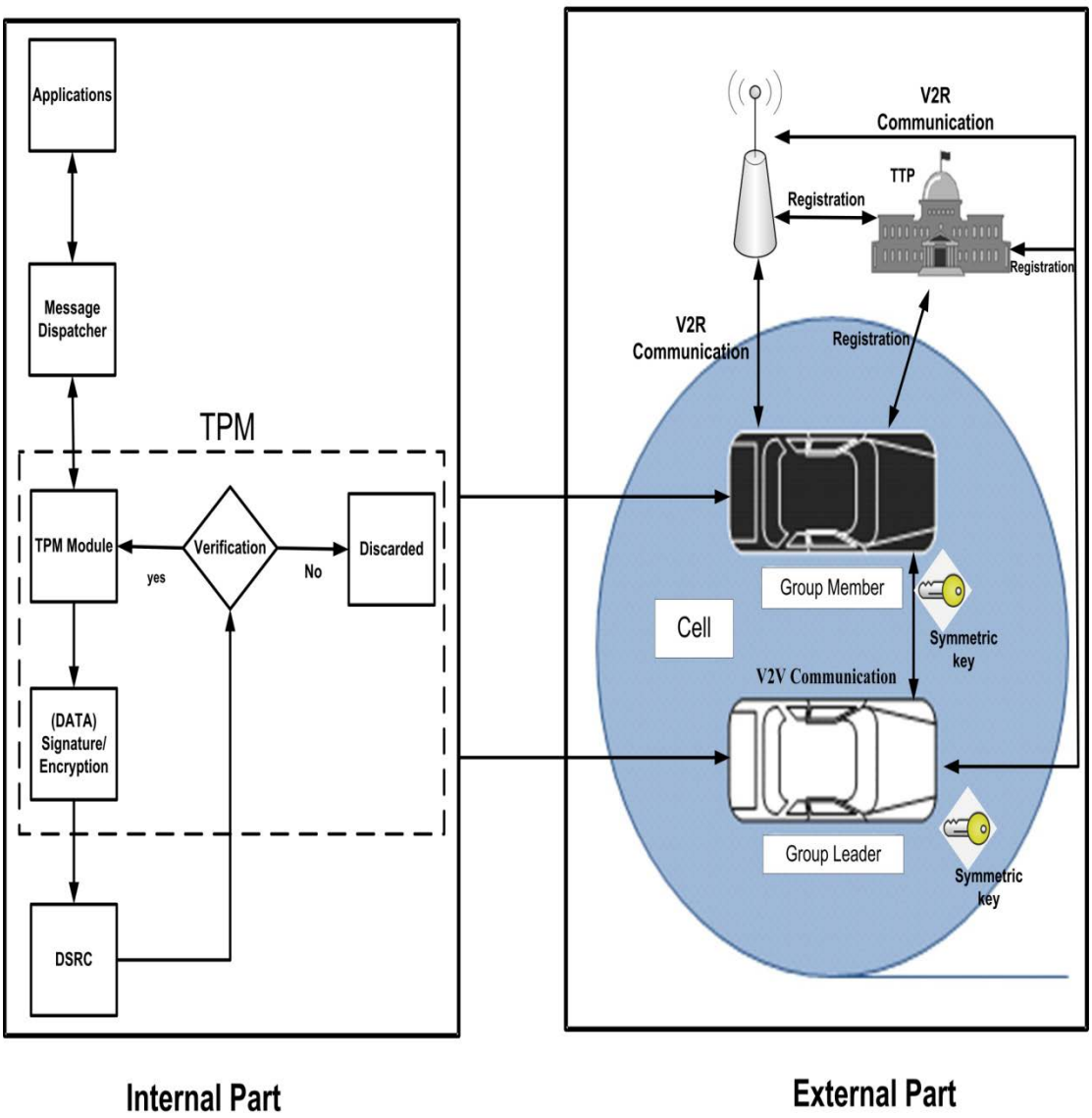

Figure 3.1: The proposed VANET security framework

This proposed security framework is divided into two parts i.e. internal and external. The internal part of the framework consists of different hardware components that are installed in every vehicle. The components of the internal part are described below following the flow of information from component to component as illustrated in the left hand box of Figure 3.1.

Step 1: Applications - This is where the flow of information in the proposed framework begins, the multiple safety applications running on vehicle at time. This step is responsible to handover applications information to the message dispatcher.

Step 2: Message Dispatcher (MD) - MD is a component which exists between the applications and lower layers in the framework. It is responsible for eliminating duplicated information received from several applications. It should be sending only a minimum set of information to TPM.

Step 3: Trusted Platform Module (TPM) - TPM is a chip, which is embedded onto vehicles to perform cryptographic functions at data in certain modules, i.e. asymmetric, symmetric, hash, and random number generator. It also performs signature and verification processes on the incoming and outgoing messages in VANET.

Step 4: DSRC - DSRC works at the lowest two layers (Phy and MAC), it is responsible to receive and send information on air.

The external part of the proposed framework is divided into two sub-parts namely Group Entities and Group Communication. There are six kinds of group entities in the framework that are defined as follows and illustrated in the external part of Figure 3.1.

Cell : Each entity has its own role in the proposed security framework. The highway is divided into small cells, in which vehicles are entered and form a group.

Group Leader and Group Members : In a group, some vehicles themselves are considered as group members and one of them is selected as the group leader.

Symmetric Key : Each group uses a symmetric key to broadcast a safety message.

Roadside Unit (RSU) : Roadside unit operates only where it has been installed on the highway.

Trusted Third party (TTP) : The trusted third party is introduced in the proposed framework for registration purposes; every vehicle and roadside unit is first registered by a trusted third party to get a certificate for key pair.

The second sub-part is group communication which deals with two communication protocols; these assist the vehicles to join the group in the particular cell and share a symmetric key.

Vehicle-to-Vehicle Protocol (V2V) : The V2V protocol defines authentication process and share symmetric key among group members.

Vehicle-to-Roadside unit Protocol (V2R) : The V2R protocol describes the vehicle-to-roadside unit communication scheme, in the same manner as a V2V protocol dose respectively.

This section only provides an abstraction of the proposed framework. It helps in understanding the architecture and functionality of each component at their positions. In the internal part, it is mainly focused on the Message Dispatcher (MD) and Trusted Platform Module (TPM).The detailed description of these components is given in the following sections. In addition, the external part consists of the group entities and group communication that are also discussed in detail in the following sections.

3.1.1 Message Dispatcher (MD)

There are many safety applications running on vehicle that contain the same type of data. It is noticed that most of early proposed studies only considered one application at the time; however there are significant possibility more than one application tries to send data simultaneously. In this study the Message Dispatcher (MD) is use to manage these similar kind of data and reduce channel utilization, MD is also significantly helps to avoid DoS attack. The message dispatcher is a component that works between the Application layer and the lower layers. It establishes a channel for

the safety applications to obtain the required data in an efficient way in both directions from the application layer to the DSRC (lower layers) and vice versa [20].

It receives data from the Application layer and extracts the similar type of data elements, e.g. speed, position, and direction. The data elements are the key information that require more than one safety application simultaneously. Figure 3.2 illustrates the basic concept of MD. The safety applications, named emergency break and curve warning in Figure 3.2 both contain the same type of data elements such as position, direction, and speed.

The related data elements are collected by the MD from the Application layer. MD puts that data elements in one packet and rest of the duplicated data elements are discarded. Actually MD creates a packet which has a minimum set of data elements. After that, the packet which contains the data elements will be delivered to the DSRC (lower layers) for broadcasting. At the receiving end, the MD receives the packet from the DSRC and it is responsible for detaching all data and data elements. Finally, the MD distributes all the data among the required applications as illustrated in Figure 3.2.

Considering the functionality of the MD and reduce the load of network during message assembly by sending one possible minimum set of data. MD breaks each message mainly into two portions, which are the data frames and data elements. The data frame part consists of unique id and all required data elements or only one data element. The second portion is data elements that are not part of data frames; it is possible that some of the data elements are put separately from data frames. This is due to some of safety applications may require different data elements [20].

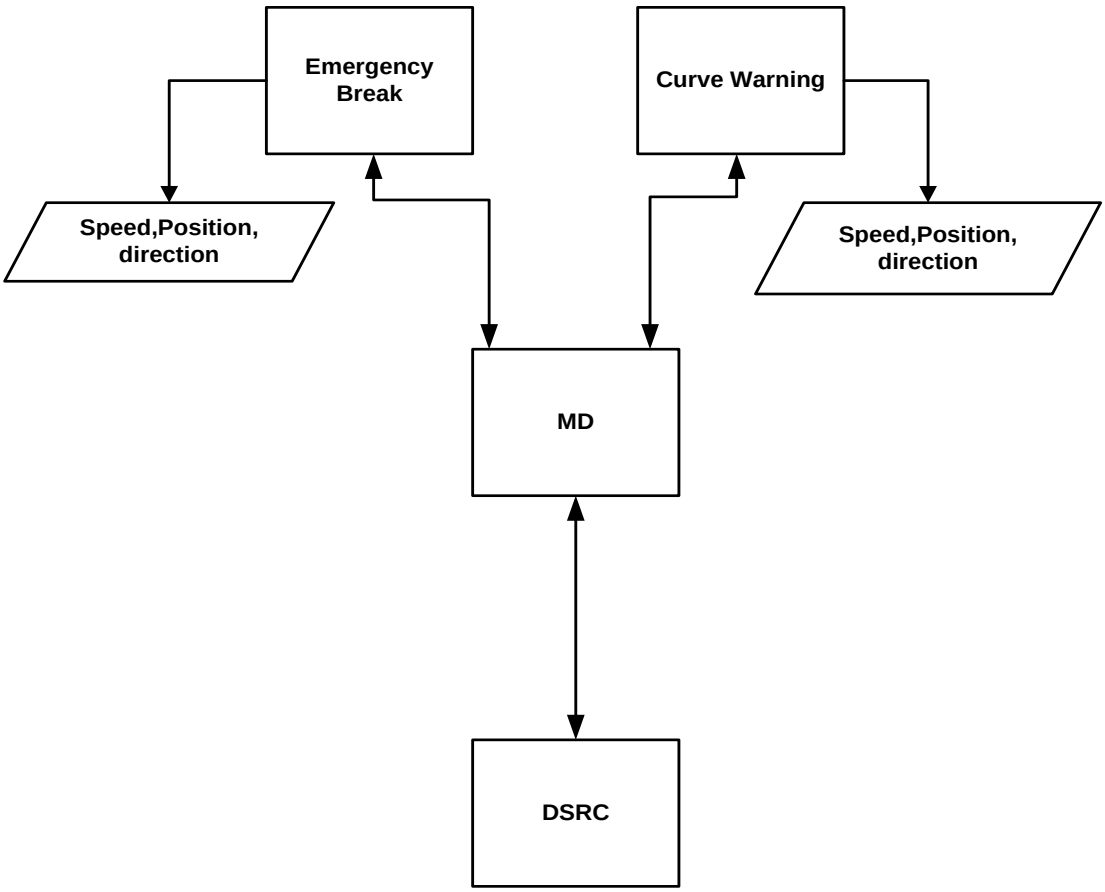

Figure 3.2: Message Dispatcher Work Flow [4]

There are more than 70 data elements that have been identified and out of that 32 have been selected as common data elements; the MD size depends on required safety application data. The two safety applications namely emergency break and intersection vehicle message size (payload) is 176.5 bytes using MD [20]. Considering this message size, the average payload size for the proposed framework is set to 180 bytes.

3.1.2 Cryptography Modules

In the proposed framework, the internal part is associated with the TPM module which consists of the security modules as illustrated in Figure 3.3. Each module plays an important role in ensuring the security of VANET. In the TPM hardware architecture in the proposed framework, the chip is further divided into several sub-

modules. This Figure also shows the interaction among input/output components of the TPM. The interaction of these sub-modules is demonstrated in Figure 3.3 that helps in understanding the architecture and functionality of each module in the proposed framework.

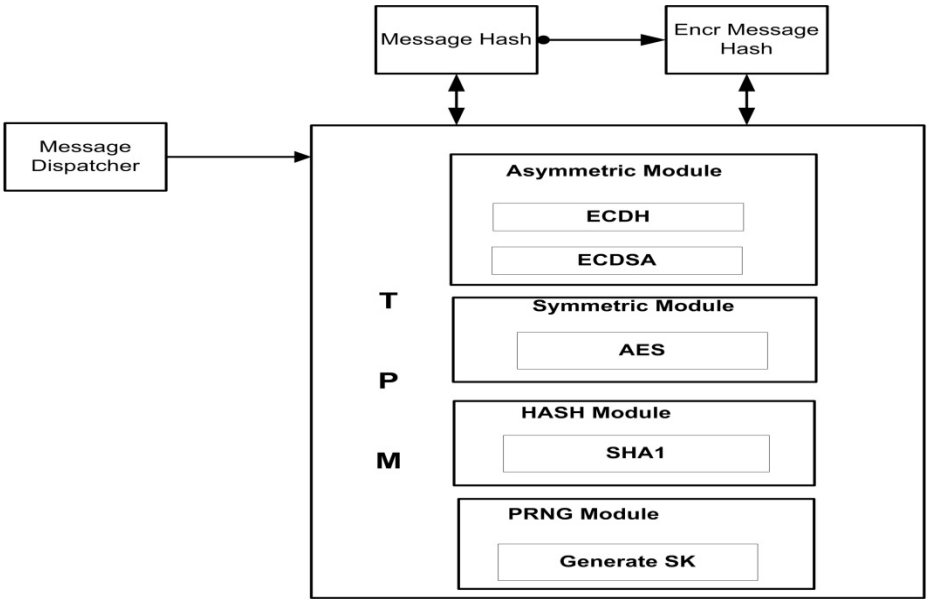

Figure 3.3: TPM hardware sub-modules and its security operations

a) Asymmetric Module: Currently, the TPM uses the asymmetric module which consists of two security methods known as the Elliptic Curve Cryptography (ECC) and Rivest, Shamir, & Adleman (RSA) [63]. These methods are responsible for generating the two keys which are public and private keys. In earlier studies, the TPM has been suggested with the RSA method [11] for providing security in VANET. It is observed through different studies that the RSA security method comes with a large key size. Whereas, the ECC security method comes with a small key size. Thus the motivation is increased to use this method in the proposed framework. This framework uses the ECC module with the TPM in order to accomplish the security of VANET. The ECC module performs two functions, i.e. ECDSA and ECDH; it has a small sized key that is generated signatures very fast. The ECC comes in different key sizes such as 224 and 256 bits. However, it has been found through studies that the ECC method

introduces slow verification using VANET. One of the most important features of the ECC is that it provides the same level of security as provided by the RSA.

b) Symmetric Module: The symmetric security module uses the Advance Encryption Standard (AES) cipher for encryption and decryption. It comes with different key sizes, i.e. 80, 128, and 256 bits. The AES method performs encryption and decryption very fast, with the possibility of a thousand times faster as compared to PKI schemes. Keeping in mind the features of this method, it is used in the proposed framework for broadcasting safety messages in VANET. However symmetric scheme is considered less in terms of security to overcome this issue a trust factor is established in this framework using vehicle to vehicle protocol.

c) Random Number Generator: The Random Number Generator (RNG) generates the seed numbers. It can generate the hash string by accepting function. Primarily, it generates seed randomly and then applies an appropriate function to get a resultant sequence number accordingly. The Random Number Generator (RNG) can also be used for generating asymmetric keys or secret keys derived from any mathematical function[24].

d) Hash Module: It is an important module, which provides the hash function that helps in receiving the data and converting it into a fixed size of digest. It is also called string. The hash module uses the Secure Hash Algorithm1 (SHA1) method which is responsible for converting the data into the hash form/cipher text form. The basic function of this method is to provide message reliability in terms of identifying the unaltered message/unchanged message [24].

3.1.3 Group Entities

It has been discussed above that the group entities relate to the external part of the proposed framework and they play an important role in accomplishing the objectives of this study. The group entities are a set of different elements that are defined in the proposed framework in order to form a group. During group formation, primarily, a cell is created and its size is defined respectively. After that, a cell is logically divided

into segments in order to select a group leader in a particular cell. When communication is established between a group leader and group members, then the communication duration is calculated accordingly for managing the next group leader in the cell. Furthermore, a symmetric key is assigned for appropriate group communication in a particular cell.

3.1.4 Cell and its Segments

Using VANET, a cell and its segments play a vital role in enhancing the performance of communication among the vehicles. These cells can be divided into different fixed and variable sizes. However, this study attempts to divide a highway and urban areas into fixed cell sizes accordingly. This technique helps in improving the performance of VANET, and it also assists in forming the groups. It is identified through various studies that there are different types of techniques that can be used to create cells. For example, the cells can be created with the help of a road side unit, the navigation map on vehicles, and the global positioning system (GPS).

However, in this proposed framework, the fixed sizes of cells are created in a circular shape with the help of a navigation map and GPS. This concept assists in occupying the whole highway; so when any vehicle enters a new cell it will be notified by the navigation map. In addition, in order to reduce the load and to achieve easy selection of a group leader, each cell is further divided into segments. This segmentation technique mainly helps in reducing the load and facilitates the selection of the group leader. Three segments are created in each cell as illustrated in Figure 3.4.

These three segments are named the Forward Segment Area (FSA), Trailing Segment Area (TSA) and Group Leader Select Area (GLSA). Each segment has its own significance in terms of selecting and joining the group leaders. For example, the group selection segment named the GLSA represents the center of the cell and occupies a small size as compared to the other two segments. The nearest vehicle travelling on the GLSA is capable of selecting a Group Leader (GL) or it can be

treated as the group leader itself for other up-coming vehicles in case there is no group leader present in that cell.

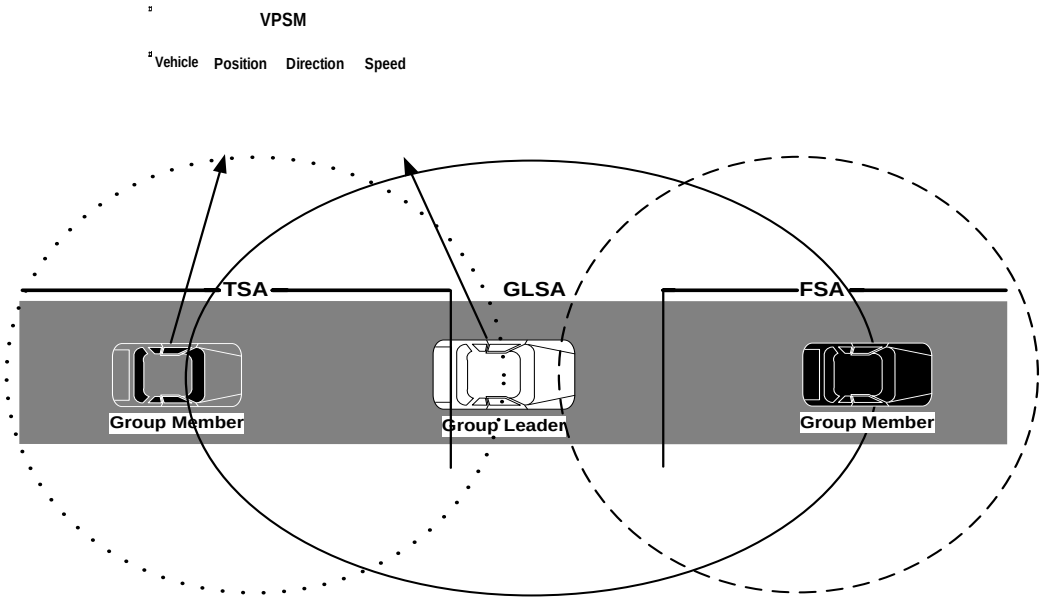

Figure 3.4: Road segments

Every vehicle maintains a table named the Vehicle Position and Speed Measured (VPSM) table for selecting a group leader. The VPSM table maintains the record of direction, position and speed of all neighboring vehicles according to their current speed and position at a particular location. The VPSM facilitates the process of selecting a group leader and assists in identifying the next group leader for each up-coming vehicle in the cell. Once, the group leader is selected then it authenticates the neighboring vehicles in a group that may consist of two or more vehicles.

After's successful authentication process, a symmetric key is shared by the group leader for proper group communication. Later on, when the role of group leader is over, it activates itself for the role of Group Member (GM). When, a group is formed completely then every vehicle is considered as a group member in the cell. There is the responsibility of each group member to authenticate and share the symmetric key among the upcoming vehicles in that particular cell. As reported in existing studies, there is a problem of frequent changing of group leaders in the cell [35]. The proposed technique in the framework helps to reduce frequent changing of the group leader and assists in managing the group easily. Furthermore the mutual authentication process

verifies *PCR*, and *SML*, that provides a guarantee that both vehicles platform is not compromised presently.

3.1.5 Forward Segment Area and Trailing Segment Area

Right next to the Group Leader Selection Area (GLSA) in a cell is the Forward Segment Area (FSA) as illustrated in Figure 3.4, in which vehicles are able of receiving messages from the present cell and the next cell. These vehicles work as relay vehicles respectively between two cells. The relay vehicle keeps both keys from the present cell and also from the next cell. The FSA segment gets the information from the upcoming Trailing Segment Area (TSA) for keeping communication continuous. Both the FSA and TSA reserve larger areas than the GLSA The size of TSA is the same as FSA. The TSA is considered as an entrance point of the cell at which any vehicle that is nearest to the GLSA can be selected as a group leader according to the VPSM table.

During the group leader selection, it is important to calculate the communication time period of vehicles in a group. It helps in identifying which vehicle remained in communication in the GLSA for the longest duration. This calculated time period does not only help in selecting the group leader, but it also plays a vital role in the authentication process. The time period is calculated accordingly between the neighboring vehicles using equations (1) and (2).

$$Lifetime_{link} = \frac{R - \left| d_{ij} \right|}{\left| v_i - v_j \right|}. \qquad (1)$$

$$Lifetime_{link} = \frac{\sqrt{R^2 - w^2} + s.\sqrt{d_{ij}^2 - w^2}}{v_i + v_j} \qquad (2)$$

Equation (1) calculates the communication duration of the vehicles which are moving towards each other in different lanes. Equation (2) calculates the communication duration for two vehicles that are on the opposite lanes. Where *'R'* represents the range,*'d'* is the absolute distance between two vehicles, *'i'* and 'j' are vehicle 1 and vehicle 2, and '*v*' represents the velocity . In equation (2), *'w'* represents the separation of the distance among two vehicles (vehicle 1 and vehicle 2). In equation 2 *'s'* represents the link distance between two vehicles, s value become s = 1 when two vehicles are moving toward each other, and s = -1 when they are moving in opposite direction. Both equations are used in the existing studies and these are recommended for time calculation among the vehicles [66].

3.1.6 Group Leader and Group Member

As discussed in the above section, the Group Leader (GL) is selected in the group leader selection area and it is responsible for two tasks i.e. authentication and sharing symmetric keys. The authentication task is performed using the vehicle-to-vehicle communication protocol upon the arrival of new vehicles in the cell. After a successful authentication process has been performed, a vehicle is considered as an authenticated group member (GM) in the cell. The group leader's second task is to generate a symmetric key using a random generator module, and to distribute it to the group members. Whenever, a new group leader is selected, it generates a new symmetric key accordingly. But first, the group leader needs to authenticate the upcoming vehicles before it is able to share the symmetric key respectively. Furthermore, a group member can be located at any segment of the cell and can even join two groups at the same time in VANET.

The group leader and group members are synchronized by time in the cell. Using this synchronization process, every message pertains to the time information as well as data of the road conditions. Every group member remains synchronized in the cell due to two reasons, i.e. the refreshing of the symmetric key after a fixed amount of time and the recreating of the group. The key refreshing takes place within the group of vehicles in a particular cell. Every group member is able to compute a new key

from the original symmetric key. This phenomenon introduces the concept of chain of keys that assists in deriving the new key from the present key.

Using this concept, it is difficult for attackers to trace the new generated key through a valid TPM. It is one of the main reasons to avoid tracing; if attackers really want to trace the generated key then they need a valid TPM. In order to find an attacker or invalid user in the group, the concept of recreation that takes place randomly is used. This recreation of a group is possible through a synchronized time frame in which a new group leader is selected in a fixed amount of time. In this process, the first group will be disjointed automatically and again the vehicles are able to create a new group using the V2V protocol in a particular cell. Meanwhile, the recreation of group, in particular, assists in identifying an attacker in the cell; whereas, the chain of keys helps in reducing key theft accordingly.

3.1.7 Symmetric Key

The symmetric key is distributed among group members through a group leader or road side unit. After a successful distribution of the symmetric key among the group members, each group member is also able to authenticate the coming vehicles and distribute the symmetric key as well. The authentication process is defined by certain steps that are illustrated in Figure 3.5. Steps 1 to 10 are responsible for authentication, whereas steps 11 to 13 are involved in symmetric key distribution. This whole process is done through the vehicle-to-vehicle protocol. The symmetric key is always generated whenever a new group leader is selected in the cell.

The authentication process is done by using ECDSA scheme and symmetric key is transferred through the secure asymmetric scheme called the Elliptic Curve Diffie-Hellman (ECDH) [26]. The ECDH is a variant of the Elliptic Curve Digital Signature algorithm (ECDSA). Basically, the ECDH is an asymmetric cryptographic scheme which provides a high level of security due to its asymmetric nature. It is a key agreement algorithm that is used to share the symmetric key between two vehicles to provide security at an unprotected channel. In the case when two vehicles want to

share a symmetric key, then they need each other's public key. This public key and certificate are transferred through a trusted third party.

Every vehicle is loaded with public and private keys in the cell. If a group leader wants to communicate with vehicle *A* to share the symmetric key, then it is necessary for the group leader to have the public key of vehicle *A*. Similarly, vehicle A would also need to have the public key of the group leader as described in Table 3.1. This table describes the sharing process of the public keys in line 3 and 4 [26]. However, the distribution of the valid public key in the whole process must be done securely. To ensure security, the agency is responsible for providing a certificate that other current vehicles are not invaders in the cell. After that, the group leader uses the public key of vehicle A to encrypt the symmetric key, and send it to vehicle A accordingly. The proposed framework uses the symmetric key, i.e. the Advance Encryption Standard (AES) key 128 bits for safety applications in the cell.

Table 3.1: ECDH Scheme

Line1 :$Vehicle_A \rightarrow PR_A\ Pub_A$
Line2 :$Vehicle_{GL} \rightarrow Pr_{GL}\ Pub_{GL}$
Line3 :$Vehicle_A \rightarrow PR_A\ Pub_{GL}$
Line4 :$Vehicle_{GL} \rightarrow PR_{GL}\ Pub_A$
Line5 : $Vehicle_{GL} \rightarrow (SK \parallel Cert_{Ps})\ encrypt_{(PUB)A}$

Basically, the AES is a well known block cipher, and this scheme is used to encrypt and decrypt a bulk of data simultaneously. It has different key sizes, i.e. 64, 128, and 256 bits. It has different combinations such as AES-ECB and AES-CCM. The 1609.2 is a VANET protocol that suggests the AES-CCM 128 scheme as a symmetric key [10] for encryption/decryption and message authentication. Based on the suggestion, the same version of AES is used in the proposed framework module.

In the proposed framework, there are three types of message sizes used; one at the time when any new vehicle enters the cell to join the group. At that time, the message format used is *message format* = $(APP_{Data}||\ PCR||SML||Cert_{Ps}||Key_{ECDSA})$, where APP_{DATA} is applications data, which is around 180 as described in message dispatcher, *PCR and SML,*these are hash values called message digest. These message digest values are required to authenticate a platform components states. $Cert_{Ps}$ is a TTP certificate for user authentication and there are two keys that are denoted as Key_{ECDSA} for digital signature. The second type of message is used when the symmetric key is shared; the *message format* = $(SK||Cert_{Ps}||Key_{ECDSA,})$. *SK is* symmetric key that is sent to newly arrived vehicle after the authentication process. The third type of message is used for safety message broadcasts, and its *message format* = $(APP_{DATA}||SK)$. All message sizes are defined in Table 3.2.

Table 3.2: Message Formats and its Sizes

Message type	Application Data (bytes)	Platform Data (bytes)	Certificate (bytes)	Key (bytes)	Total Size (bytes)
Join the group	180	30	125	64	399
Share the symmetric key	NA	NA	125	32 and 64	221
Safety Messages	180	NA	NA	32	212

3.1.8 Group Communication

In order to achieve group communication, the two protocols named the Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside unit (V2R) are used. Pertaining to the V2V protocol, it defines certain steps for a new vehicle to go through in order to join an existing group and provide its credentials in the cell. Whereas, the V2R protocol also describes certain steps of a roadside unit fixed (infrastructure) in order to authenticate the vehicles and share a symmetric key as well. Furthermore, the trusted third party took part in these protocols to register and validate the credentials of vehicles and the

RSU on the highway. The specific notations which are used in these protocols are illustrated in Table 3.3.

Table 3.3: Protocols Notations

Abbreviation	Explanation
V_A	Vehicle $_A$
V_{GL}	Vehicle Group Leader
RSU_K	RSU Key
EK	Endorsement Key
PS	Pseudonym
Cert	Certificate
AIK	Attestation Key
SK	Symmetric Key
TPM_A	Vehicle $_A$ TPM
OBU_A	Vehicle $_A$ OBU
TPM_{GL}	Vehicle $_{GL}$ TPM
OBU_{GL}	Vehicle $_{GL}$ OBU

3.1.9 Vehicle-to-Vehicle Protocol

The communication that takes place in the cell between the group leader and new member has been discussed in the previous sections. When any new vehicle enters into the cell, then that vehicle broadcasts an acknowledgment message accordingly. In this case, the group leader responds back. However, if there is no vehicle in a cell, then a newly entered vehicle will be considered as the group leader. This whole process is illustrated in Figure 3.5, and steps are defined after this figure.

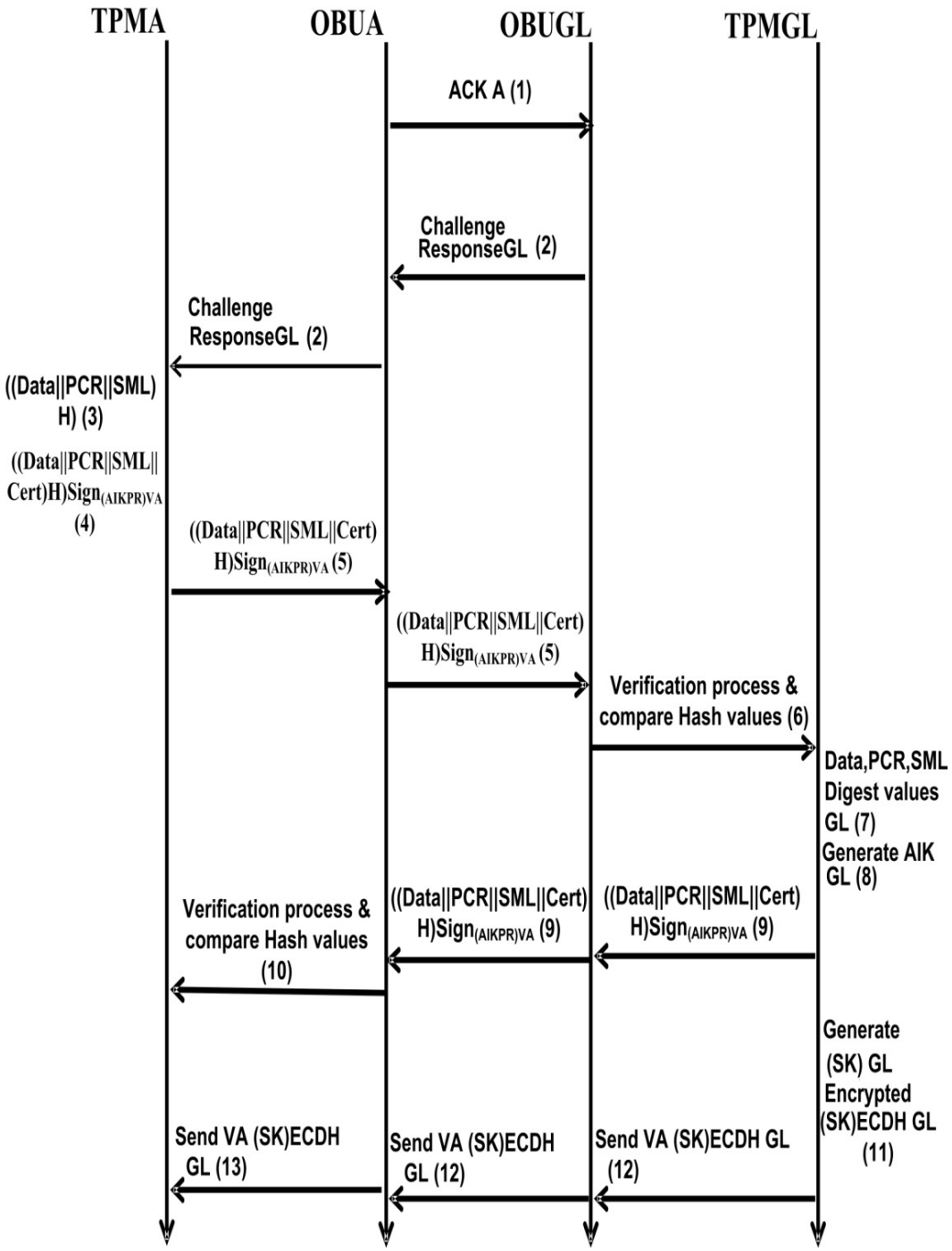

Figure 3.5: Group Leader and New Member Communication

Step 1: Vehicle A (V_A) sends an acknowledging (Ack) message to a group leader (V_{GL}).

Step 2: Group leader (V_{GL}) receives a request from the vehicle A (V_A) and sends the challenge response to vehicle (V_A).

Step 3: Vehicle A (V_A) receives the challenge response from the group leader (V_{GL}). In addition, vehicle A (V_A) collects the application DATA, PCR values, SML values, and digest them; ((Data||PCR||SML)H).

Step 4: Vehicle A (V_A) also generates attestation identity key (AIK_{PR}) and encrypts ((Data||PCR||SML)H) digest values using Vehicle A's private key, (AIK_{PR})V_A. After that, vehicle A (V_A) embeds a pseudonym certificate with message and sends to the group leader (V_{GL}); ((Data||PCR||SML||Cert)H)$Sign_{(AIKPR)VA}$.

Step 5: Group leader (V_{GL}) receives the message from vehicle A (V_A).

Step 6: After receiving the signed message from vehicle A (V_A); the group leader (V_{GL}) runs a verification process to authenticate Vehicle A (V_A). If that verification process is done successfully, then the group leader runs a hash algorithm to compare the hash values. If the hash values are equal as the sender's hash values, then the message is considered as unaltered. Otherwise, the message is discarded. V_{GL} ((Data||PCR+SML||Cert)H)Verify(AIK_{VA}) = comparing of hash values and verification of signature.

Step 7: Group leader (V_{GL}) collects the DATA, PCR values, SML values, and digests them using hash module; (Data||PCR+SML)H).

Step 8: Group leader (V_{GL}) generates an attestation identity key (AIK_{PR}) and encrypts the message using group leader's private key (AIK_{PR}) $V_{GL,}$ and embeds a pseudonym certificate with a message. After that, the message is sent to vehicle A; V_{GL}(Data||PCR||SML||Cert)H)$Sign_{(AIKPR)VGL}$.

Step 9: Vehicle A (V_A) receives the message from the group leader (V_{GL}).

Step 10: Vehicle A (V_A) runs verification process to authenticate the group leader (V_{GL}). If a verification process is done successfully, then vehicle A runs a hash algorithm to compare the hash values. If the hash values are equal as the sender's hash values, then the message is considered as unaltered. Otherwise, the message is discarded accordingly.

((Data||PCR+SML||Cert)H)Verify$_{(AIKPR)VGL}$ = comparing of hash values and verification of signature.

Step 11: Group leader (V_{GL}) generates Symmetric Key (SK) and encrypts it with vehicle A's public key, (SK)$V_{A(Pub).}$

Step 12: After that, the group leader (V_{GL}) sends an encrypted SK to vehicle A (V_A).

Step 13: Vehicle A (V_A) receives the secret key and stores it for future communication.

3.1.10 Vehicle-to-Roadside Unit Communication Protocol

In vehicle to roadside communication, if any vehicle enters the range of the roadside unit, then it is the responsibility of the RSU to verify and distribute the symmetric key to that vehicle. This communication protocol introduces the trusted third party; the RSU is responsible for generating a pseudonym certificate for the concerned key pair. Basically, the pseudonym certificate is provided to the authorized vehicles for future communication. Here, the RSU plays the same role as the group leader in the vehicle-to-vehicle communication. However, the RSU is connected with the TTP which plays the role as the middle agent between a vehicle and the TTP. If any vehicle wants a certificate for the concerned key pair then it encrypts an attestation key with the endorsement key and sends it to the RSU.

Since the all over installation of the RSU or TTP on the highway is very costly, the proposed protocol is used only in the specific areas wherever the RSU is already installed on the highway. If the RSU is installed in a particular area, then the vehicle initially needs to communicate with the RSU instead of the group leader of the cell. This has several advantages. For example, the RSU has faster processing capabilities and more resources than the vehicle itself. In particular, the RSU also covers a greater communication range as compared to a single cell. In this process, the RSU remains in communication within its neighboring RSUs in VANET. Once any vehicle gets a symmetric key, then it is able to communicate with other vehicles in the cell. The

steps which are involved in the vehicle-to-roadside unit communication protocol are illustrated in Figure 3.6 and steps are described after this figure.

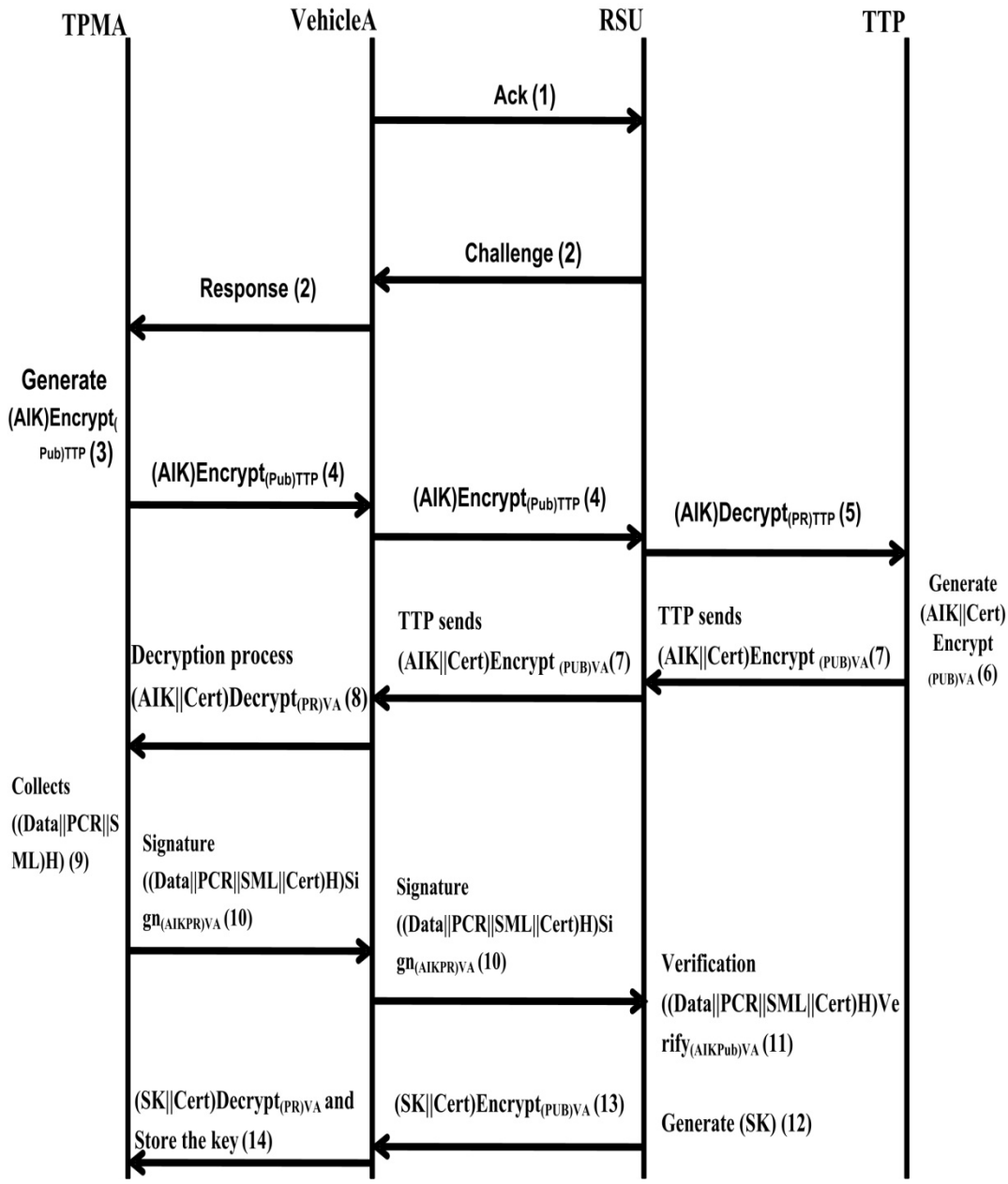

Figure 3.6: Vehicle and RSU Communication

Step 1: Vehicle A (V_A) sends an acknowledging (Ack) message to the RSU.

Step 2: RSU receives a request from vehicle A (V_A) and sends a challenge response to Vehicle A (V_A).

Step 3: Vehicle A (V_A) receives the challenge response from RSU. Then TPM generates an Attestation Key (AIK) and encrypts it with a Trusted Third Party public key, (AIK)Encrypt$_{(Pub)TTP}$.

Step 4: Vehicle A (V_A) sends an encrypted Attestation Identity Key (AIK)Encrypt$_{(Pub)TTP}$ to the RSU. Then RSU forwards that message to the Trusted Third Party (TTP).

Step 5: Trusted Third Party (TTP) is responsible for decrypting Vehicle A's (V_A) message, using TTP private key. If the decryption process is successfully done, then TTP generates a pseudonym certificate for Attestation key pair (AIK) and encrypts it with vehicle A (V_A) public key. If (AIK)Decrypt$_{(PR)TTP}$ is successfully, then (AIK||Cert)Encrypt$_{(PUB)VA.}$

Step 6: Trusted Third Party (TTP) sends the encrypted Attestation Identity Key (AIK) and certificate (Cert) with Vehicle A's public key to RSU,(AIK||Cert)Encrypt $_{(PUB)VA}$.

Step 7: Roadside Unit (RSU) forwards that message to vehicle A.

Step 8: Vehicle A receives the encrypted message from RSU. Vehicle A (V_A) decrypts the message using private key. If the decryption process is successfully done, then Vehicle A (V_A) stores the Attestation Identity key pair (AIK) and certificate; (AIK||Cert)Decrypt$_{(PR)VA}$.

Step 9: Vehicle A's TPM_A collects the Data, PCR and SML values and digest them; ((Data||PCR||SML)H).

Step 10: After collecting the required values, Vehicle A (V_A) signs those values using attestation identity key(AIK), and attaches them with AIK certificate and finally sends to the RSU, ((Data||PCR||SML||Cert)H)Sign$_{(AIKPR)VA}$.

Step 11: Roadside Unit (RSU) receives the message and verifies Vehicle A's signature and compare digest values. If any value or certificate of the vehicle is invalid, then the message will be discarded; ((Data||PCR||SML||Cert)H)Verify $_{(AIKPub)VA}$.

Step 12: If the verification process is completed successfully, then the RSU generates Symmetric Key (SK), and encrypts it. But before that, the RSU also executes step 5 to step 9 in order to authenticate mutually.

Step 13: Roadside Unit (RSU) sends an encrypted Symmetric key with Certificate to Vehicle A; (SK||Cert)$Encrypt_{(PUB)VA}$.

Step 14: Vehicle A (VA) compares the decrypts. After a successful decryption process, Vehicle A (VA) stores the Symmetric Key (SK) for future communication; (SK||Cert)$Decrypt_{(PR)VA.}$

3.1.11 Trusted Third Party

In the proposed framework, the Trusted Third Party (TTP) is used to register the road side unit and vehicles for authorization. The vehicles are registered by giving an endorsement key (EK) to the TTP. Whereas, every RSU has a unique key and that is used for registration by the TTP. One of the advantages of registering the RSU is that mutual authentication between a vehicle and RSU can be achieved. Figure 3.7 describes the TTP registration process for the vehicle and roadside unit. After registration, the registered vehicle can generate the AIK key pair, and verify it by the TTP in order to get a certificate for future communication.

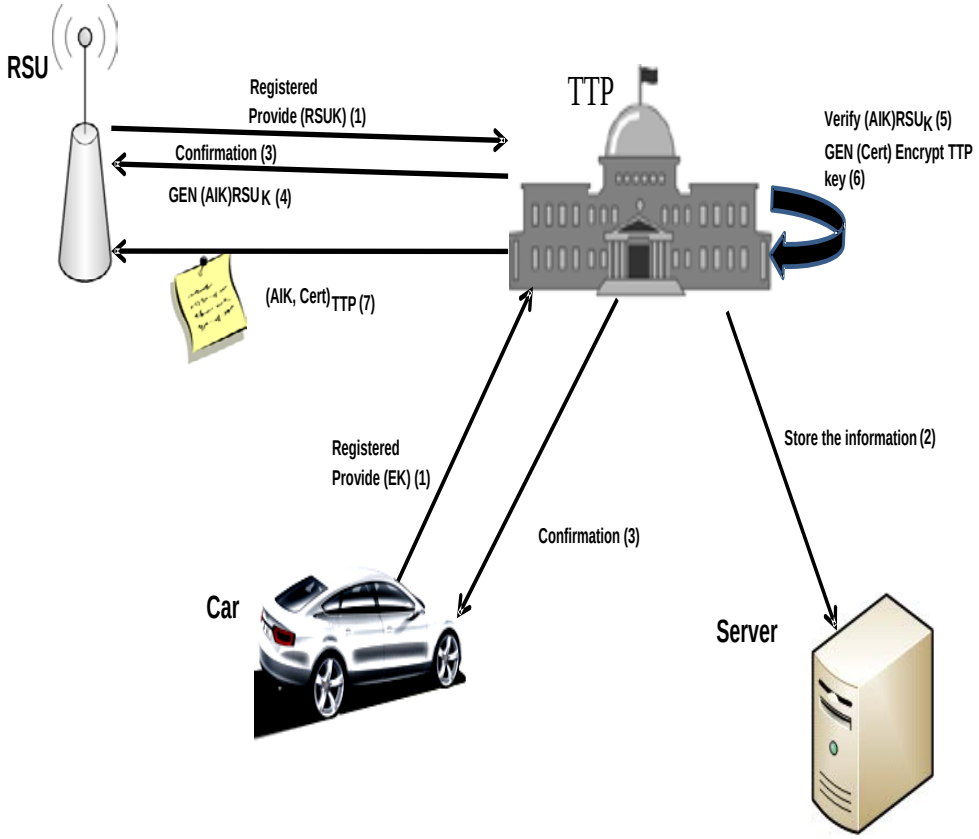

Figure 3.7: RSU and Vehicle Registration

Step 1: Roadside Unit (RSU) and Vehicles will be registered from the Trusted Third Party (TTP).

Step 2: Trusted Third Party (TTP) is responsible for registering vehicles and RSU. After the verification of vehicles Endorsement Key (EK) key and RSU key.

Step 3: Trusted Third Party (TTP) sends confirmation message to RSU and vehicles.

Step 4: After that the RSU generates Attestation Key (AIK) and encrypts it with RSU's master key and sends to the TTP.

Step 5: Trusted Third Party (TTP) is also responsible for verifying the RSU's master key.

Step 6: After that, the Trusted Third Party (TTP) generates certificate for AIK key and encrypts it with the TTP key.

Step 7: Finally, the TTP sends Attestation Key (AIK) and certificates to the RSU.

3.2 AVISPA Tool

In order to build the trust among vehicles during communication, a V2V protocol has been proposed in this study. It is very important to make sure that the proposed protocol works appropriately and enrich the trust among vehicles. In this respect, AVISPA tool is used that helps in designing, developing, and analyzing the security protocols.

This tool provides a console environment in which code is written in *"High Level Protocol Specification Language (HLPSL)"*. This language is used for defining the security protocols and assists in analyzing the proposed security properties of a protocol. Furthermore, this tool is used to validate the new defined security protocol and its parameters. The structure and architecture of AVISPA, is illustrated in Figure 3.8.

The first stage of AVISPA tool is HLPSL, HLPSL written code is translated into the Intermediate Format (IF) by using hlpsl2if. The second level of this tool is intermediate format (IF), it is a lower-level language and is interpreted by the back-ends. There is no input from user and this tool is called automatically. Intermediate Format (IF) is developed to give easy interface to the user to select different back-ends and analysis the results. Basically in AVISPA back-end term is used for different model checkers, these model checkers are designed to verify the protocol's security property and possible attacks. Currently, AVISPA tool provides suite with four back-ends, that are On-the-fly model checker (OFMC), SAT-Based Model- Checker (SATMC), Constraint-Logic-based Attack Searcher (CL-AtSe), and Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP) [67].

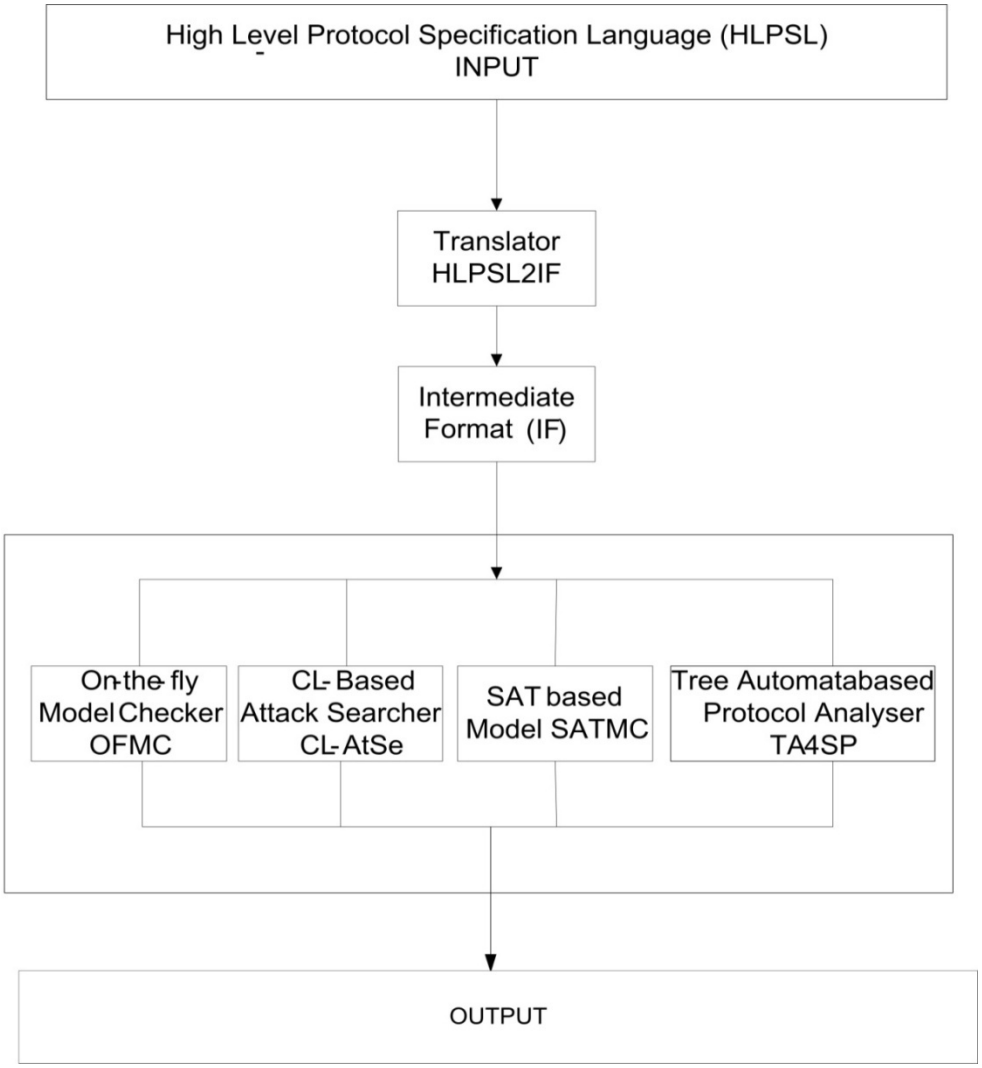

Figure 3.8:HLPSL Architecture [68]

3.2.1 On-the-Fly Model Checker (OFMC)

OFMC is a symbolic model checker for analyzing security protocols, The OFMC is a mixture of two techniques based upon lazy and demand driven search. The lazy technique is used to create the data type, which builds an efficient *on-the-fly model checker* to handle very large data types, or infinite state spaces for protocols. The demand-driven search is a combination of symbolic techniques for modelling a Dolev-Yao attacker. The Dolev-Yao, attacks are created in a demand-driven manner[67].

3.2.2 CL-ATse automatic security protocols analyzer (CL-ATse)

CL-ATse automatic security protocols analyzer is designed for two main objectives. The first objective is simple to extend the set of protocols that can be investigated. The second objective is to get large number of protocol sessions outputs.CL-ATse gets a input from intermediate format that describes the rules and limitation. It runs solving methods to checks all available states of the participants, if attack exists[67].

3.2.3 SAT-Based Model Checker (SATMC)

SATMC stand for SAT-Based Model Checker, SATMC is also model checker for security and cryptographic protocols. The goal of SATMC is to perform operation on the fixed number of sessions and analyzed the problem. The SATMC considers general attacks (Dolev-Yao Model) that are involved in transmission of messages[67].

3.2.4 Tree Automata-based Protocol Analyzer (TA4SP)

The Tree Automata-based Protocol Analyzer is based on the automata theory. It is designed to create an automaton language, which is represents network resources and over-approximation. This language approximates the network configuration and works on limitless number of sessions[67].

3.3 Design Goals for V2V Protocol

The main purpose of V2V protocol is to authenticate vehicles credentials to built trust among vehicles on-the-fly. Trust is provided in several possible ways or trust can be measured in levels. The main possible ways are:

1) A trust can be created based on any proof or evidence of identity that is provided in preceding communication protocols [69]. In VANET two or more nodes communicate with each other and provide some sort of facts (digital signatures, certificates) and on the basis of those facts authenticated node are to be trusted.

2) There is study in which trust is defined on levels such that 0 means distrust and 1 means trustful nodes [69]. In VANET trust can be measured on level basis in which there are two possibilities

- In first case, there is no trust because vehicle does not provide any kind of proof during verification procedure.
- In Second case, there are nodes that provide proof and they called trusted vehicles.

There is another level of trust that is called weak trust, in weak trusted vehicle provides proof, however verifier is not sure of the originality of the credentials, this issue can be mitigated by TPM as it was discussed in chapter 2.

In addition, to the security attacks such as fake identity, bogus information, and impersonating a vehicle, keeping in mind these security attacks, a V2V protocol is designed, in which three security properties are placed as illustrated in Figure 3.9.

1. Mutual Authentication
2. Message integrity
3. Privacy

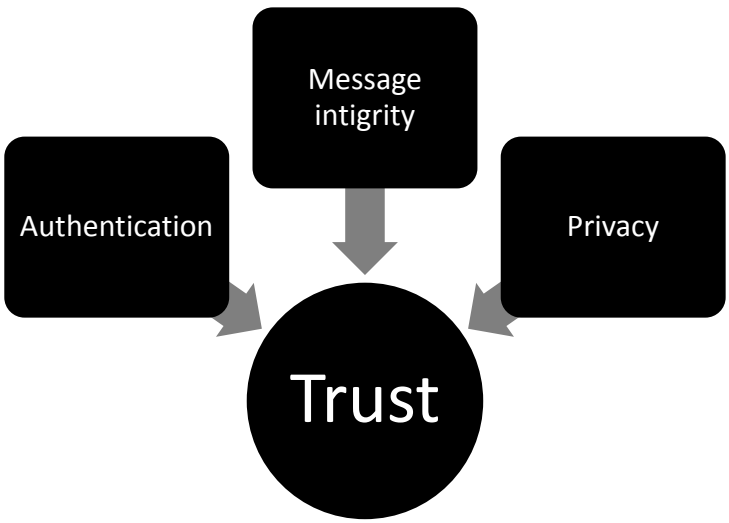

Figure 3.9: Trust building parameters

3.3.1 Authentication

The purpose of authentication is to design a security process such that it validates vehicle by verifying its credentials. In the proposed framework three different kind of credentials are part of the algorithm. These are

1. Digital signatures that is unique for each vehicle.
2. Certificate that is given by TTP (Trusted Third party).
3. PCR (Platform Configuration Register) and SML (Stored Measure Log) for validation of the platform.

Furthermore there are two kinds of authentications i.e one way authentication and two way authentication/mutual authentication. In the one way authentication operation is performed by a vehicle, whereas the mutual authentication both vehicles perform the operation to provide strong verification.

The V2V protocol performs two operations as described below, sender vehicle collects application data APP_{DATA} that contain information regarding road conditions (speed, position, warning), platform registers and log values *PCR+SML*, and certificate is provided by *TTP Cert.* These credentials are then used to calculate the hashes which are finally signed by a private key. The recipient vehicle executes verification process, in which receiver authenticates source signer by a public key. In the same way group leader also sends its credentials to be verified by vehicle and assure strong authentication. It is noted, that two credentials are being verified here, one is user credential and second is the vehicle platform such that it increases level of trust.

Source $\rightarrow((APP_{Data||}\ PCR+SML||Cert_{Ps})HASH)Sign_{(vehicle)}$

Destination $\rightarrow((APP_{Data||}\ PCR||SML||Cert_{Ps})HASH)Verify_{(GL)}$

3.3.2 Message Integrity

The message contains the same information from the source node to the destination node. In which no modification has been made during the transmission period and this is called message integrity. Message integrity is one of the most important security elements in VANET. In order to achieve message integrity, a security method named the Secure Hash Algorithm-1 (SHA-1) is used, which ensures data integrity. The Secure Hash Algorithm-1(SHA-1) creates a hash string known as a message.

The secure hash algorithm is able to convert meaningful data into a special character string called a message digest. This digest is compared at the recipient end, if the received message digest produces the same results, then it is considered as a valid message otherwise that message is considered as bogus and discarded respectively. In the proposed V2V protocol, the message integrity provides security using asymmetric and symmetric schemes. In the asymmetric scheme, every message should be encrypted and digested using SHA-1 as described in the lines below. Whereas, using the symmetric scheme, the SHA-1 is also used to create the digest of the message without generation of a certificate.

Line 1: Source $\rightarrow$(APP_{Data}||PCR+SML|| $Cert_{PS}$)HASH = Digest

Line 2: Destination $\rightarrow$ compare = Digest = (APPData||PCR+SML||$Cert_{PS}$)

3.3.3 Privacy

During communication, confidentiality is an important requirement for protecting the secrecy of the vehicles' details. Therefore, it is necessary to ensure their confidentiality. It provides a protection against forgery and spoofing attacks. In order to provide privacy to the user and vehicle, a technique is used in the proposed framework in which only the trusted third party knows the real identity of the node. The trusted third party (TTP) provides the pseudonym short certificates (line 1) to the nodes for future communication. The pseudonym certificate contains information that is not related to the user's original information; only the TTP can link that pseudonym certificate to the original certificate.

However, if it is a case of fraudulence then, a symmetric key is used by multiple vehicles (group members) in which no one can trace the real identity. There are detailed steps described in V2R and V2V communication protocols that ensure security among the roadside unit and vehicles. In order to provide a secure channel, the proposed scheme uses the ECDH algorithm. Considering privacy in the message through asymmetric and symmetric keys, the two pseudo codes are described as follows. These pseudo codes provide typical messages in the proposed framework that ensure privacy in the message.

Line 1: Vehicle $\rightarrow$(APP$_{Data}$||speed||time||Direction||position|| Cert$_{Ps}$)sign$_{(AIK)}$

Line 2: Vehicle $\rightarrow$(APP$_{Data}$||speed||time||Direction||position)Encrypted $_{(SK)}$

3.4 V2V Protocol

In the V2V protocol, two parties are involved one is vehicle and second is group leader denoted as V and GL respectively. The vehicles initial role is to send a message and signature to group leader for authentication then group leader sends a message and signature to vehicle. The public keys are denoted as PKa, PKb, where hash function is denoted as H, Symmetric key denoted as Sk, and finally Na, and Nb are respectively nonces for detail check appendix A.

Protocol V2V :

Identifiers
GL, V : user;
Na, Nb : number;
Ta, Tb : number;
Mv, Mgl : number;
Xa, Xb : number;
PKa,PKb : public_key;
Sk : symmetric_key;

Messages

1. V$\rightarrow$ GL : V, {Ta, Na, GL, Xa, {Mv, {H(Mv)}PKa'}PKb}PKa'
2. GL $\rightarrow$ V : GL, {Tb, Nb, V, Xb, {Mgl, {H(Mgl)}PKb'}PKa}PKb'
3. GL $\rightarrow$ V : GL, ({Sk}PKa')

Knowledge

GL : GL,V,PKa,PKb,Xa,H;

V : GL,V,PKa,PKb,Xb,H;

Session_instances

[GL:groupleader,V:vehicle,Xa:data,Xb:data,PKa:pk1,PKb:pk2,H:h];

Goal

GL authenticates V on Na;

V authenticates GL on Nb;

Secrecy of Data

3.5 Network Simulator

Network Simulator 2 (NS2) is a well known simulator for wired and wireless networks, and a lot of work with respect to VANET has been done in NS2 [70], [71],[72] . The flow of NS2 working mechanism is defined in Figure 3.10 First, a TCL file is created that contains the configurations including propagation models (such as the TRG, Nakagami), topology settings, and node behavior. In the topology settings, usually a straight road is considered for simplification. Other parameters include simulation duration, packet interval, etc. After these settings TCL file executes, at the end of simulation, a file is created, which is called a trace file. The trace file contains the data like packet sending time and packet receiving time, and how many packets are received or dropped by a particular vehicle. Basically, trace files contain discrete events, that are undertaken during the simulation, these events are difficult to interpret and very large in numbers. Therefore, from the trace file required data is filtered using AWK or grep scripts, the filtered data is interprets according to the results. Then results and graphs are generated. This simulation process is illustrated in Figure 3.10 [73].

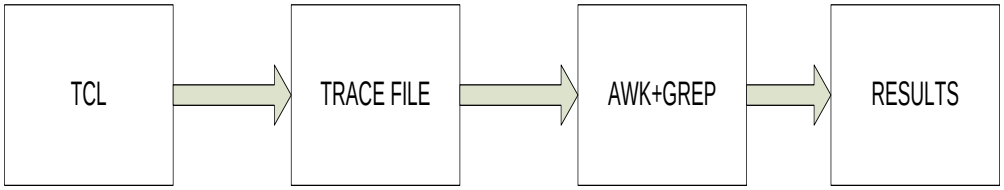

Figure 3.10: Network Simulator 2

3.6 Parameters used in simulations

The basic configurations for a VANET simulation are shown in Table 3.4. These configurations are incorporated in the extended 802.11 module with enhanced PHY and MAC layers [70]. There are different inter-frame spaces settings discussed in [71] [72] to ensure better utilization of channel, this study settings are defined follows.

Table 3.4: Default Configuration Setting

Configuration Parameter	Value
Transmission Range (set_p)	50/300 Meters
Frequency	5.85 GHz
Header Duration	40 μs
Basic Modulation Scheme	0
Preamble Capture Switch	1
Data Capture Switch	1
SINR Preamble Capture	3.1623 dB
SINR Data Capture	10.0 dB
CW Min	15 slots
CW Max	1023 slots
Slot Time	13 μs
SIFS	32 μs
Short Retry Limit	7
Long Retry Limit	4

- The set_ p stands for transmission power or communication range, which is 50/300 meters in this case.

- The frequency is 5.85 GHz, a default value for VANET.

- The header duration is the time when the packet header is sent, it takes 40 microseconds.

- There are 4 basic modulation schemes 0 to 3; the 0 scheme has 6 Mbps, the second has 12 Mbps, the third has 24 Mbps and the fourth has 54 Mbps. In our case, the 12 Mbps modulation is used in the simulation.

- Short Inter-frame space (SIFS): The SIFS is a time set between two frames and also used for the highest priority communication transmissions.

- Contention Window (CW): The CW is a mechanism, which is used to select a random number for the time to back-off.

- A preamble is used to notify the recipient that the frame has arrived; this function is at the physical layer. The Physical Layer convergence Procedure (PLCP) header encloses with information about the modulation scheme, frame body, frame length, and preamble. The starting part of the preamble contains a signal part, which is a modulation scheme (BPSK) radio configuration.

- Short Retry Limit: it is time that has been set for RTS, if a vehicle not able to send an RTS packet at specific time, it discards the corresponding data packet.

3.7 Propagation Models

The various propagation models are used for a VANET simulation environment to predict the effectiveness of signals at receiving and transmitting end at a certain distances. These models are capable of detecting fluctuation of signals at constant and variable distances. In order to establish propagation modeling the two common techniques always used, i.e. physical model and empirical model. For example, the free space model is used in scenarios that only require fading over the medium and the Two Ray Ground (TRG) model accommodates a direct and ground reflection path. The TRG is capable of providing reliable prediction at long distance paths as compare to free space model [72].

However, it has also been reviewed through different studies [72] that the Nakagami model is the most suitable propagation model for VANET. It consists of multipath and several fading effects in an environment and it can be customized for highway and urban scenarios. In this study, the both TRG and Nakagami propagation models are considered in simulation to verify the effects on traffic. Hence, the parameters of Nakagami propagation model are configured as shown in Table 3.5.

Table 3.5 has *gamma0*, *gamma1*, and *gamma2*; the gamma parameters represent the radio signal average attenuation over distance. The *d0_gamma_* and *d1_gamma_* are values for the distance where the gamma value discontinues and the *m* parameter is defined by the radio signal fading, corresponding to the *m* function. The variable is *use_nakagami_dist_* (true/false); all parameters are defined in Table 3.5 [70][72].

Table 3.5: Nakagami Default Setting

Parameters	Value
Omni Antenna	2.512
Gr_	1.0
dist_ false	500
gamma0_	1.9
gamma1_	3.8
gamma2_	3.8
d0_gamma_	200
d1_gamma_	500
m0_	1.5
m1_	0.75
m2_	0.75
d0_m_	80
d1_m_	200

3.8 Performance Metrics

The broadcast mechanism is used for a safety application in VANET; where all vehicles periodically send/receive messages simultaneously. It is an important to use the appropriate performance metric in order to understand the actual behavior of the given parameters. The performance metrics that have been used in the simulation of this study, these are introduced as follows.

- Packet Delivery Ratio (PDR): The packet delivery ratio of recipient vehicle is described, in which, the number of packets are sent by all neighboring vehicles to a recipient vehicle that exist in a communication range. The formula which is used to obtain PDR, Number of packets received by the receivers / total packets sent.

- End to End Delay (EED): The end to end delay of a packet is a specific time interval that is consumed by a packet from sending to receiving vehicle. The estimated average time can be calculated as consumed time by total received packets / total number of obtained packet.

- Message Drop Counts (MDC): The MDC is described using VANET, in which, the number of messages are dropped by recipient vehicle in total simulation time. It is necessary for the assessment of a security scheme. It helps in determining the MDC of a node to verify the impact of scheme on particular node.

- Processing Delay (PD): The time of a packet from sending to receiving vehicle and time taken by a packet for internal verification process is called PD. Basically, this time is included in EED, however in this study, PD is separated from EED to analyze result of schemes.

- Network Throughput (NT): The number of packets successfully transferred from one vehicle to another vehicle in specific amount of time in network is called network throughput. All vehicles in VANET environment broadcast messages among each other periodically and those messages are received accordingly. In this case, throughput can be calculated by selecting a particular receiving vehicle from simulation scenario. NT is calculated in a unit named as Kilo bytes per-second (Kbps).

3.9 Summary

In first part of this chapter, a new security framework that consists of two main parts i.e. internal and external parts is proposed. Basically, the internal part defines the Trusted Platform Module (TPM) and Message Dispatcher (MD). The main objective of the internal part is to provide a trust between vehicles using the TPM platform when there is usage of the symmetric scheme. The TPM is a hardware chip that comes with cryptographic modules that provides platform authentication. In addition, a Message Dispatcher (MD) is used to extract the data from the application and to reduce the redundancy of the duplicated data.

In addition, the external part in the proposed framework defines a setup for group communication among the vehicles in the cell. The main objective of the external part is to design a grouping scheme that assists in creating a group of vehicles and establishes a way for new vehicles to join that group easily and frequently. In order to select a group leader, the highway is divided into cells, and each cell is further divided into segments in VANET. Finally, the two communication protocols, i.e. V2V and V2R are designed to establish a fast way for vehicles to join a group, and securely handover the symmetric key.

In second part of this chapter, a protocol validation software is discussed, that is used to get results for V2V protocol. Finally in third part of this chapter, a network simulator flow is defined including its basic setting of 802.11p and propagation models (Nakagami and TRG). The network simulator is used in th study to get results of security schemes.

CHAPTER 4

RESULTS AND DISCUSSIONS

This chapter is divided into two parts. In the first part of this chapter, the two simulation scenarios are introduced i.e. highway and urban areas. The highway scenario is designed in such a way so that vehicles are placed at different speeds and locations, whereas in the urban scenario, vehicles are placed near each other to create a congested situation. By simulating both scenarios based on the proposed framework, the results are obtained and analyzed accordingly. In addition, these results are taken from two different propagation models in order to identify the different performance effects. In the second part of this chapter, AVISPA results analyzed and discussed with respect of security goals

4.1 Highway Simulation Setup

Generally, in order to design and simulate the highway scenario in VANET, three lanes in each direction are configured. In which, vehicles are placed at different distances. By following this concept of designing and simulating the highway in VANET, the number of parameters has been configured for simulation. In this setup, 384 vehicles are placed in 6 lanes at different distances. In the most inner lane, each vehicle is placed at distance of 50 meters with reference to another vehicle. However, at most outer lane, every vehicle is placed at a 30 meters distance from other vehicle. Subsequently, at the middle lane, each vehicle is configured at 40 meters distance from other vehicle. In order to simulate the highway scenario for three opposite lanes, the same procedure is undertaken for positioning the vehicles. This simulation scenario is illustrated in Figure 4.1.

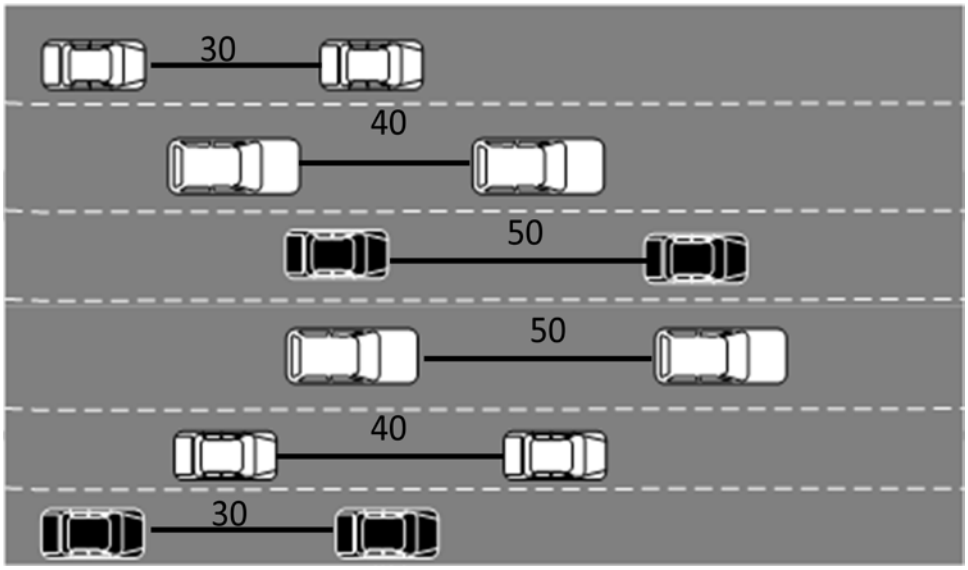

Figure 4.1: Highway Simulation Scenario

In this simulation, every vehicle broadcasts a message in 100 milliseconds with a 5 microsecond interval variation. This simulation is performed using the Nakagami and TRG propagation model with specific parameters as given in Table 4.1. Regarding the simulation, the packet delivery ratio, communication delay, message drop ratio, processing delay and network throughput performance metrics are undertaken. Furthermore all results are calculated the average values, the six vehicles taken in simulation scenario as receiving nodes (1 from each lane), the average value of these vehicles considered as a result.

In addition four security schemes are considered for simulation, i.e. RSA, NTRU, ECDSA, and AES, in which their key sizes are compared as given in Table 4.1. These schemes proposed by researchers for VANET security. In particular, the ECDSA and AES scheme have small key size and therefore are suitable for encryption/decryption in the VANET application. These schemes are implemented in proposed simulation setup and their results in terms of the performance parameters for safety application are analyzed.

Table 4.1: Highway Simulation Setting

Highway Simulation	Simulation Parameters
Total Vehicles No	384
Simulation time	20 second
Lane	6 (three in each direction)
Inner, Middle, Outer lane distance	30 m, 40 m50 m
Message size	100, 200, 300 ……. 1000 bytes
Broadcast interval	100 ms
Interval variance	0.05 ms
Communication Range	300 m
Propagation Model	TRG/Nakagami
Radio System	5.9 GHz DSRC
Bandwidth	6 Mbps

4.1.1 Packet Delivery Ratio (PDR)

By simulating the parameters, it is identified that large size of message has direct effect on receiving message ratio as illustrated in Figure 4.2. It is clearly mentioned that, if a message size is large then its performance delivery at receiving end drops down. As simulation is undertaken in two propagation models, i.e. Two Ray Ground (TRG) and Nakagami, in which, the key sizes of four different security schemes are investigated.

In TRG model, the outcome of investigation suggests that the NTRU scheme receives 33%, whereas the RSA scheme receives 28% respectively as shown in Figure 4.2. In addition, the ECDSA and AES methods have small size messages. Therefore, the outcome of the ECDSA obtains PDR up to 62% and AES scheme gets 86% approximately.

In Nakagami model, the obtained results suggest that the NTRU scheme receives 38% PDR and RSA scheme obtains 36% approximately. Whereas, the ECDSA scheme gets 57% PDR and AES scheme receives 71% as illustrated in Figure 4.2. It is

observed that performance of the AES scheme is better as compared to other schemes. It increases the probability of message reception in the emergency cases.

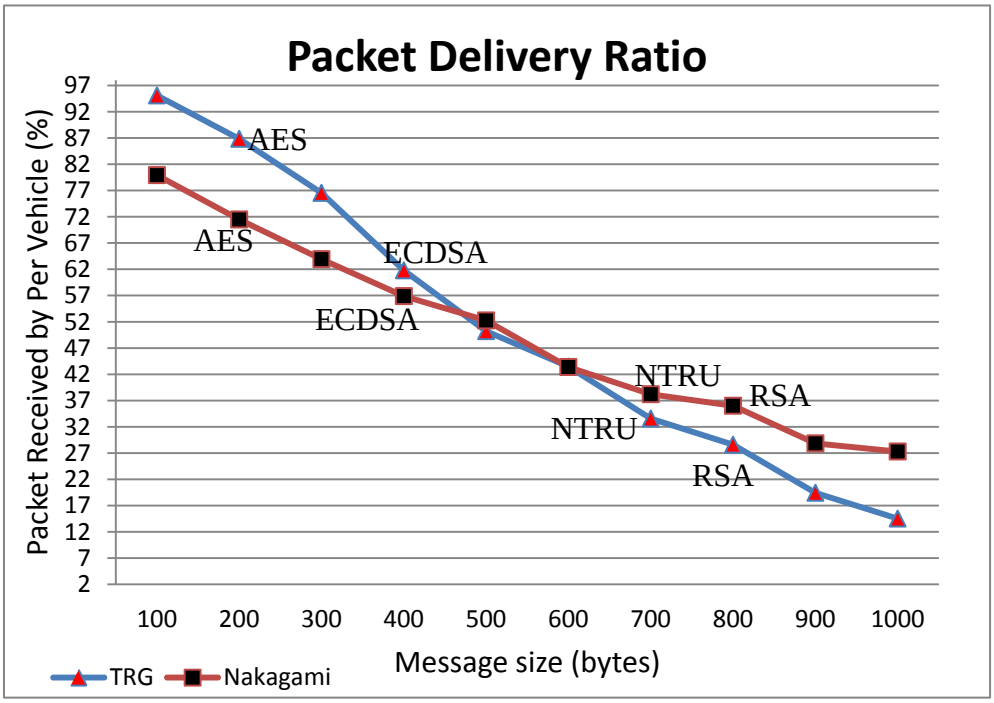

Figure 4.2: Packet Delivery Ratio versus Message Size

Considering the PDR versus increasing distance, the results are also obtained using the TRG and Nakagami models respectively. It is found in both models that the large size distance among vehicles also adversely affects the packet delivery ratio as illustrated in Figure 4.3, and 4.4 respectively. It is observed that the vehicles which are positioned at distance from 150 to 300 meters in Figure 4.3 then the overall results of the RSA and NTRU schemes represent the vehicles packets received ratio is decreased. It is below 10% respectively.

By analyzing the obtained results, it is planned to compute average PDR of vehicles that are positioned at different distances. It is identified that the average PDR of RSA scheme is 2.2% and the PDR of NTRU scheme is 3.5% respectively. Similarly, the average PDR of the ECDSA scheme is 14.5 % PDR and the average PDR of the AES scheme is 37% within the communication range as illustrated in Figure 4.3.

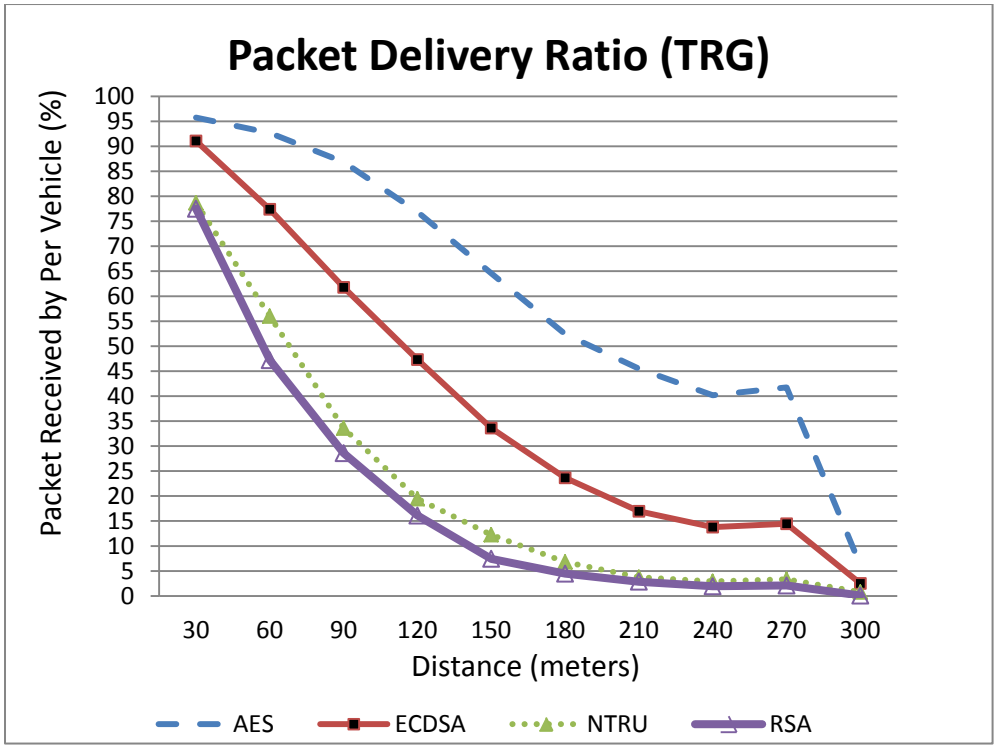

Figure 4.3: Distance versus Packet Delivery Ratio

In order to analyze the PDR at different distances, it is identified PDR is dropped for NTRU and RSU schemes, when the vehicles are positioned at distance of 240 meters and above meters as illustrated in Figure 4.4. It is below 10% that clearly indicates that this distance adversely affects the PDR. In addition, an average PDR is calculated for vehicles that are positioned at distance range from 150 to 300 meters. It is identified that RSA scheme receives 8.2% PDR and the NTRU obtains 9.69% average PDR. Similarly, the ECDSA scheme obtains 22% of average PDR at distance range from 150 to 300 meters. Keeping in view the average PDR using AES scheme, it is identified that AES scheme obtains higher PDR that is 32% at the distances range from 150 to 300 meters as shown in Figure 4.4.

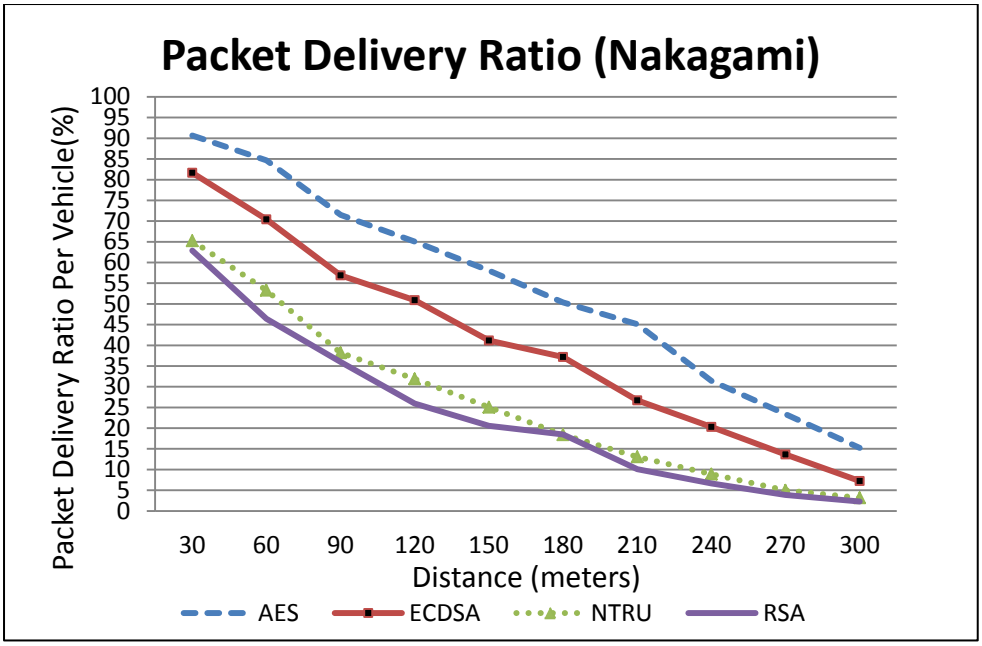

Figure 4.4: Distance versus Packet Delivery Ratio

Since, it is discussed about distance versus PDR, it is identified that as distance is increased then the PDR is decreased. In addition, the PDR of vehicles is also calculated using all schemes at distance of 30 meters. It is identified that all schemes obtain high PDR as shown in Figure 4.3 and 4.4. It ensures that the distance is directly associated with PDR.

4.1.2 End to End Delay (EED)

In order to obtain secure message transmission, end to end delay plays an important role in data communication. Therefore, it has been computed using the four different security schemes key size. This simulation is performed using the TRG and Nakagami model, in which, the message size versus end to end delay is considered. The End to End delay results are shown in Figures 4.5. It is clearly shown that large message size significantly impacts delay in communication.

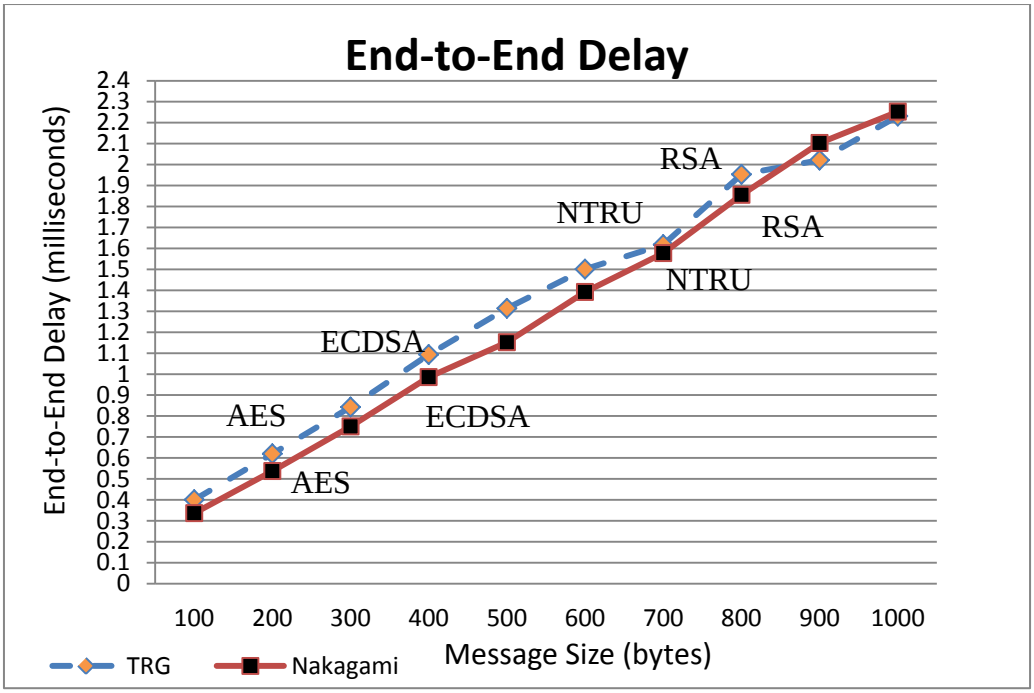

Figure 4.5: End-to-End Delay versus Message Size

In TRG model, it is identified that NTRU and RSA schemes produce highest end-to- end delay during message transmission. The RSA scheme takes 1.95 millisecond ms and the NTRU scheme consume 1.6 ms approximately for the transmission of each message from one vehicle to another. Whereas, ECDSA takes 1.1 ms and the AES takes 0.6 ms respectively.

In the Nakagami model, the RSA scheme takes 1.85 milliseconds ms and NTRU scheme consumes 1.57 ms. The ECDSA takes 0.985 ms for each message transmitted from source to destination vehicle. Whereas, the AES scheme consume 0.53 ms, which is less communication delay than the ECDSA method.

In order to analyze the performance of EED versus distance, it is planned to compute the end-to-delay during message transmission form source to destination vehicles. It is identified that increased distance between the vehicles does not have much effect on small key size schemes in the communication delay as shown in Figure 4.6 and 4.7. In both figures, it is clearly shown that RSA has highest EED as compare to other schemes.

However, it is illustrated in Figure 4.9 that the vehicles which are located at distance of 300 meters consuming less delay due to less PDR. It is identified that the vehicles which are located at distance of less than 300 meters that consumes less delay. The RSA scheme takes 1.9 to 2.4 ms, it is noticed that RSA EED has increased as distance is vary at 240 and 270 RSA getting highest EED. The NTRU scheme drops EED when distance between vehicles are increased, which is opposite then RSA scheme. NTRU scheme consumes 1.9 to 1.8 ms respectively.

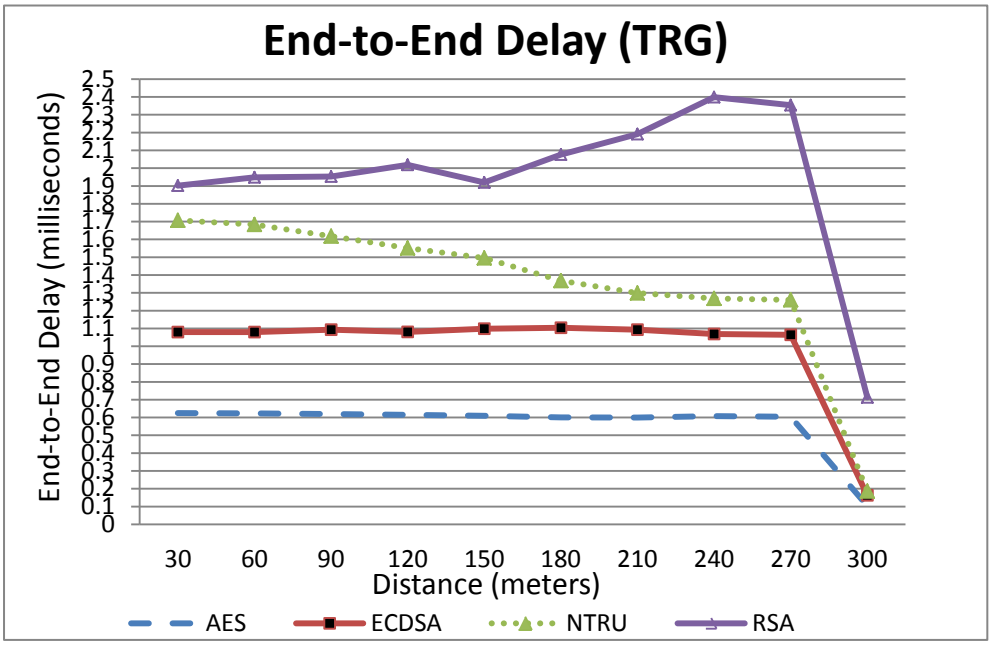

Figure 4.6: Distance versus Communication Delay

Furthermore, the ECDSA scheme consumes 1.1 ms from a vehicle located at distance range from 30 to 270 meters. The AES obtains optimum results throughout the distance range from 30 meters to 270 meters. The AES scheme also takes less delay, i.e. only 0.65 ms for all vehicles that are positioned at distance range from the 30 to 270 meters.

For measuring and analyzing the performance of message transmission, similar schemes are used in the Nakagami model. It is identified that the RSA and NTRU schemes take less EED as compare to TRG model. The RSA scheme fluctuates as distance increased, RSA EED remain between 1.9 to 1.86 ms, and the NTRU scheme EED between 1.6 to 1.5 ms at distance ranges from 30 to 270 meters. Whereas, the ECDSA takes almost 1ms with vary slight variation till 30 to 270 meters. The AES

obtains better results throughout the distance range from 30 to 300 meters. The AES takes 0.54 ms EED which is less than other schemes. Furthermore AES scheme remain stable from 30 to 300 meters distance as illustrated in 4.7.

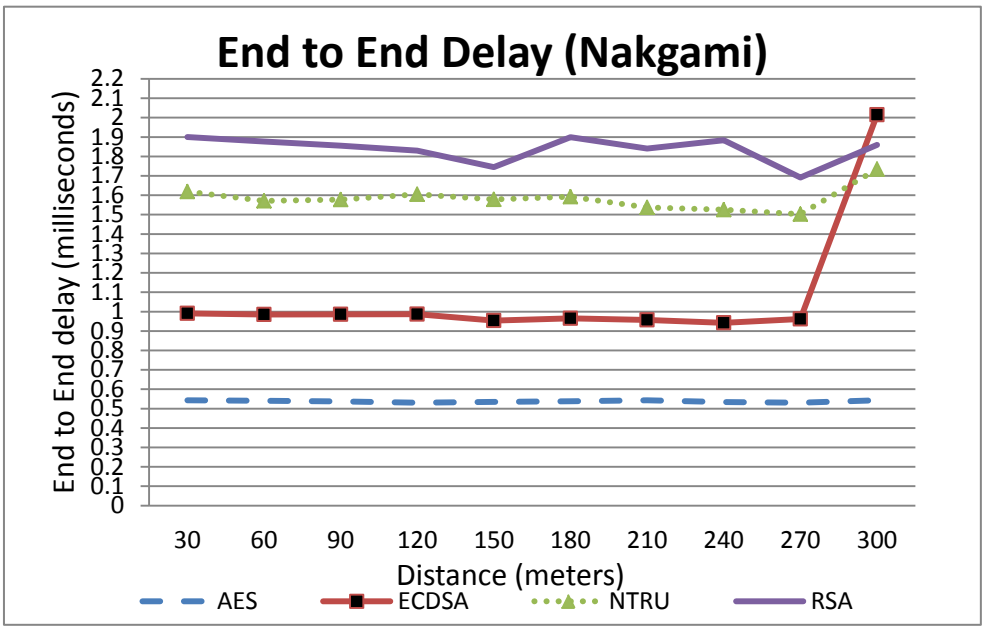

Figure 4.7:Distance versus Communication Delay

4.1.3 Message Drop Count (MDC)

It is found through different studies that the Message Drop Count (MDC) plays a vital role in measuring and analyzing the performance of the message transmission. In this respect, the message size versus MDC is analyzed. In this study MDC convert into fix messages drops during communication, in order to observe the effect of cryptographic schemes. It is identified that the large message size has significant effect on the MDC as illustrated in Figure 4.8. It validates that the ECDSA and AES schemes have small key sizes and these provides an optimum performance as compared to the NTRU and RSA schemes. The RSA technique has large key size therefore; the messages is dropped drastically around 21775 in the TRG model and 12954 in Nakagami model in 20 seconds. However, the NTRU technique also has large key size thus; the message dropped is approximately 21430 in TRG model and 1200 in Nakagami model in 20 seconds.

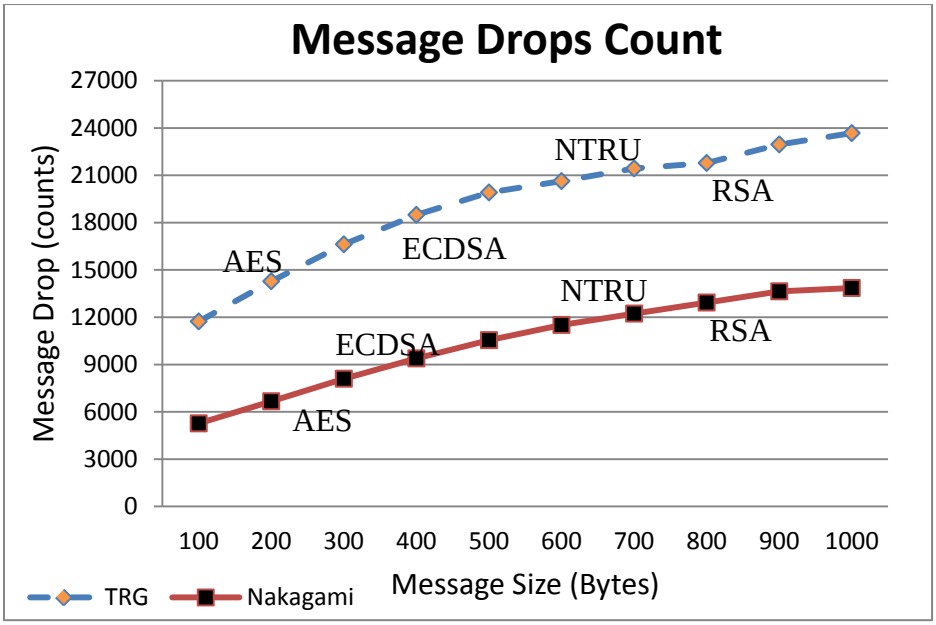

Figure 4.8: Message Drop Count versus Message Size

Pertaining to the MDR for the ECDSA, it is identified that 18488 messages dropped in TRG model and 9384 dropped in Nakagami model in the 20 seconds. The AES obtains the lowest MDR related to other schemes and its MDR is approximately 14280 in the TRG model and 6670 in the Nakagami model.

4.1.4 Processing Delay

In Processing Delay (PD) ECDSA is compared with proposed V2V protocol to estimate differences between these two schemes. It takes place during verification of a message. In order to get the total delay, a verification delay is included to the EED. The verification time is taken from the benchmark as stated in [27]. The ECDSA scheme consumes 8.53 ms for the verification of each message. The Elliptic Curve Diffe-Hellman (ECDH) scheme takes 2.82 ms. Hence, the AES scheme consumes less time during data encryption/decryption process that is approximately 3 (µs) for each message and 61mbytes in a second.

In the highway scenario, 96 vehicles are positioned in the communication range in which vehicles need to verify all received messages in 100 ms before broadcasting a new message. It is identified that the PDR for the ECDSA scheme is 62% in the TRG

model as illustrated in Figure 4.2. It is discussed in the Section 4.1.1 which represents that 52 messages are received by the ECDSA scheme within 100 ms.

Relating to processing delay, following Table 4.2 shows that the ECDSA takes 481.154 ms(0.48 s) in order to receive and authenticate the 50 messages. It is identified that the ECDSA takes 4 times more delay, which does not meet the requirements of the safety applications. Thus, a V2V protocol is proposed that takes 2 ECDSA messages and 1 ECDH message to join the group, verify the credentials and share the SK. After that, the rest of the communication is done by the AES scheme. The AES obtains a higher PDR that is 86%. It means that 80 messages are received in 100 ms. The AES takes 1000 time lesser delay in the decryption of a message as compare to ECDSA. The AES takes 53.4 ms (0.053 s) in receiving and in verifying 50 messages respectively.

Table 4.2: TRG Processing Delay

Schemes	EED (ms)	Verification time (ms)	Total Time (ms)	Msg quantity
ECDSA	1.0930	8.53	9.62	1
ECDSA	54.65	426.5	481.15	50
ECDSA	109.30	853	962.30	100
V2V (ECDSA)	1.0930	8.53	19.2	2
V2V (ECDH)	0.8429	2.82	3.66	1
V2V (AES)	53.37	0.15	53.52	50
V2V (AES)	84.67	0.30	84.97	100

In Nakagami model, the ECDSA scheme obtains 57% PDR as illustrated in Figure 4.2, it means 60 messages are received within 100 ms. The Table 4.3 also shows that the ECDSA takes 475.79 ms (0.47 s) to receive and authenticate 50 messages. The proposed V2V protocol takes 2 ECDSA messagea and 1 ECDH message to join the group, verify the credentials and share the SK then the rest of the communication is done by the AES scheme. The AES gets a higher PDR that is about 64% which means the 78 messages are received in the 100 milliseconds. The AES takes 53.01 ms (0.053 s) to receive and verify the 50 messages. It is observed that the

ECDSA still takes 7 times more processing delay which does not meet the requirements of the safety application. Whereas, the V2V protocol is more suitable for low latency safety application.

Table 4.3: Nakagami Processing Delay

Schemes	EED (ms)	Verification time (ms)	Total Time (ms)	Msg quantity
ECDSA	0.985	8.53	9.51	1
ECDSA	49.29	426.5	475.79	50
ECDSA	98.58	853	951.58	100
V2V (ECDSA)	0.985	8.53	19.2	2
V2V (ECDH)	0.750	2.82	3.57	1
V2V (AES)	49.27	0.15	49.42	50
V2V (AES)	75.77	0.30	76.07	100

Assuming that, if 96 vehicles are in communication range and each vehicle broadcasts a message that is received by all neighboring vehicles. In this worst case situation, approximately 100 messages are need to be verified within 100 ms. In this scenario, the ECDSA takes 962.30 ms (0.96 s) in TRG model and 951.58 ms (0.95 s) in Nakagami model. This outcome clearly suggesting that it does not meet the safety application requirements. However, the AES takes 84.97 ms (0.084 s) in TRG model and 76.07 ms (0.076 s) in Nakagami model and it is acceptable in terms of the safety applications.

4.1.5 Network Throughput

Since, the simulation is conducted in the highway scenario using the different schemes. In which, the average throughput is computed using the TRG and Nakagami model as illustrated in Figure 4.9. It is identified that the large sized schemes such as the RSA and NTRU obtain the highest throughput in both models. The RSA gets 1400 kbps in TRG model and 1670 kbps in Nakagami model respectively. The NTRU gets 1430 Kbps in the TRG model and 1680 kbps in the Nakagami models. The RSA

and NTRU schemes provide a significant MDR but these use large key size. Thus, these schemes consume a lot of bandwidth which minimizes the performance.

However, the ECDSA contains a small key size, and its average throughput is around 1350 kbps in the TRG model and 1410 kbps in the Nakagami model respectively. The AES takes lesser throughout than the ECDSA and provides the optimum results in terms of the PDR. The average throughput of AES is 978 and 910 kbps in the TRG and Nakagami models respectively.

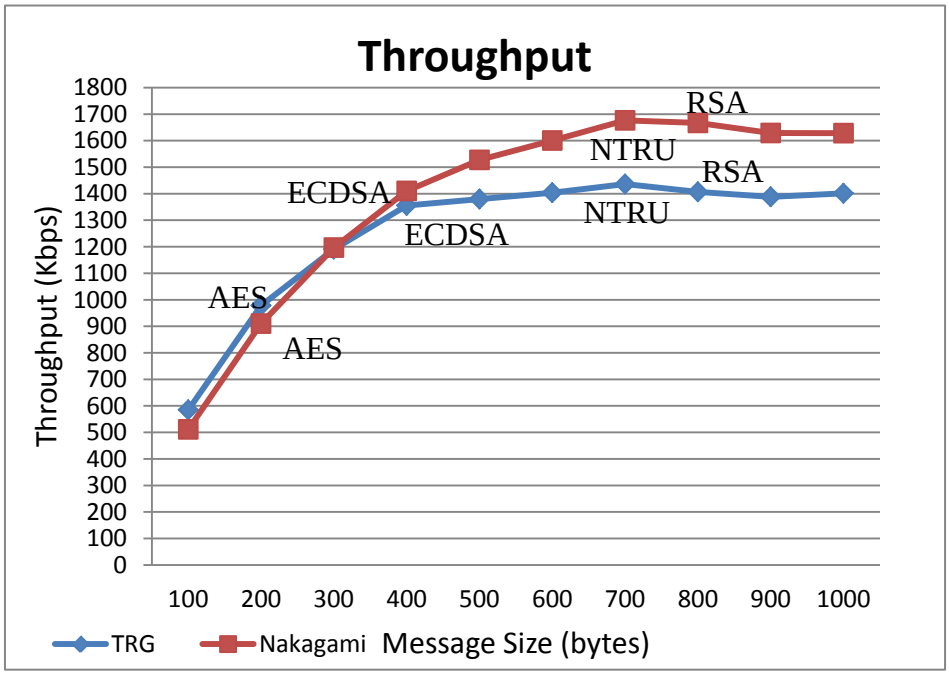

Figure 4.9: Network throughput versus Message Size

4.2 Urban Simulation Setup

Since, the simulation setup is configured and implemented with different parameters for the highway. In which, the performance metrics are analyzed using different security schemes. In the same way, simulation setup is configured and implemented for urban scenario. In which, same parameters with different positions of vehicles are defined. The urban environment is a congested by means of space where vehicles are placed very close to each other as illustrated in Figure 4.10.

Similarly, in this scenario six lanes are defined for the vehicles in which each vehicle is placed at distance of 5 meters. The urban scenario consists of 2160 vehicles in the simulation environment. Every vehicle is configured for broadcasting a message in the 100 ms and the communication range is established up-to 50 meters. Furthermore all results are calculated the average values, the six vehicles taken in simulation scenario as receiving nodes (1 from each lane), the average value of these vehicles considered as a result.

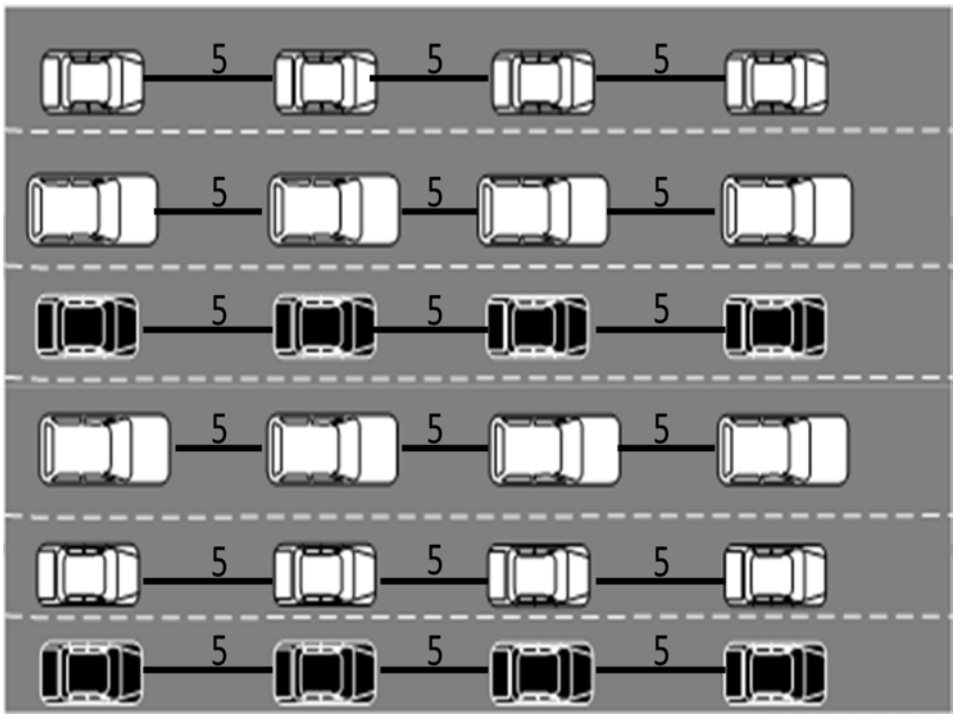

Figure 4.10: Urban Simulation Scenario

The following Table 4.4 defines all the parameters that are used in urban simulation scenario. In addition, the same TRG and Nakagami models are considered for urban simulation.

Table 4.4: Urban Simulation Setting

City Simulation	Simulation Parameters
Total Vehicles No	2160
Simulation time	5 seconds
Lane	6 (three in each direction)
Inner, Middle, Outer lane distance	5 m, 10m, 15 m to 50 m
Message size	100, 200, 300 ……. 1000 bytes
Broadcast interval	100 ms
Interval variance	0.05 ms
Communication Range	50 m
Propagation Model	TRG/Nakagami
Radio System	5.9 GHz DSRC
Bandwidth	6 Mbps

4.2.1 Packet delivery Ratio (PDR)

Since, it is discussed above that the same performance metrics are used for the simulation of urban scenario. In which, the PDR plays a vital role in measuring the performance of message transmission. The PDR is calculated using TRG and Nakagami model as shown in Figure 4.11. It illustrates that message size has direct impact on the packet delivery ratio.

Using the TRG model, it is identified that the RSA and NTRU schemes are fast in verification. However, these schemes get less PDR that is 18.5% and 24% respectively. In addition, the ECDSA and AES schemes have small key size. These schemes obtain 63.3% and 95% PDR which is optimum outcome as compare to other schemes.

In the Nakagami model, results of RSA scheme is very much same as stated in the TRG model and NTRU scheme is 1% less than as in TRG model, but ECDSA and AES scheme get much different in PDR. In Nakagami model, still ECDSA and AES achieve the highest PDR as compare to other schemes. However, it is identified that the TRG model depicts more PDR than the Nakagami model.

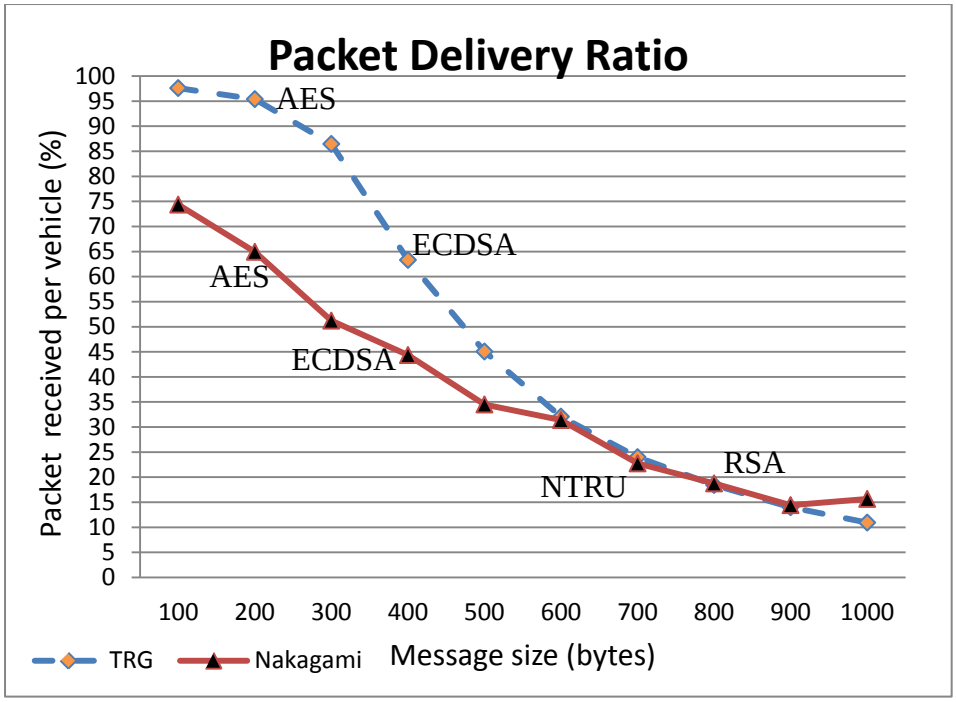

Figure 4.11: Packet Delivery Ratio versus Message Size

In the Nakagami model, the highest PDR could be obtained for the ECDSA scheme that is 44%. Whereas, the AES scheme accomplishes the 64.5% PDR, which leads to optimum performance as illustrated in Figure 4.11.

In order to investigate the PDR versus Distance, in the urban environment, a simulation has been performed using the TRG and Nakagami model. The outcome of simulation suggests that large distance among the vehicles critically affect on the PDR. In Figures 4.12 results of TRG models are shown that determine the impacts of distance on PDR. In TRG model, the RSA and NTRU schemes get the suitable PDR that are 33.7% and 44% at the distance of 5 meter in each vehicle.

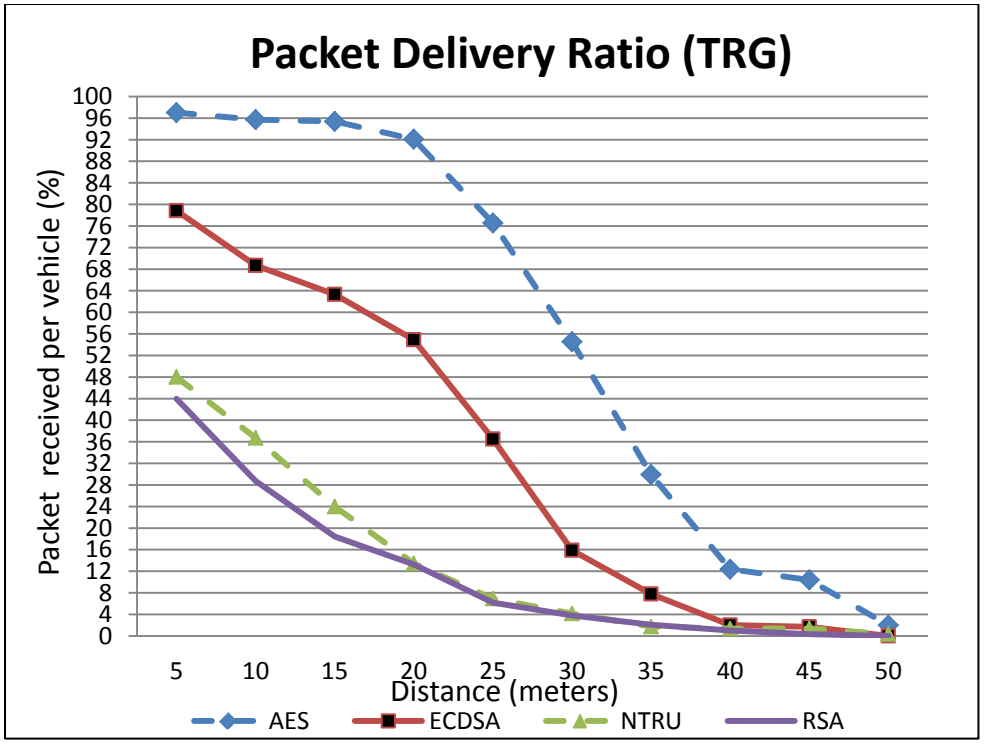

Figure 4.12: Packet Delivery Ratio versus Distance

However, when the distance is 25 meters, it is identified that their PDR is less than 10%. Furthermore the average PDR versus distance from 25 to 50 meters for RSA and NTRU are 1.4% and 1.79% which is ever less. Where ECDSA scheme also not obtaining suitable average PDR, that is 5.4% however it is still much better than RSA and NTRU schemes. In contrast to this AES scheme getting optimum PDR, the average PDR of distance from 25 to 50 is 21.8%. In addition, the AES accomplishes suitable PDR from 5 to 40 meters distance. When distance is increased 40 meters than PDR is degraded, i.e. 10% approximately.

In addition, the simulation is performed using the Nakagami model for the investigation PDR versus distances. In this model, it is identified that the NTRU and RSA security schemes obtain 54% and 46% at distance of 5 meters respectively. It is observed that, this PDR is bit increased as compare to the PDR that is obtained in the TRG model as illustrated in Figure 4.13. Furthermore the average PDR versus distance from 25 to 50 meters for both RSA and NTRU schemes dropped PDR drastically that are 0.33% and 0.86% respectively. That is even less than TRG model

average PDR. Then the PDR is dropped drastically that are 0.86% and 0.33% respectively. After that, when the vehicles are placed at the distance of 30 meters for

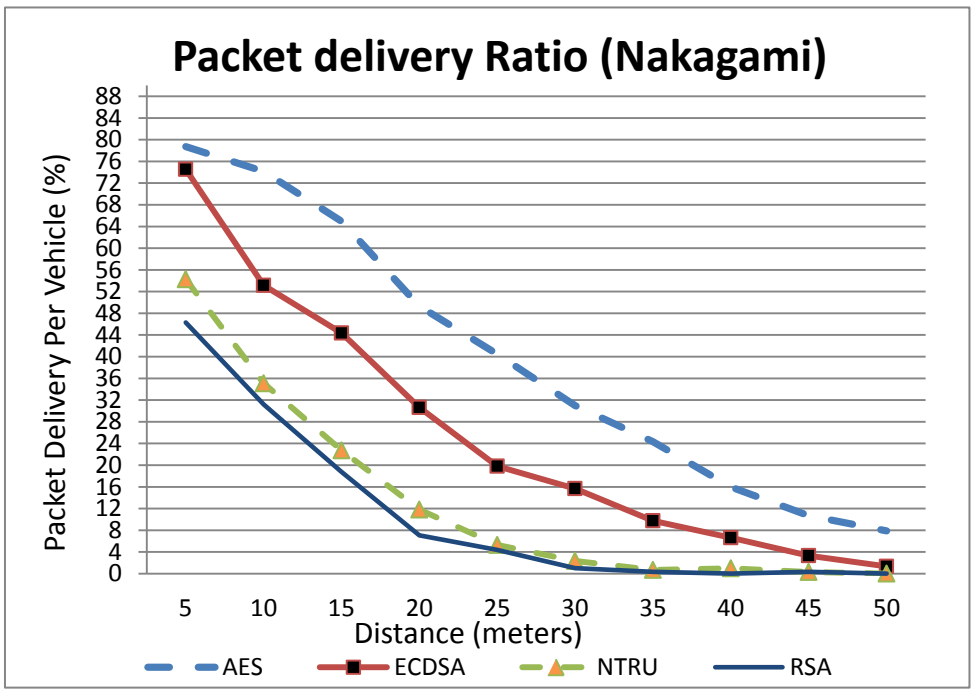

Figure 4.13: Packet Delivery Ratio versus Distance

Considering the 5 meter distance of vehicle, the ECDSA and AES schemes are used for measuring the PDR versus distance. It is identified that ECDSA and AES schemes achieve 74% and 79% PDR for nearby vehicles, as comparing models TRG getting much better result for these schemes. Since, the average PDR from 25 to 50 meters distance for ECDSA and AES schemes provide 7.32% and 18% PDR respectively. It represents much better PDR than RSA and NTRU schemes in the Nakagami model. Hence, the AES security scheme is still obtaining much better results than the rest of schemes.

4.2.2 End-to-End Delay (EED)

In order to identify the end-to-end delay, a simulation is undertaken using TRG and Nakagami models for urban scenario. It is identified that large message size and traffic jam in limited space highly affect on end-to-end delay. Considering the case of the TRG model, it is discovered that there is higher delay in communication due to

large key size of NTRU and RSA security schemes. It is found that the NTRU takes 23.4 ms and the RSA gets 22.5 ms which means the EED in the TRG model is reasonably high. In contrast to NTRU and RSA scheme, it is identified that the ECDSA scheme takes 8.2 ms, whereas the AES scheme only consumes 1.6 ms. It is clearly representing that ECDSA and AES consume minimum time in message transmission. In particular, the performance of AES is better than the rest of security schemes in the case of the TRG model as shown in Figure 4.14.

Keeping in view the importance of end-to-delay in the message transmission, a simulation is undertaken for identifying EED using the Nakagami model. It is found that the delay is increased when communication takes place among the vehicles in a congested environment.

It is observed that the congested environment and traffic jams also have effect on end-to-end delay as compare to highway during the message transmission. In addition, it is discovered that security schemes, i.e. ECDSA and AES have small message size (range from 100 to 500 bytes) that provide the less delay in the communication, i.e. 3.1 ms and 1.0 ms. However, the schemes NTRU and RSA have large message size (range 700 bytes to above) that produces a higher delay, i.e. 31.5 ms and 91 ms respectively. The results of the Nakagami model are illustrated in Figure 4.14.

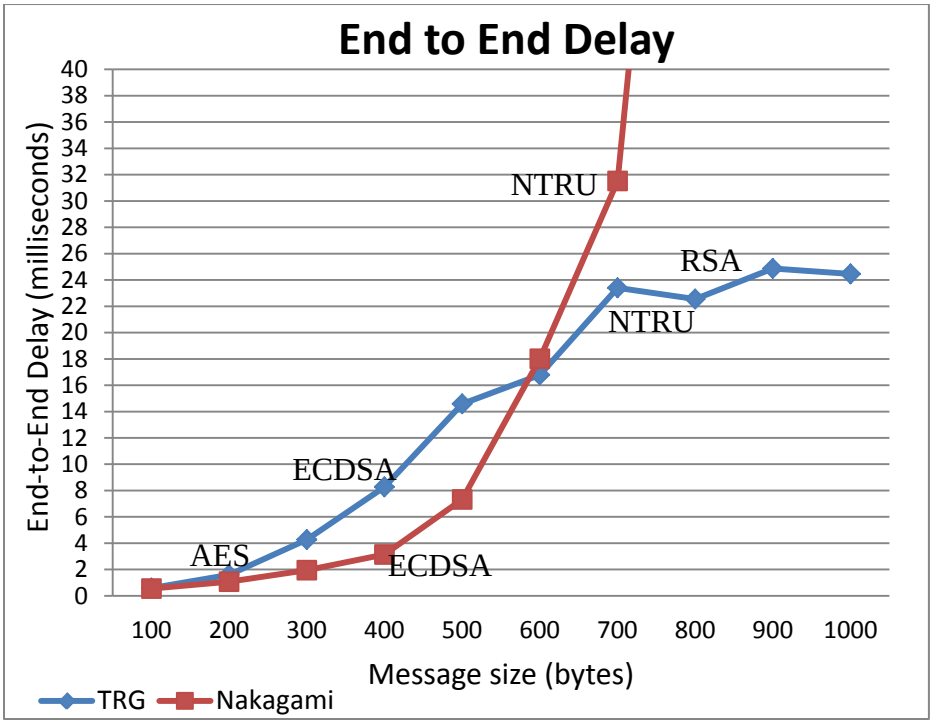

Figure 4.14: End to End Delay versus Message Size

Relating to the importance of the end-to-end delay in the message transmission, it is computed through considering the different distances in an urban environment using the TRG model. The Figure 4.15 shows the obtained results. It represents that the NTRU and RSU security schemes still provide the unsuitable results. The NTRU scheme consumes 22.11 ms and RSA scheme uses 25 ms during the transmission a message among the vehicles at the distance of 5 meters. It is discovered that the end-to-end delay decreases as distance is increased within the communication range. It is also observed that due to large number of messages collision decreases the EED at particular distance.In TRG model, it is discovered that ECDSA and AES security schemes consume less delay that is 8.8 ms and 1.6 ms respectively at the distance of 5 meters.

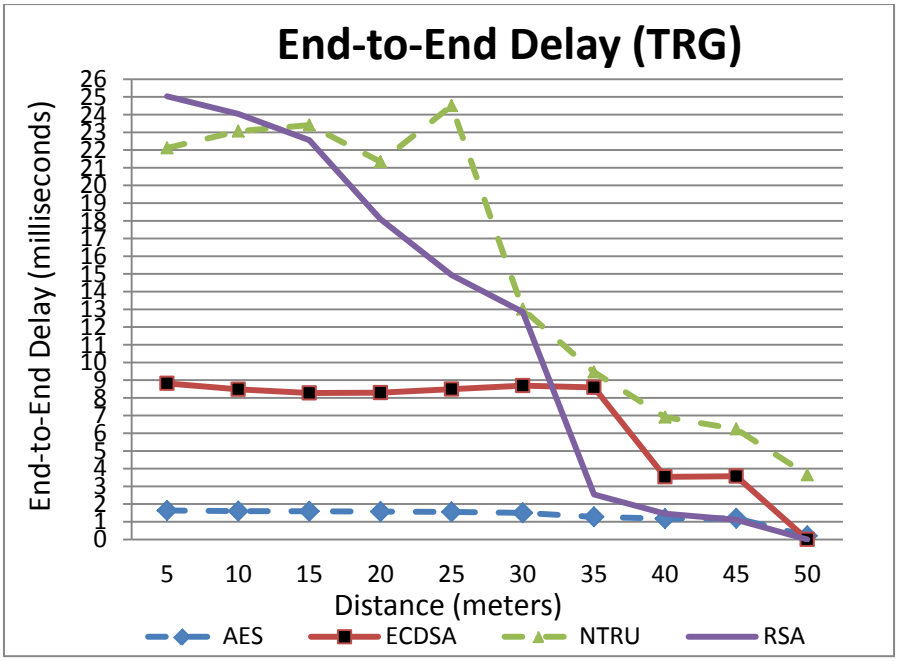

Figure 4.15: End to End Delay versus Distance

In order to measure end-to-end delay versus distance, a Nakagami model is used in the urban simulation scenario. In this simulation, similar security schemes are considered and their results are illustrated in Figure 4.16. It is found that the NTRU and RSA scheme take higher delays due to the congested environment in urban areas. The EED of these schemes are significantly increased when each message is transmitted by the vehicles in a communication range. The NTRU takes 29.2 milliseconds and the RSA consumes 93.8 milliseconds respectively. Furthermore, it is noticed that the vehicles which are located at distance of 40 and 50 meters then they do not receive any messages because of the collision as shown in Figure 4.16. However, in the TRG model, it was observed that a very small number of messages are received at the same distance as managed in the Nakagami model.

The AES and ECDSA schemes consume very less delay as compare to NTRU and RSA schemes. The ECDSA takes 3.3 ms whereas AES acquire 1 ms for each packet during communication. In both schemes, EED is nearly same for the vehicles located at distance of 5 meters but not for those vehicles which are located at distance of 50 meters. It is due to large number of messages collision during communication.

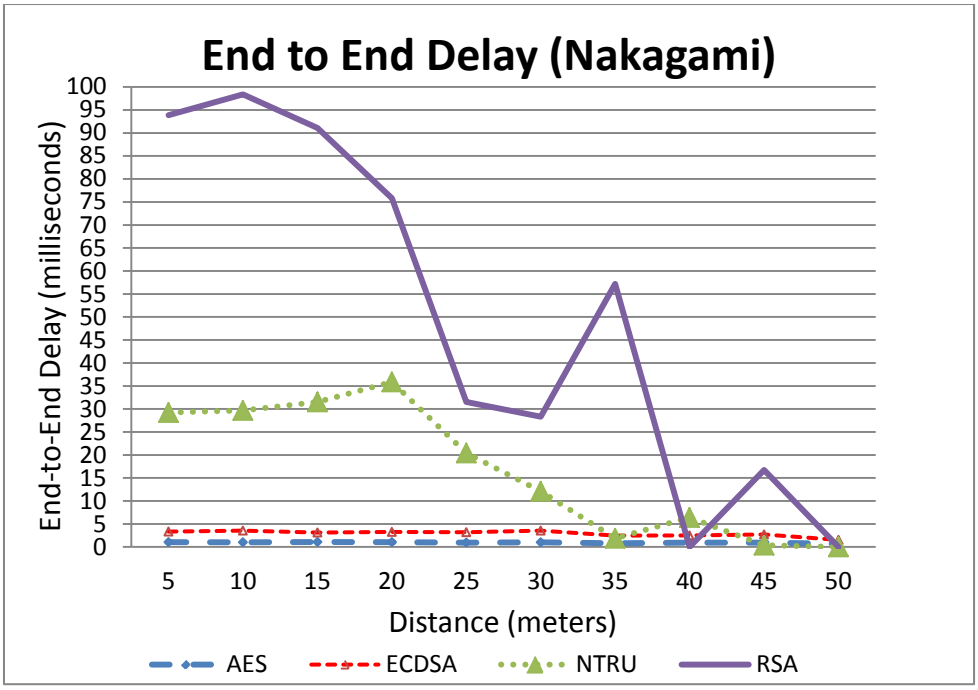

Figure 4.16: End to End Delay versus Distance

4.2.3 Message Drop Count (MDC)

Message Drop Ratio (MDC) plays an important role in the message transmission in urban communication. In this respect, a simulation is undertaken to compute the MDC using the TRG and Nakagami model. In these models, the four different schemes have been used to measure the MDC and their results are shown in Figure 4.17. It was observed that as message size is increased then MDC is increased respectively from 100 to 1000 bytes. It was found that the large key size schemes that are based on NTRU and RSA still accomplish the higher MDC.

In TRG model, the NTRU scheme drops 7366 messages and RSA scheme drops 7495 message approximately. These schemes drop 6531 and 6451 messages during communication using the Nakagami model. In addition, it is observed that NTRU and RSA schemes consume more bandwidth and it produces the message collision.

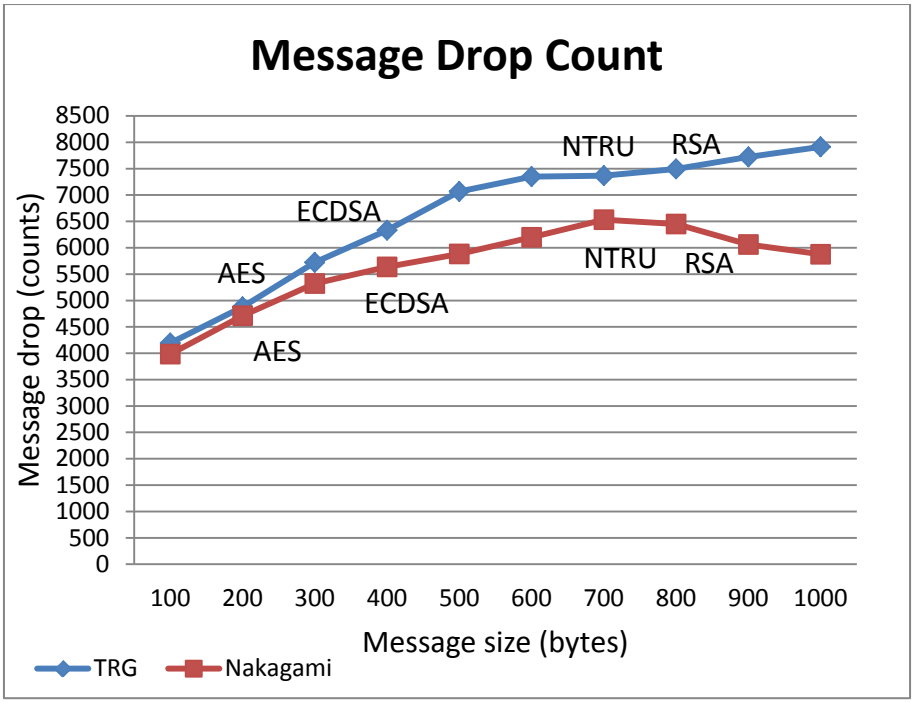

Figure 4.17: Message Drop Count versus Message Size

The ECDSA and AES schemes in the TRG model drop 6722 and 4877 messages respectively at the communication time. Whereas, in Nakagami model, these schemes drop the 5322 and 4711 messages. It is found that the congested situation among the vehicle all four schemes have significant MDC. In addition, the security schemes which have small key size (e.g. ECDSA and AES) perform much better in the both models.

4.2.4 Processing Delay (PD)

Keeping in view the importance of processing delay, it is computed using the TRG and Nakagami models. In which, the two different security schemes are used. The processing delay is the total delay between two vehicles communication. The PD includes the verification delay into the EED. The verification time is taken from the benchmark a as stated in [27]. The ECDSA consumes 8.53 ms for the verification of each message transmitted among the vehicles. The Elliptic Curve Diffe-Hellman (ECDH) takes 2.82 ms. At the other hand, the AES scheme takes much less time for encryption/decryption of each message, i.e. about 3 (µs) and also encrypt/decrypt

61mbytes data in one second [50]. As urban scenario is different from the highway scenario in which 120 vehicles are in the transmission range. This situation suggests that it is a very congested scenario for obtaining the appropriate urban communication. Considering this reason, the vehicles get a higher PDR and introduce higher delay during message transmission. In the TRG model, suppose that ECDSA receives 76 messages within 100 ms while the AES receives 114 messages within 100 ms respectively as shown in Figure 4.11. It has been represented in Figure 4.14 that the EED is increased 3 times more as compared to the highway scenario.

The ECDSA scheme uses 16.80 ms for one message that is received and verified during communication. It is found that, when numbers of messages are increased up to 50 then PD is increased significantly as shown in Table 4.5. Using the ECDSA, processing delay is 840 ms and it is considered as higher delay according to VANET requirements. Thus, it is not suitable for the many safety applications.

Table 4.5: TRG Processing Delay

Schemes	EED (ms)	Verification time (ms)	Total Time (ms)	Msg quantity
ECDSA	8.27	8.53	16.80	1
ECDSA	413.58	426.5	840.08	50
ECDSA	827.16	853	1680.16	100
V2V (ECDSA)	8.27	8.53	33.6	2
V2V (ECDH)	4.26	2.82	7.087	1
V2V (AES)	80	0.15	120.83	50
V2V (AES)	160	0.30	200.1	100

Regarding the performance of V2V protocol, it is identified that the V2V takes 120.83 ms (0.12 s) during the receiving and verifying the 50 messages in a communication range. In addition, one message is handover to SK, in which undertaken time is included as given in Table 4.5. However, the obtained processing delay using the AES scheme is not satisfactory according to the safety application requirements. It is identified that this delay is 7 time less as compare to ECDSA. It is identified that, when 100 messages are verified using the ECDSA scheme, it uses approximately 1680 ms (1.68 s). In addition, the AES scheme takes only 200.1 ms

(0.2 s). From this computation, it is discovered that ECDSA scheme still takes much more delay.

In the case of the Nakagami model, suppose that the ECDSA scheme receives 53 messages and AES scheme obtain 78 messages in 100 ms during communication among vehicles, the received messages results are interpreted according PDR as shown in Figure 4.11. It is discovered that the EED is obtained less using the Nakagami model than the TRG model for both schemes (ECDSA and AES). The ECDSA takes 9.51 ms for each message that is quite less than the TRG model.

However, when 50 messages are verified in 100 ms then it noticed that ECDSA delay 583.65 ms (0.58 s) as given in Table 4.6. It is not considered as suitable for safety applications. The AES scheme obtains much better results in the case of the Nakagami model when 50 messages are received and verified. The AES takes 72.74 ms (0.07 s) which is an acceptable delay for the safety applications. However, the AES also consumes 123 ms PD when the number of messages is increased from 50 to 100. The AES scheme still gets much less time as compare to the ECDSA scheme and it is about 10 times less as given in Table 4.6.

Table 4.6: Nakagami Processing Delay

Schemes	EED (ms)	Verification time (ms)	Total Time (ms)	Msg quantity
ECDSA	3.14	8.53	9.51	1
ECDSA	157.15	426.5	583.65	50
ECDSA	314.31	853	1167.31	100
V2V (ECDSA)	3.14	8.53	19.2	2
V2V (ECDH)	1.95	2.82	3.570	1
V2V (AES)	50	0.15	72.74	50
V2V (AES)	100	0.30	123	100

4.2.5 Network Throughput

Since, it is studied that identification of the network throughput during the message transmission among the vehicles is very important in both highway and urban

simulation scenarios. It is computed using both Nakagami and TRG model as illustrated in Figure 4.18. It is identified that the average throughput of messages within the simulation is 100 to 1000 bytes. In addition, it is noticed that the small packet size schemes get higher throughput. The ECDSA has the highest throughput as compared to other schemes. The AES and ECDSA schemes are getting messages in large number due to small packet size. There is also low collision among the messages during transmission. It is clearly suggesting that the small packet size schemes successfully receive a large quantity of packets.

However, the large packet size schemes produce low throughput due to high collision of packets during communication. It is noticed the packet delivery ratio for the NTRU and RSU schemes lacks in receiving the messages of more than 5% of the overall broadcasted messages as illustrated in Figure 4.11.

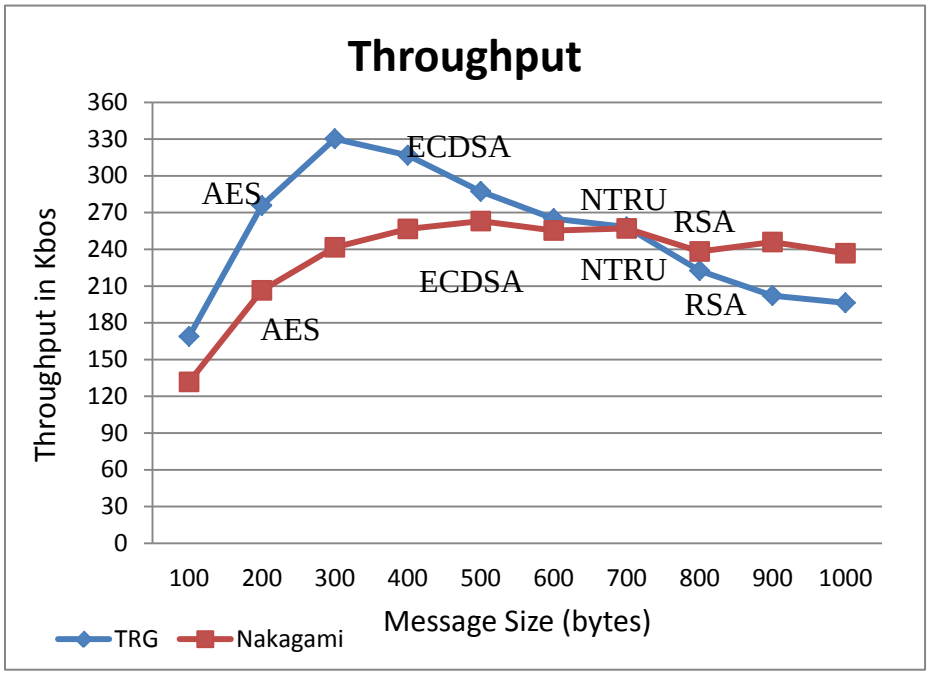

Figure 4.18: Network Throughput

In the case of TRG model, the throughput of AES and ECDSA are much better as compare to other schemes. The results of the Nakagami model are stable almost for every scheme.

4.3 Backend Results Analysis

The V2V protocol is implemented in AVISPA to analysis the results of protocol. AVISPA tool runs HLPLS script to check possible attacks on V2V protocol and security goals, that are mutual strong authentication between vehicle group leader, message integrity, and secrecy of data. The results are analyzed in two backends i.e OFMC and CL-AtSe.

The mutual authentication is a process which provides guarantee that both vehicles (group Leader and Vehicle A) recognize each other and that they are communicating with the desirable vehicle. In V2V protocol mutual authentication takes place by following statements.

V → GL; Snd(Pka.A.{Pka.A}_inv(Pks).

Na'.Nb'.B.ctext3.{Na'.Nb'.B.ctxt2}_inv(Pka))

/\ witness(A,B,na,Na')

Group Leader verifies all credentials of vehicle A, after verification group leader also send credential in same manner as above statements are described. For details please refer to Appendix A.

The message integrity is a procedure in which information is converted in a cipher text so that only legitimate vehicle can read that cipher text. The V2V protocol also maintains message integrity property during message transactions described in following statements. The privacy is a process that secures the credential of owner so that original details of owner can to be delivered to any unauthorized users. V2V protocol uses an anonymous certificate to achieve privacy. In HLPSL code is described as secrecy, as it is defined below that the information secrecy put in V2V protocol.

V → GL : /\ Snd(Pka.A.{Pka.A}_inv(Pks).

Na'.Nb'.B.H(ctext3).{Na'.Nb'.B.ctxt2}_inv(Pka))

V → GL secret (Sk',nanb,{A,B}).

In the Figure 4.19 the intruder role is defined in proposed V2V protocol. The intruder cannot directly attacks against valid vehicle; however, attacker can join the group if it contains valid key and certificate. The attacker can generate messages and send on the network, also can receive the messages. Thus, the proposed V2V protocol scope is the massage should be unaltered and keep the user privacy. V2V protocol obtained results shows that the security goals are accomplished and that the V2V protocol is safe, there is no attack found for the specified goals.

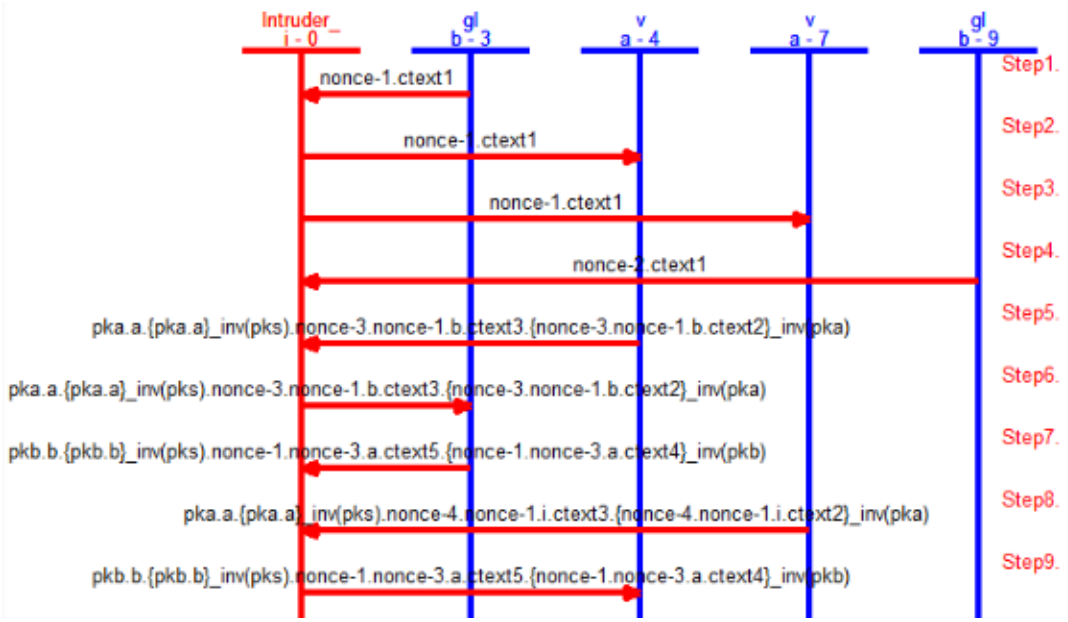

Figure 4.19: Intruder Simulation

The OFMC uses symbolic techniques and carry outs protocol fabrication and bounded verification by investigates the limited number of sessions. In addition OFMC utilizes the requirement of algebraic functions of cryptographic operators. The results of OFMC are in Table 4.7, the first line summarizes (SAFE), which means that no attack has been found in V2V protocol. (BOUNDED NUMBER OF SESSIONS) it means limited session visited and security goals (as specified) it means particular security goal are achieved as it defined. The CL-AtSe technique defines some simple redundancy rules that easily interpreted and run. The basic techniques to execute possibly number of sessions to find the attacks or else protocol consider secure if

attack is not found. The CL-AtSe results are shown in Table 4.7 there is no attack which has been found in proposed V2V protocol.

Table 4.7: Backend Results

OFMC	CL-Atse
SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL C:\Program Files\SPAN\testsuite\results\v2v protocol.if GOAL As_specified BACKEND OFMC STATISTICS parseTime: 0.00s searchTime: 2.82s visitedNodes: 1299 nodes depth: 10 plies	SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS TYPED_MODEL PROTOCOL C:\Program Files\SPAN\testsuite\results\v2vprotocol.if GOAL As specified BACKEND CL-AtSe STATISTICS Analysed : 213 states Reachable : 134 states Translation: 0.03 seconds Computation: 0.01 seconds

4.4 Summary

In the first part of this chapter, the four different schemes have been considered for addressing the latency issues. It supported in obtaining the results using different security schemes and considering the various performance parameters.

The results have been obtained using both TRG and Nakagami propagation models and their results are discussed extensively. It is reported in the results that the large key size schemes take higher delay and receive less PDR. The AES and ECDSA schemes have small key size and the performance of these schemes is much better in terms of the EED and PDR. However, the AES scheme is more suitable as compare to all other schemes. The performance of AES and ECDSA schemes can be differentiated in the processing delay. Whereas, the AES only takes few microseconds

and the ECDSA requires few millisecond. The AES is 1000 times faster than the ECDSA scheme which suggests that the AES is suitable for safety applications.

The second part of this chapter, V2V protocol is analyzed in the two different model checkers to get results using different techniques. In addition, an attacker model is used to check the possible attack on the protocol where an attacker is aware of the communication. However, an attacker cannot be involved unless if it has a valid set of keys. This leads the protocol to achieve security goals, i.e. mutual strong authentication and secrecy of data. By obtaining this goal, vehicles can build trust between surrounding vehicles. It also ensures that no one can join the group until and unless vehicle has validate key pair.

CHAPTER 5

CONCLUSION AND FUTURE WORK

In this chapter, it is attempted to conclude this study in the context of the problem statement, research questions, and objectives. This chapter summarizes an overall outcome of the whole study into three main sections, i.e. achievements, contribution, limitations, and future work. These are section are described as follows.

5.1 Achievements

In order to achieve the objectives of this study, a rigor and relevant literature of the VANET technologies have been reviewed. It is identified that the VANET technology is become a well established technology for handling variety of applications in a real environment. However, the VANET technology is inherited with many challenging issues, in which, specifically a time delay in message verification is one of the most critical issue. It has been addressed through a new proposed security framework.

In this study, a security framework has been proposed in which trusted platform module and vehicle grouping scheme are combined accordingly. This framework consists of two types of cryptographic modules, asymmetric and symmetric, that assists in achieving the secure and fast communication as per the requirement of a safety applications. Two communication protocols have been proposed that help in authenticating the credential, as well as the platform. In addition, a vehicle grouping scheme has been proposed that support in selecting a group leader by dividing roads into cells and segments in efficient way. This vehicle grouping scheme is also used to achieve a fast authentication for newly entering vehicles in the cell.

In order to ensure the functionality and performance of the proposed framework, a basic VANET (IEEE 802.11p) configuration is setup and simulated using NS2. The

simulation has been performed in two scenarios, i.e. highway and urban. The simulation results showed that the proposed framework satisfy the requirements for safety applications. It performs substantially well in terms of some performance parameters; particularly for its end-to-end delay and processing delay.

5.2 Contribution

This study contributes toward the knowledge of VANET technology, particularly in security domain. This study proposed a framework to provide solution of problem statement/research questions. There are five main contributions, which are highlighted as below.

a) The proposed framework is a combination of trusted platform module and vehicle grouping scheme, which assists in satisfying the requirement of low latency safety applications in VANET technology.

b) This study contributes in achieving the secure and fast communication for the safety application using the both asymmetric and symmetric cryptographic methods.

c) This study contributes in building the trusted among group of vehicles using vehicle to vehicle protocol. The V2V protocol provides a mutual authentication mechanism to build trust.

d) In addition, a new vehicle grouping scheme is designed for proposed framework that help in reducing the extra burden from the group leader and provides a fast way to join group for new vehicles.

e) This study compares four cryptographic scheme message sizes to analyzing the proposed framework and its functional scheme through simulation under 802.11p in the domain of the highway and urban scenarios.

5.3 Future Directions

- The proposed framework lacks in implementation of TPM chip as only software simulation has been performed in this study to measure its performance. Therefore, a research study can be conducted to implement the proposed framework with TPM chip.

- After that, another study can be conducted to verify and validate the results of hardware and software based solutions in a real case scenario implementation.

REFERENCES

[1] H. Moustafa, S. M. Senouci, and M. Jerbi, “Introduction to Vehicular Networks,” *Zhang, Yan (Hrsg.) Vehicular networks: Techniques, Standards and Applications. Boca Raton, FL, USA: Auerbach Publications*, pp. 1-20, 2009.

[2] R. Subramanian, “Traffic safety facts,” *Stroke*, vol. 5, pp. 1-687.

[3] 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*, 2005, pp. 11-21.

[4] S. Olariu and M. A. C. Weigle, *Vehicular networks: from theory to practice*, vol. 20. Chapman & Hall/CRC, 2009.

[5] M. Torrent-Moreno, P. Santi, and H. Hartenstein, “Fair sharing of bandwidth in VANETs,” in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005, pp. 49-58.

[6] A. Carter, “The status of vehicle-to-vehicle communication as a means of improving crash prevention performance,” *National Highway Traffic Safety Administration, USA, Tech. Rep*, pp. 5-264.

[7] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, “Design of 5.9 GHz DSRC-based vehicular safety communication,” *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 36-43, 2006.

[8] “IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,” *IEEE Std 1609.2-2006*, pp. 01 -105, 2006.

[9] “IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager,” *IEEE Std 1609.4-2006*, pp. 1 -63, 2006.

[10] H. Hartenstein and K. Laberteaux, *VANET Vehicular Applications and Inter-Networking Technologies*. Wiley Online Library, 2009.

[11] G. Guette and C. Bryce, “Using TPMs to secure vehicular ad-hoc networks (VANETs),” *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, pp. 106-116, 2008.

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

[13] J. Douceur, “The sybil attack,” *Peer-to-peer Systems*, pp. 251-260, 2002.

[14] J. P. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” *Security & Privacy, IEEE*, vol. 2, no. 3, pp. 49-55, 2004.

[15] M. Raya, P. Papadimitratos, and J. P. Hubaux, “Securing vehicular communications,” *Wireless Communications, IEEE*, vol. 13, no. 5, pp. 8-15, 2006.

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

[17] X. Lin, X. Sun, X. Wang, C. Zhang, P. H. Ho, and X. Shen, “TSVC: Timed efficient and secure vehicular communications with privacy preserving,” *Wireless Communications, IEEE Transactions on*, vol. 7, no. 12, pp. 4987-4998, 2008.

[18] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *infocom 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1229-1237.

[19] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005, pp. 1-6.

[20] C. L. Robinson, L. Caminiti, D. Caveney, and K. Laberteaux, “Efficient coordination and transmission of data for cooperative vehicular safety applications,” in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, 2006, pp. 10-19.

[21] H. Hartenstein and K. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164-171, 2008.

[22] A. Studer, F. Bai, B. Bellur, and A. Perrig, “Flexible, extensible, and efficient VANET authentication,” in *Proceedings of the 6th Annual Conference on Embedded Security in Cars (escar 2008)*, 2008.

[23] C. Zhang, X. Lin, R. Lu, and P. H. Ho, “RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks,” in *Communications, 2008. ICC’08. IEEE International Conference on*, 2008, pp. 1451-1457.

[24] TCG Published, “Trusted Computing Group, Trusted Platform Module Main Specification, Part 1: Design Principles, Part 2: TPM Structures, Part 3: Commands.”

[25] P. U. B. FIPS, “186-2. Digital signature standard (DSS),” *National Institute of Standards and Technology (NIST)*, 2000.

[26] Certicom Research, “SECG, ‘Elliptic Curve Cryptography’,” 2000.

[27] “Crypto++5.6.0Benchmarks.”[Online].Available: http://www.cryptopp.com/benchmarks.html. [Accessed: 20-Oct-2011].

[28] R. L. Rivest, A. Shamir, and L. Adleman, “A method of obtaining digital signatures and public-key cryptosystems, Communication,” *Assoc. Comput. Mach*, vol. 21, pp. 120-126, 1978.

[29] 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*, 2006, pp. 94-95.

[30] 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.

[31] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” in *Proceedings of the 11th ACM conference on Computer and communications security*, 2004, pp. 168-177.

[32] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in *Advances in Cryptology--CRYPTO 2004*, 2004, pp. 227-242.

[33] D. L. Chaum, “Blind signature systems.” Google Patents, 1988.

[34] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “The TESLA broadcast authentication protocol,” *RSA CryptoBytes*, vol. 5, no. 2, pp. 2-13, 2002.

[35] 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*, 2006, pp. 67-75.

[36] Y. C. Hu and K. P. Laberteaux, “Strong VANET security on a budget,” in *Proceedings of the 4th Annual Conference on Embedded Security in Cars (escar 2006)*, 2006.

[37] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in VANET,” in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, 2007, pp. 19-28.

[38] C. Tchepnda, H. Moustafa, H. Labiod, and G. Bourdon, “A Layer-2 Multi-hop Authentication and Credential Delivery Scheme for Vehicular Networks,” in

Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, 2008, vol. 51, no. 1, pp. 1-6.

[39] H. J. Reumerman, M. Roggero, and M. Ruffini, "The application-based clustering concept and requirements for intervehicle networks," *Communications Magazine, IEEE*, vol. 43, no. 4, pp. 108-113, 2005.

[40] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, 2007, pp. 422-432.

[41] M. Verma and D. Huang, "SeGCom: secure group communication in VANETs," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, 2009, pp. 1-5.

[42] O. Gaddour, A. Koubaa, and M. Abid, "SeGCom: A secure group communication mechanism in cluster-tree wireless sensor networks," in *Communications and Networking, 2009. ComNet 2009. First International Conference on*, pp. 1-7.

[43] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 4, pp. 1606-1617, 2010.

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

[45] Y. Park, C. Sur, C. D. Jung, and K. H. Rhee, "Efficient Anonymous Authentication Protocol for Secure Vehicular Communications," *Journal of Information Science and Engineering*, vol. 26, no. 3, pp. 785-800, 2010.

[46] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 6, pp. 3357-3368, 2008.

[47] J. Santa, R. Toledo-Moreo, and A. F. Gomez-Skarmeta, "A novel vehicle communication paradigm based on Cellular Networks for improving the safety in roads," *International Journal of Intelligent Information and Database Systems*, vol. 2, no. 2, pp. 240-257, 2008.

[48] H. Moustafa, G. Bourdon, and Y. Gourhant, "AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture," in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005, pp. 79-80.

[49] D. Simon, B. Aboba, and R. Hurst, “The EAP-TLS authentication protocol,” in *RFC 5216, IETF*, 2008.

[50] S. Yuan, C. Zhang, and P. H. Ho, “A secure business framework for file purchasing in vehicular networks,” *Security and Communication Networks*, vol. 1, no. 3, pp. 259-268, 2008.

[51] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinm, “Secure and efficient beaconing for vehicular networks,” in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, 2008, pp. 82-83.

[52] E. Schoch, B. Bako, S. Dietzel, and F. Kargl, “Dependable and secure geocast in vehicular networks,” in *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, 2010, pp. 61-68.

[53] 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*, 2004, pp. 259-268.

[54] C. Piro, C. Shields, and B. N. Levine, “Detecting the sybil attack in mobile ad hoc networks,” in *Securecomm and Workshops, 2006*, 2006, pp. 1-11.

[55] 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*, 2006, pp. 1-8.

[56] S. Brands and D. Chaum, “Distance-bounding protocols,” in *Advances in Cryptology—EUROCRYPT’93*, 1994, pp. 344-359.

[57] G. Guette and O. Heen, “A TPM-based architecture for improved security and anonymity in vehicular ad hoc networks,” in *Vehicular Networking Conference (VNC), 2009 IEEE*, pp. 1-7.

[58] C. Y. Yeun, M. Al-Qutayri, and F. Al-Hawi, “Efficient Security Implementation for Emerging VANETS,” *Ubiquitous Computing and Communication Journal 30 Oct. 2009*, vol. 4.

[59] B. Li, J. Wang, T. Dong, and Y. H. Liu, “An new approach to access VANETs,” in *Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on*, vol. 2, pp. 482-485.

[60] X. Zhang, M. Zhou, J. X. Zhuang, and J. Li, “Implementation of ECC-Based Trusted Platform Module,” in *Machine Learning and Cybernetics, 2007 International Conference on*, vol. 4, pp. 2168-2173.

[61] J. Krasner, “Using elliptic curve cryptography (ECC) for enhanced embedded security,” *Embedded Market Forecasters, American Technology*, 2004.

[62] M. Strasser, “A software-based TPM emulator for Linux,” *Department of Computer Science. Swiss Federal Institute of Technology Zurich*, 2004.

[63] H. Zhang, Z. Qin, and Q. Yang, “Design and Implementation of the TPM Chip J3210,” in *Third Asia-Pacific Trusted Infrastructure Technologies Conference*, 2008, pp. 72-78.

[64] C. V. S. C. Consortium and others, “Vehicle safety communications project: Task 3 final report: Identify intelligent vehicle safety applications enabled by DSRC,” *National Highway Traffic Safety Administration, US Department of Transportation, Washington DC*, 2005.

[65] C. V. S. C. Consortium and others, “Vehicle safety communications project task 3 final report, Mar. 2005,” *Online: http://www. intellidriveusa. org/documents/vehicle-safety.pdf*.

[66] V. Namboodiri and L. Gao, “Prediction-based routing for vehicular ad hoc networks,” *Vehicular Technology, IEEE Transactions on*, vol. 56, no. 4, pp. 2332-2345, 2007.

[67] “The AVISPA backends.” [Online]. Available: http://www.avispa-project.org/.

[68] The AVISPA team, “HLPSL Tutorial A Beginner’s Guide to Modelling and Analysing Internet Security Protocols IST-2001-39252 Version: 1.1 June 30, 2006.”

[69] K. Ramana, A. Chari, and N. Kasiviswanth, “A survey on trust management for mobile ad hoc networks,” *International Journal of Network Security & Its Applications*.

[70] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein, “Overhaul of IEEE 802.11 modeling and simulation in ns2,” in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, 2007, pp. 159-168.

[71] Q. Chen, D. Jiang, V. Taliwal, and L. Delgrossi, “IEEE 802.11 based vehicular communication simulation design for NS-2,” in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, 2006, pp. 50-56.

[72] A. Khan, S. Sadhu, and M. Yeleswarapu, “A comparative analysis of DSRC and 802.11 over Vehicular Ad hoc Networks,” *Project Report, Department of Computer Science, University of Californai, Santa Barbara*, 2009.

[73] “Network Simulator 2 (NS2).” [Online]. Available: www.isi.edu/nsnam/ns/. [Accessed: 10-Oct-2011].

LIST OF PUBLICATIONS

1. **A. A. Wagan**, B. Munir Mughal, and H. Hasbullah, "**VANET Security Framework for Safety Applications Using Trusted Hardware**," in *Digital Information Processing and Communications*, vol. 189, V. Snasel, J. Platos, and E. El-Qawasmeh, Eds. Springer Berlin Heidelberg, 2011, pp. 426-439.

2. **A. A. Wagan**, B. M. Mughal, and H. Hasbullah, "**VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination**," in *International Symposium on Information Technology (ITSim), in*, 2010, *vol. 2, pp. 607-611*.

3. **A. A. Wagan**, B. M. Mughal, and H. Hasbullah, "**VANET Security Framework for Trusted Grouping Using TPM Hardware**," in *2010 Second International Conference on Communication Software and Networks*, 2010, pp. 309-312.

4. B. M. Mughal, **A. A. Wagan**, and H. Hasbullah, "**Impact of Safety Beacons on the Performance of Vehicular Ad Hoc Networks**," *Software Engineering and Computer Systems*, pp. 368-383, 2011.

5. .B. M. Mughal, **A. A. Wagan**, H. Hasbullah, B. Munir Mughal, A. Ali Wagan, and H. Hasbullah, "**Efficient congestion control in VANET for safety messaging**," in *International Symposium on Information Technology (ITSim), in*, 2010, vol. 2, pp. 654-659.

6. B. M. Mughal, **A. A. Wagan,** and H. Hasbullah, "**Analyzing safety beacon loss rate in VANETs with two-ray ground and Nakagami propagation models**," in *National Postgraduate Conference (NPC)*,2011, pp. 1-6.

APPENDIX A

VEHICLE-TO-VEHICLE PROTOCOL

```
role gl( A,B: agent,
         Pkb,Pks,Pkv: public_key,
         Snd,Rec: channel(dy))
played_by B
def=

 local  State      : nat,
        Pka        : public_key,
        Nb,Sk      : text,
        Na,Txt2,Txt3: text

 const ctxt1,ctxt4,ctxt5: text

 init State := 0

 transition

  1. State = 0
     /\ Rec(start)
     =|>
     State' := 1
     /\ Nb' := new()
     /\ Snd(Nb'.ctxt1)
     /\ witness(B,A,nb,Nb')

  2. State = 1
     /\ Rec(Pka'.A.{Pka'.A}_inv(Pks).Na'.Nb.B.H(Txt3)'.
          {Na'.Nb.B.Txt2'}_inv(Pka'))
     =|>
     State' := 2
     /\ Snd(Pkb.B.{Pkb.B}_inv(Pks).Nb.Na'.A.ctxt5.{Nb.Na'.A.ctxt4}_inv(Pkb))

     /\ request(B,A,na,Na')

3. State = 2
/\ Rec({Sk'}_Pkv)=|>
   State' := 3

end role

role v ( B,A: agent,
         Pka,Pks,Pkv: public_key,
         Snd,Rec: channel(dy))
played_by A
def=

 local  State       : nat,
        Pkb         : public_key,
        Na,Sk       : text,
        Nb,Txt1,Txt4,Txt5: text

 const ctxt2,ctxt3: text

 init State := 0
 transition

  1. State = 0
     /\ Rec(Nb'.Text1')
```

```
    =|>
    State' := 1
    /\ Na' := new()
    /\ Snd(Pka.A.{Pka.A}_inv(Pks).
          Na'.Nb'.B.H(ctext3).{Na'.Nb'.B.ctxt2}_inv(Pka))
    /\ witness(A,B,na,Na')

  2. State = 1
    /\ Rec(Pkb'.B.{Pkb'.B}_inv(Pks).
          Nb.Na.A.Txt5'.{Nb.Na.A.Txt4'}_inv(Pkb'))
    =|>
    State':= 2
    /\ Sk' := new()
    /\ Snd({Sk'}_Pkv)
    /\ secret (Sk',nanb,{A,B})
    /\ request(A,B,nb,Nb)

end role

role session (A,B:agent,
            Pka,Pkb,Pks,Pkv: public_key) def=

 local SA,RA,SB,RB: channel (dy)

 composition

        gl(A,B,Pkb,Pks,Pkv,SA,RA)
     /\ v(B,A,Pka,Pks,Pkv,SB,RB)

end role

role environment() def=

 const na, nb, nanb       : protocol_id,
       sk                 :text,
       a, b, i            : agent,
       pka, pkb, pks, pki,pkv : public_key

 intruder_knowledge={a,b,pki,pkv,sk,inv(pki),pks,
                     ctxt1,ctxt4,ctxt5,{pki.i}_inv(pks),
                     ctxt2,ctxt3,{pki.i}_inv(pks)}

 composition

       session(a,b,pka,pkb,pks,pkv)
    /\ session(a,i,pka,pki,pks,pkv)
    /\ session(i,b,pki,pkb,pks,pkv)

end role

goal
   secrecy_of nanb
   V authentication_on nb
   GL authentication_on na

end goal

environment()
```