Efficient and Secure Message Transfer in VANET

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

Master of Engineering

in

Information Security

Submitted By

Rajeev Singh

(Roll No. 801433021)

Under the supervision of:

Mr. Sumit Miglani

Assistant Professor

Thapar University, Patiala

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2016

Certificate

I hereby certify that the work which is being presented in the thesis entitled, "*Efficient and Secure Message Transfer in VANET*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Mr. Sumit Miglani* and refers other researcher's work which are duly listed in the reference section.

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

(Rajeev Singh)

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

(Mr. Sumit Miglani)
Assistant Professor.
Computer Science and Engineering Department

Countersigned by

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

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

Abstract

Wireless medium shows a key role from past few years in the world of communication. Mobile Adhoc Network (MANET) is an important field of wireless communication. Vehicular Adhoc Network (VANET) is a new area of MANET in which a car acts as node communicator with rest of the cars and road side infrastructure in the network. Security is a major issue in VANET as it provides safety as well as non safety application to the users. Varied work has already been done by researchers for the security in VANET but securing the message communication between cars still poses an issue. From this paper, we introduce a model which provides a secure communication between cars. In our model, RSUs acts as a Certificate Authority (CA) which will generate the key using Elliptic Curve Cryptography (ECC) for the cars and after that communication between cars takes place using Elliptic Curve Diffie Hellman (ECDH).

Acknowledgement

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life. It is a great privilege to express my gratitude and admiration towards my respected supervisor **Mr. Sumit Miglani,** Assistant Professor, Computer Science & Engineering Department, Thapar University, Patiala. He has been an esteemed guide and great support behind achieving this task. This work would not have been possible without the encouragement and able guidance of him. I also thank my supervisor for his time, patience, discussions and valuable comments. His enthusiasm and optimism made this experience both rewarding and enjoyable. I am truly grateful to him for extending his total co-operation and understanding whenever I needed help and guidance from him. I am also heartily thankful to **Dr. Deepak Garg**, Associate Professor and Head, Computer Science & Engineering Department and **Dr. Jhilik Bhattacharya**, PG coordinator, for motivation and providing uncanny guidance and support throughout the preparation of the thesis report.

I will be failing in my duty if I do not express my gratitude to **Dr. S. S. Bhatia**, Senior Professor and Dean of Academic Affairs, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable. Last but not least, I would like to thank my family for their wonderful love and encouragement, without their blessings none of this would have been possible.

Rajeev Singh

(**801433021)**

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background

Population in the world increases in a rapid way from day to day. So, depend on the need, the demand of human being increases and transport facility is one of those demands. Due to demand of transport facility, there is increase in number of vehicles, by which huge volume of traffic is on the road and large increase in number of road accidents. Each year about 1.4 million persons killed in the road accidents [1]. Now a days, there is a demand of decrease the traffic and also decrease the road accidents. So, in the traffic management road traffic safety is a major issue.

One solution is that if we give the traffic information to the vehicles, so that they can use the data to analyses the traffic environment. For analysis of traffic environment, information they needed can be achieved by exchanging the information among vehicles. Due to high mobility of vehicles, all vehicles are mobile in nature, so there is a requirement of mobile network which are infrastructure less and self organized. With the advancement in microelectronics, we can create a wireless adhoc network in which we integrate the nodes and the network devices into a single unit. Further this wireless adhoc network evolved as Mobile Adhoc Network.

1.2 Mobile Adhoc Network (MANET)

A MANET is compromised of a group of mobile nodes which is deployed without infrastructure support and which have capability of self organization in a decentralized fashion [2]. In MANET, nodes are mobile in nature which communicates over relatively bandwidth and network topology changes in a rapid way. It is a wireless adhoc network which consists of self forming, peer-to-peer, self-healing network and has routable networking environment that work on top of link layer. The decentralized network of MANET includes delivery of messages and discovering of network topology that executed by nodes itself.

MANET applications are diverse in nature which ranges from small to large scale, with static and dynamic networks. One of application is that it is used as collection of sensor

data for data mining for example air pollution monitoring. There are four ways in which MANET are further divided like adhoc network for vehicle communication, adhoc network for smart phones, mobile adhoc network based on internet that associate mobile nodes and established Internet gateway nodes, adhoc network used for Military purposes like security, range and integration with existing systems.

1.3 Vehicular adhoc network

Vehicular Adhoc Networks (VANETs) is a new technology in which researchers from worldwide shows a great interest. It is a new area of mobile adhoc network that have the capability of self-making of network in a decentralized fashion with infrastructure less plan [3]. In VANET the communicating nodes form a network to improve the safety for driver and manage the internet access by drivers and programmers. As shown in Figure 1.1 there are mainly two communicating nodes, one is infrastructure equipment is also known as Road Side Unit (RSU) or Access Point Unit (APU) and the second one is vehicles. The vehicles are mobile nodes while RSU are immobile nodes that are stationary which connected to internet for transferring of messages and also used for providing geographical location of vehicles.

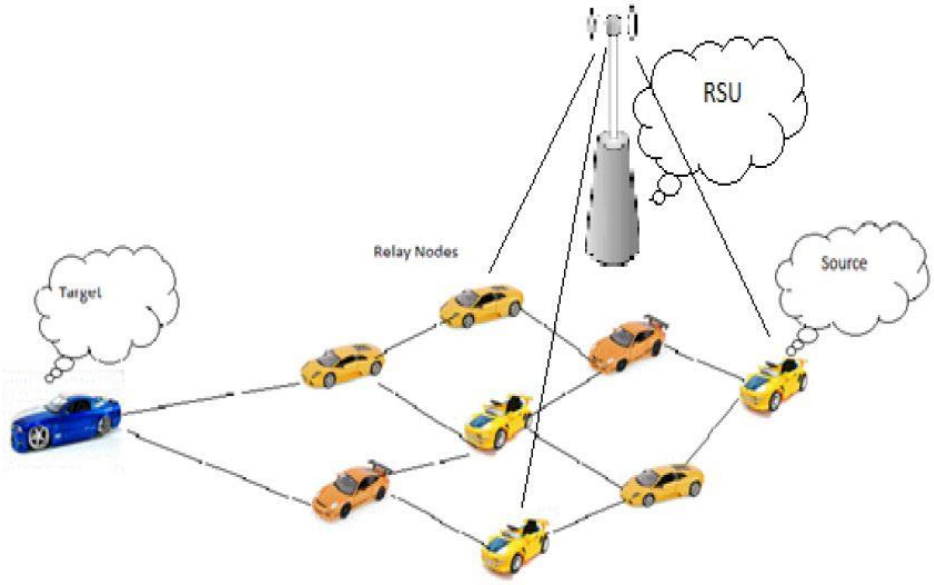


Figure 1.1 Scenarios of General VANETs

There are mainly three types of communication available in VANET one is inter vehicle communication that is V2V communication, second is V2R that is vehicle to roadside communication and last is R2R that is inter road side communication as shown in Figure 1.2. VANETs play an important role in the Intelligent Transportation Systems (ITS) in which each vehicle communicates to other vehicle or RSU by sending or receiving the message with help of transceiver assembled in each vehicle known as On-board Unit (OBU) [4].

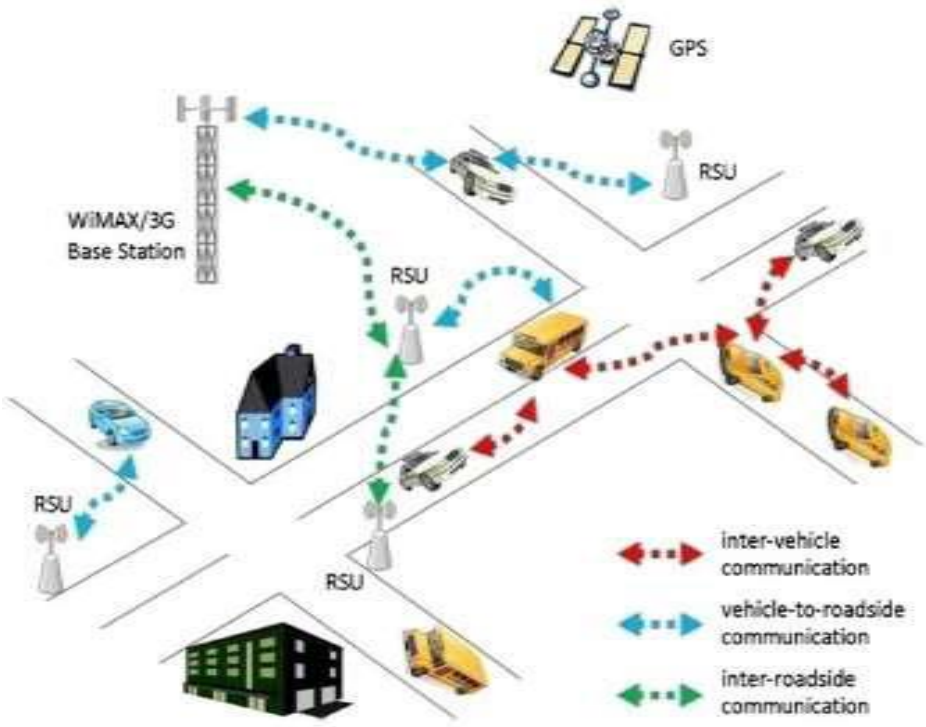


Figure 1.2 Type of VANET

With the increment in advance of communication protocols and decrease in price of hardware available, on the road accident increases day by day, so there is lot of pressure from the society to the automobile companies to enhancing their work on road safety and also for providing various types of application for upgrading the technology for example satellite based navigation system like GPS are integrated in vehicles.

The applications of VANET include security warning about distance, vehicular collision detection, planned driving, location tracking, and relaying information about the road, automatic parking and access to internet. As VANET is new area of MANET, so various properties of VANET is similar to MANET are radio transmission used by vehicles and self-organizing capacity of vehicular nodes. The high mobility of vehicular nodes and very fast speed of nodes are properties of VANET which do not resemble with MANET, so the routing protocols are different for both MANET and VANET. The difference between the MANET and VANET are shown in Table 1.1. Due to fast speed of vehicles in VANET, we have to upgrade the routing protocols of MANET to be used in VANET. The vast application of VANET and its features attracted the worldwide attention of education institutes, government, industry and researchers for developing the user friendly and security related applications of VANET.

Table 1.1 Comparisons of VANET and MANET

Main characteristics	**VANET**	**MANET**
Movability	High speed	Average Speed
Network topology	installation remains on the bearing of the road route	Normal deployment
Model for communication	V2V and V2R	Peer to peer
Route direction	Into the driving direction	Any direction
Connected ranges and nodes	Many nodes and large scale	Few nodes and small scale
Resource constraints	Unlimited computation power and ability	Limited computation power and ability
Area of application	Traffic safety, traffic control, electronic tolls etc.	Emergency, military and civil environment etc.

1.4 Intelligent Transport System (ITS)

It is a non specific term which characterizes the methods practiced in transportation frameworks to oversee traffic adequately in all methods of transportation, i.e., water, street, air and rail. ITS arrangements with the system required for both intra and between mode transmissions of essential data between vehicles, which expands the level of movement security, upgrades productivity of vehicles and lowering the ill-effects upon environment, which straightforwardly cuts cash spent on upkeep of vehicles, streets and expense of fuel [4].

Intra-mode transmission implies stream of data between vehicles going in same method of transportation, as roadways to roadways or aviation routes to aviation routes and so on. While Inter- mode transmission implies stream of data between various methods of transportation, e.g. roadways to aviation routes, roadways to railroads, aviation routes to conduits, and so forth.

ITS handles telemetry and correspondence which can either be vehicle to-vehicle correspondence or vehicle to-some altered framework. In ITS, each vehicular node works about as a receiver, sender or switch at various time to show a message to different vehicles in the system or to some centralized office of transportation whose obligation is to guarantee bother free and safe stream of traffic. For the correspondence between the vehicles or between a vehicle and RSU, which is altered on either side of street, there must be a radio handset coordinated in the vehicles, which can empower vehicular hubs to make a short range remote adhoc system. Differential worldwide situating Framework (DGPS) and Worldwide Situating Framework (GPS) should likewise be fitted in the vehicles for determination of position of vehicles as shown is Figure 1.3.

At present for the development of ITS, the project which are running into the world are:

- Continuous Air Interface Medium and Long range (CAML) : It is taking a shot at the communication of RSUs with the vehicles by utilizing diverse sorts of media utilized for communication like cellular connections, infra red connections and some dedicated remote connections. Its applications incorporate security of

vehicles and drivers, stream of data amongst vehicles and applications identified with the live entertainment for travelers and drivers.

- Dedicated Short-Range Communication (DSRC): DSRC works for the communication between nodes like vehicle and some fixed location on roads like restaurant or toll booths for the electronic fee collection and prepaid parking facility [4].

- Association for Intelligent Transportation System (AITS) of India is a nonprofit company whose aim is to save time, money, live and nature is combined with a million dollar project from 2001 for the development of ITS for cities in India with the foreign help. Industries and researchers from institutes have combined their hands with government of India to work for the project on the basis of regulation and rules formed by government with a vision for making the India with safest and most appropriate transport network.

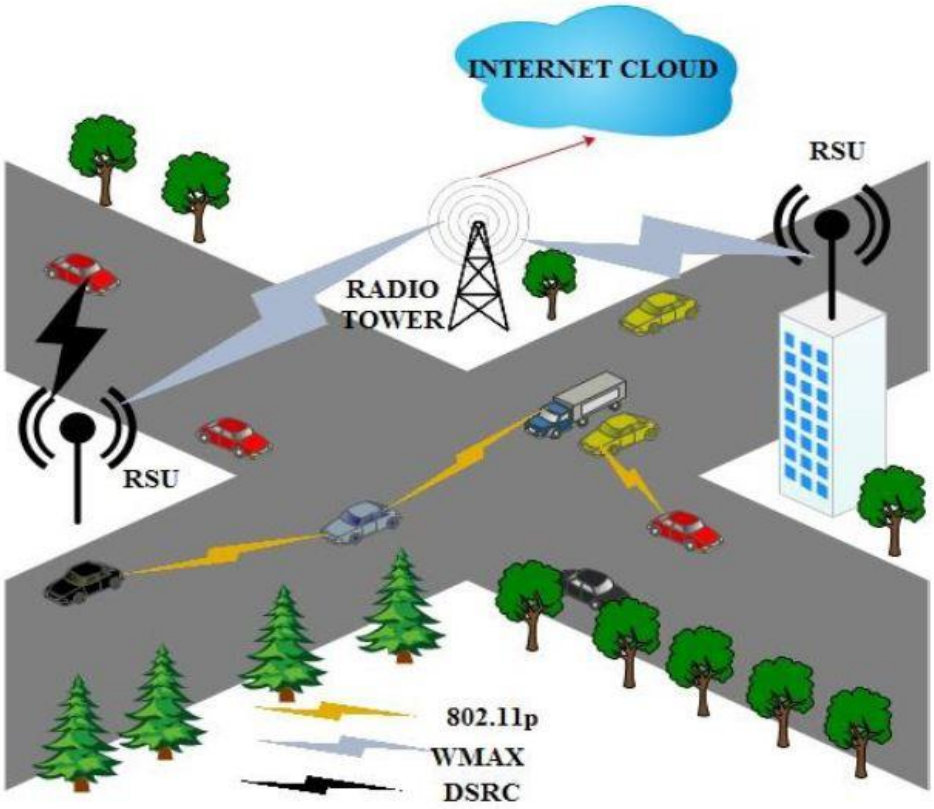


Figure 1.3 Scenarios of ITS

RSUs must be legitimately arranged to encourage the correspondence. The number, course of action and appropriation of RSU vigorously relies on upon the sort of road and convention utilized, e.g. necessity of a portion of the conventions is to distribute the RSUs equitably all through the entire road, while some require RSUs to be available on border of the transmission area and others require RSUs to be available just at the purpose of convergences.

1.5 VANET Model Overview

For the deployment and settlement, VANET contains various entities but Majority of entities are mobile nodes that are vehicles and remaining entities contains road side infrastructure which are also used for doing the basic task of network. For understanding the model of VANET is shown if Figure 1.4. We divide the network entities in two main environments. As shown in Figure 1.5 one is Infrastructure environment and other is Adhoc environment. In Infrastructure environment, entities are interconnected with each other permanently. It mainly made up of those entities which provide external services and manage the traffic.

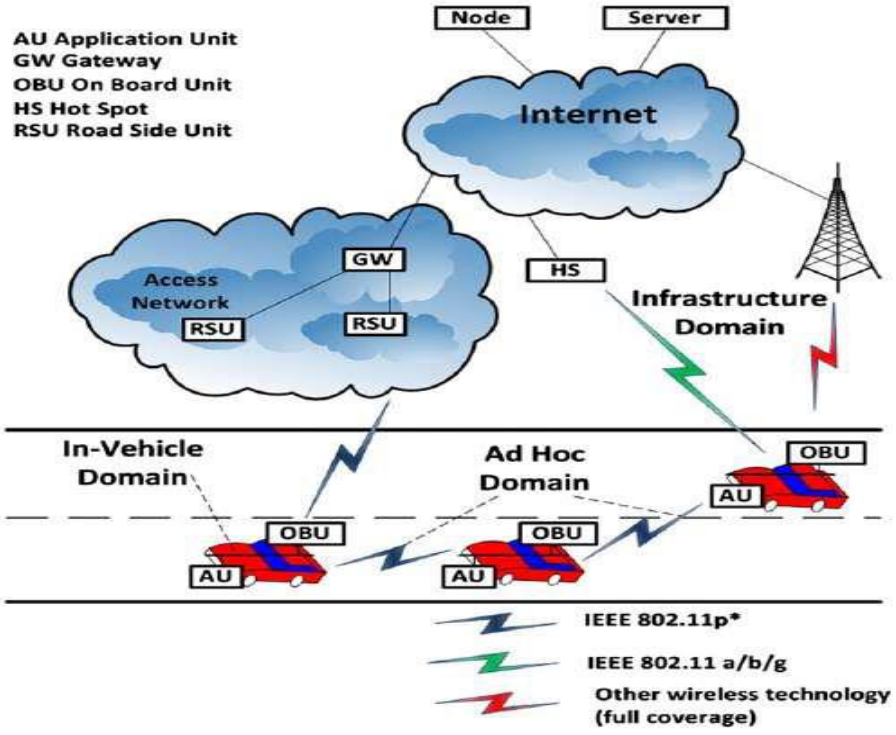


Figure 1.4 VANET model overview

The main entities are Manufacturer, Trusted Third Party (TTP), Service Provider and Legal Authority, in which RSU and are directly connected to TTP. Manufacturers are basically the manufacturing company of vehicle which gives unique identification to each vehicle. Legal Authority is used for providing registration of vehicles and reporting of offences. It is used as a regulatory body of VANET in which each vehicle should be registered and proof of registration is that each vehicle should have a license plate. It is also used for providing traffic reports and fine to vehicles that break the rules. TTP are also the important part of this environment as it provide services like time stamping and other credential management. Both authority and manufacturers connected to the TTPs because they need the services of both like providing electronic credentials. Now Service Provider provides the services which are access through VANET like Digital Video Broadcasting (DVB) [5].

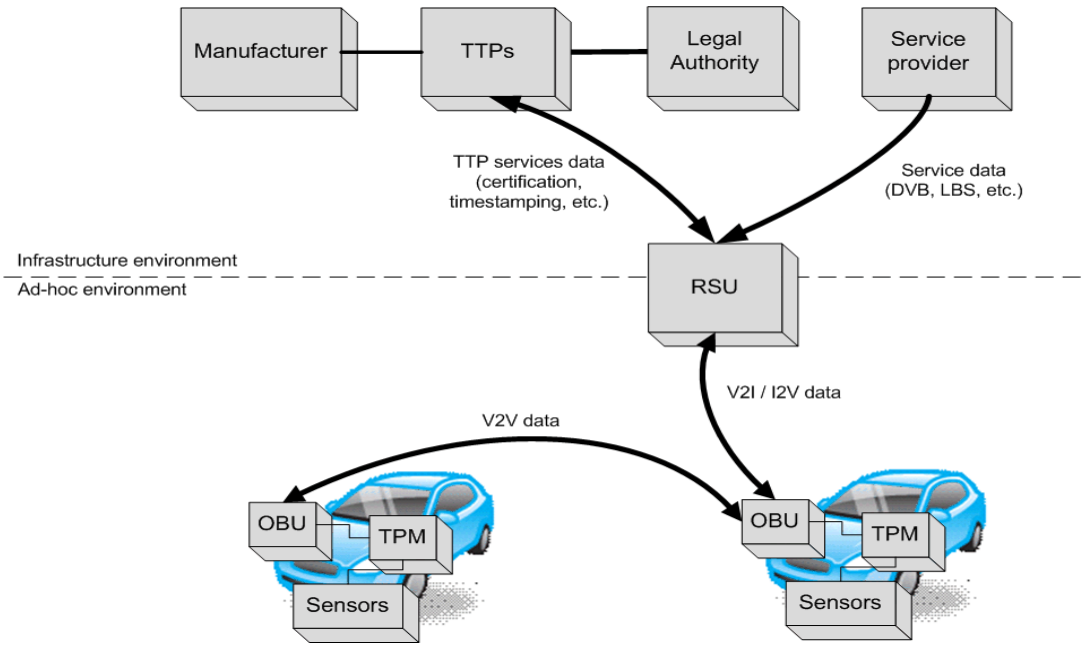


Figure 1.5 Details of VANET model

Other is Adhoc environment which provide adhoc communication between vehicles and vehicle to RSU. In VANET, each vehicle is equipped with three important devices which are used for the communication that is On-Board Unit (OBU), Sensors and Trusted Platform Module (TPM). OBU acts as a communication unit which provide vehicle to

vehicle and vehicle to RSU communication. Sensors are used for measuring the indications of its own status like fuel consumption or safety distance and slippery road. The data generated from sensors are shared among vehicles to improve traffic safety. TPM is implemented on vehicles which are used for security purposes as they provide computation and storage in which sensitive information of users are stored.

1.6 Type of Communication

In VANET, each node communicates to other node either in voice form or through messages. Communication in VANET is necessary to provide up-to-date and exact information to the vehicles in the VANET area and this information is given by the vehicles to other vehicles.

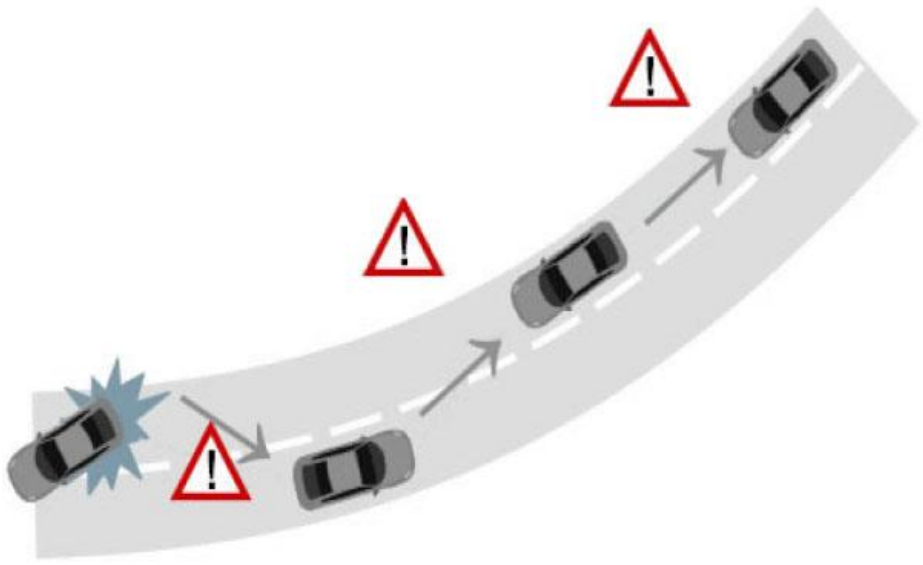
To provide the exact information, system needs perfect communication protocols and good positioning devices. Perfect communication protocols is needed due to unreliable shared communication medium and limited bandwidth for providing secure and efficient messages to all the vehicles. There are mainly three types of communication available in VANET that are:

1.6.1 Vehicle-To-Vehicle(V2V) Communication

It is a multi-hop or multi-cast technique is used to forward the messages related to situation of road and traffic over multiple hops [6]. In ITS, the vehicles needs the critical information of forward direction not the backward direction like emergency messages related to any collision, huge traffic or environment warning. As shown in Figure 1.6 the messages forward in V2V are of two types; first is naïve broadcasting while second is intelligent broadcasting.

Naïve based broadcasting is used when the vehicle want to broadcast the message periodically and at usual intervals. Another vehicle who receives the broadcast message ignores it if message comes from behind it and accept the message if comes from the front and further broadcast to the vehicles behind it. The limitation of naïve based broadcasting is that it broadcast a large number of messages by which collision between messages increases and delivery rates of message decreases and delivery time increases.

Intelligent broadcasting solves the problem of naïve based broadcasting by adopting the acknowledgement method in which we restrict the number of message in an emergency. If emergency detecting vehicle receives same message from front and behind, then it will not broadcast that message and assume that the vehicles behind it broadcast the message so, the vehicle behind it is responsible for broadcasting the message to rest of vehicles.



.

Figure 1.6 Inter-Vehicle Communication

1.6.2 Vehicle-To-Roadside(V2R) Communication

The communication which takes place between the vehicles and RSU with a single hop Broadcasting are known as V2R communication. In this, RSU sends the broadcast message to all the vehicles which make a network with it. It provides a high bandwidth link between the RSU and the vehicles. As shown in Figure 1.7 the RSU can be at any place either at every kilometer or less but they provides high data rates in heavy traffic also. For example when broadcasting speed limits, RSU will find the relevant speed limit through its internal traffic conditions and time table. On time to time the RSU broadcast the message which include speed limits and compare the directional or geographic limits of vehicles to determine if the vehicle goes beyond given speed limit or not and then broadcast the warning messages to the vehicle and request him to reduce the speed.

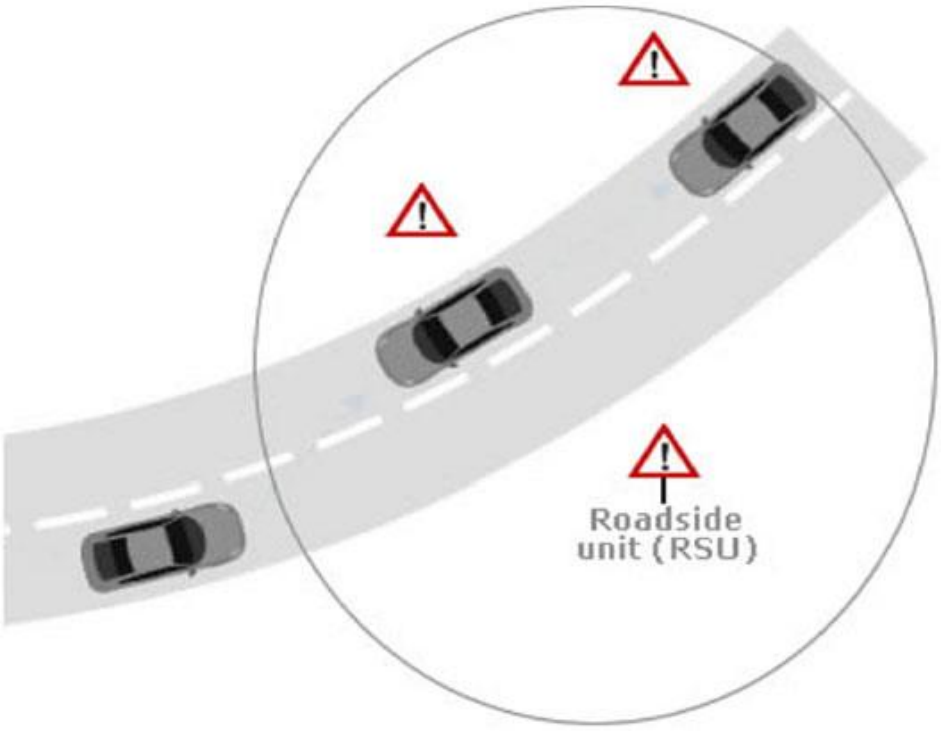


Figure 1.7 Vehicles to RSU Communication

1.6.3 Inter Roadside Communication

The communication which takes place between the local RSU and local RSU to main RSU is known as INTER ROADSIDE communication. Depends on requirement when the vehicle retrieves the information from the RSU it forward its data to the local RSU, then the local RSU forward its data to the main RSU through multi hop route. If a vehicle want to forward its data to other vehicle through end to end delivery inter roadside route, then RSU which is in range of sending vehicle send the data to other RSU and soon by which data reaches to the final RSU and this final RSU is in range of destination vehicle. The data are sending through that route which is of minimum hop and cost. Then the final RSU send the data to destination vehicle.

1.7 Application of VANET

To implement the VANET, there should be some particular application that gets profit from them. We divide the application of VANET in two main parts [7, 8]

1.7.1 Application related to safety

The applications which are link to safety are used to provide the safety on the roads and also for the passengers. These are the applications which are builds and implemented in vehicles to provide safety to the passenger and drivers. These applications are further divided into three major parts that is:

- **Collision prevention and avoidance:** According to the research, about 65% of the accidents can be prevented if we provide a warning message to the driver some second before the collision. For the safety of passenger, we need the application to be installed in the vehicles which provide warning message.
- **Cooperative driving:** We can also provide signals to the drivers related to traffic warnings including Lane change warning, curve speed warning etc. This traffic related signals help the driver for safe and uninterrupted driving.
- **Traffic optimization:** Sending signals of traffic jam, accidents etc to the vehicles help in optimization of traffic so that they can change their route and take another path to save the time.

1.7.2 Application related to User

These applications are made for commercial purpose of users. Apart from safety these application provides entertainment to the users. These applications are part of VANET and are made due to the demand of user and advancement in technology, so vehicular manufacturers need to upgrade their vehicle time to time. The VANET applications which provide services to the user are:

- **Peer to peer application:** These applications are use to make temporary adhoc network between vehicles for the sharing of music, movies etc.
- **Internet connectivity:** Internet is thing through which everyone want to connect all the time. Internet become the basic communication medium between the two or more person. In the VANET various applications are based upon the internet so constant connectivity is needed to the users which are provided by the VANET.
- **Other services:** VANET also provide others applications for the users like locate to fuel station, payment of taxes at toll taxes, restaurant etc.

1.8 Characteristics of VANET

VANET is a new area of MANET, so in comparison with MANET some characteristics resemble but there are some own characteristics of VANET which are different from MANET and they are:

- **High movability:** The vehicular nodes in VANET are moving with a very high speed. This makes difficulty in predication of node position by which it creates problem in providing security to node privacy [9].
- **Uncertain network topology:** The vehicular node in VANET changes their position very frequently because of random speed and high movability. Due to this the network topology changes very rapidly.
- **Unbounded size of network:** VANET can be installed for a region, a city, a state or for whole country. It means the size of network is unbounded with respect to geographic.
- **Rapid exchange of messages:** There are various types of messages exchange between vehicles or vehicle to RSU in adhoc network of VANET. Hence rapid exchange of message takes place in VANET.
- **Wireless Communication:** VANET is designed on adhoc network which is based upon wireless environment. Nodes make the network and exchange their information through wireless medium. There are some security measures which should be adopted in wireless communication.
- **Time Critical:** The warning messages which are transfer in VANET are very critical so, these messages should be delivered in time so that appropriate action can be taken by receiver according to message.
- **Sufficient Energy:** There is no problem related to energy and computation resources in the VANET. Due to this various techniques like RSA and ECDSA are implemented and provide infinite transmission power.
- **Good physical security:** The physical protection of VANET nodes are good than any other mobile nodes. Thus on physical level, VANET nodes are hard to attack and thus lowering the network attack.

1.9 Challenging issue in VANET

In spite of the fact that the characteristics of VANET recognizes it an alternate network however a few characteristics forces some difficulties to deploy the VANET. These challenges can be categorized in following way [10]:

1.9.1 Technical Challenges

The technical problem raises the technical issues which should be removed before the installation of VANET. The technical challenges are:

- **Network management:** Due to high movability of nodes, high changes in network topology and rapid changes in channel condition, we cannot make any structure like tree because these structures cannot be settled down for longer time due to this challenge raised in management of network.
- **Congestion and Collision control:** The infinite size of network also creates the issue. The load of traffic is less in night in urban region and also less in rural region by which it creates the partition of network with the high traffic area by which there occurs congestion and collision in network.
- **Environmental impact:** For the communication purpose VANET use the electromagnetic waves and electromagnetic waves are affected by environment by which it becomes a technical issue in VANET.
- **MAC design:** For the communication purpose VANET uses shared medium by which MAC become a big issue. Various techniques like CSMA, TDMA and SDMA etc. are adopted. In VANET, CSMA has been adopted by IEEE 802.11.
- **Security:** The VANET application is related to the road safety which provide critical information to the vehicles therefore message security must be satisfied.

1.9.2 Economic and Social Challenges

To install the VANET, apart from technical issue, there is also the issue of economic and social. It is difficult to persuade manufacturers to construct a framework that conveys on the traffic signal infringement in light of the fact that a purchaser may reject such sort of

checking. On the other hand, consumers value the notice message of police trap. So to propel the manufacturers for the installation of VANET will get minimal motivation.

1.10 Issues of Security in VANET

Towards security issue, the attention of researchers and manufacturers are very less in comparison with other issues. Information in VANET are exchanged in the form of packets which involve life critical messages so it is necessary to secure that these messages should not altered and neither inserted through the attackers, furthermore the obligation of vehicle drivers should be made up that they advise the environment of traffic within time with effectively. The issues in security of VANET are not similar to communication network. The extent of network, versatility, geographic pertinence and soon build the installation difficult and particular from another network security.

The difficulties of security should be recognized amid the composition of VANET architecture, cryptographic algorithm and security protocols etc. The security challenges are [9]:

- **Real time Constraint:** Messages related to safety should be sent with transmission delay of 100ms as they become time critical message. So to accomplish real time constraint, fast algorithm of cryptography, need to be utilized. Node with message authentication should be done within time.
- **Information Consistency Risk:** Even into the VANET validate node can do the noxious works which can bring out the accidents or bother network. Hence to evade the inconsistency, a particular method must be designed. Connection between the received data from different nodes on particular information may evade this type of inconsistency.
- **Lowering resistance for error:** A few protocols are composed based on the probability. VANET uses the data which are life critical on that activity which is done in small time. A small mistake in calculation based on probability may bring harm.
- **Sharing of keys:** In VANET, all the implemented security mechanisms are based on the keys. By using the asymmetric or symmetric mechanism,

encryption and decryption of every message is done at sender and receiver side. Additionally diverse manufacturer can give keys in different ways and into the public key base trust on certification get to be significant issue. In this way making of secure protocols, key distribution among vehicles becomes a critical challenge.

- **Incentives:** Manufacturers are intrigued to construct applications that consumers enjoy most. Not very many purchasers will become agree upon a vehicle that consequently reports any type of traffic rule infringement. Hence strongly installation of vehicular adhoc networks should need motivators for manufacturers of vehicles, buyers and higher authority is a test to execute VANET security.
- **High Movability:** The supply of energy with computational ability into the VANET is approx to the non-wireless system node. Although for same throughput, VANET need minor time for execution in comparison with wired network because of high movability of nodes in VANET. Hence to lowering the time of execution, we use the architecture of security protocols. Two methods can execute to fit into this prerequisite. First is security algorithm of low complexity and other is transport protocol.

1.11 Security requirements in VANET

Before the installation of VANET, it must fulfill some security requirements. A security framework in VANET ought to fulfill the following specification [8]:

- **Authentication of message:** Authentication provides that the message is produced by the valid client. Into the VANET a vehicular node counter upon that the data which is send from the different vehicle consequently authentication of message must be completed.

- **Availability of message:** It ensures that is message is available to each available user who is legitimate. Some attacks like DOS can lower down the system and subsequently data are not available.

- **Non-repudiation of message:** Non-repudiation is way in which a node can't deny that he doesn't send the message. Into the critical situation, it is difficult to determine the actual sequence.

- **Privacy of message:** In contrast to unauthorized nodes, the security of a node ought to be ensured. So, privacy is needed to dispose the attacks like message delay.

- **Verification of data:** To lowering of the wrong message a time to time verification of data is needed.

1.12 Attackers in Vehicular Network

For the VANET security, first of all we need to find who are the attackers, their tendency, and ability to harm the framework. We divide these attackers on the basis of their capacity:

- **Outsider and Insider:** Outsider attacker are the intruder who is outside the system by which they have their limited capacity while Insider attacker are authenticated members of system so they can harm the system in very bad way.

- **Rational and Malicious:** Rational attacker attack due to their personal profitable nature by which they are predictable while malicious attacker do not have any personal profitable nature they simply hurt the usefulness of the system.

- **Passive and active:** Passive attacker does not generate any time of signal they only sense the system and do not harm the system while packets or signals are generated by active attacker and they also harm the system.

1.13 Attacks on Vehicular network

In spite of the requirement of security, we should have information about the different types of attacks into the VANET with help of that knowledge we can provide better protection. Attacks on various security requirements are given below [11]:

- **Impersonate**: In this type of attack, the attacker expect about character with benefits of the approved node, to build utilization of architecture assets that cannot be accessible to it into any type of typical condition, disturb any ordinary working of the architecture. This kind of different attack is executed by current attackers. They might be both that is outsider and insider. Impersonate is a multilayer type of attack implies attacker who exploit either transport layer, application layer or network layer.
- **Hijacking of session:** At the beginning of session, maximum number of authentication is done. Subsequently after establishment of connection it is simple to hijack any of the session. Into the session hijacking, hijackers hijack the session which are created between nodes.
- **Location Tracking:** The path followed for a long period of time and location of vehicles at a given moment can be utilized to get the location of any vehicle and get driver information.
- **Repudiation:** Fundamental risk in repudiation is denial of sending of any message in communication. This is not quite the same as the impersonate attack. In this attack two or more elements has common identity subsequently it is anything but difficult to get undefined and consequently they can be revoked.
- **Eavesdropping:** It is the most common confidentiality attack. This attack is passive in nature and of network layer attack. The basic aim of this attack is to get contents of secret information.
- **Denial of Service (DOS):** This attack is very much noticeable attack in this classification. In this attack attacker puts the authentic client to take help of the service from the victim node [12].

1.14 Cryptography

Cryptography is most essential aspect to provide security in communication. In cryptography we learn about verification and hiding of information. Cryptography is made of combination of two greek words that is “kryptos” which means “hidden” and graphein which means “hidden writing” or “to write” [13]. Cryptography is the

mechanism through which we can change the sending information into an unreadable format such that except communicate nodes, no other nodes can read it. There are some services which are provided by the cryptography that are:

- **Confidentiality of message**: The receivers who are authorized can only able to read the message extracting from an unreadable form that is in encrypted form.
- **Integrity of message:** The receiver should have some method through which he can determine that the message is alter or not.
- **Authentication of sender:** From the message the receiver should be able to identify the sender of message and the path through which this message comes.
- **Non- repudiation of sender**: the sender who sends the message should not able to deny of sending of message.

There are two form of the message into cryptography that are:

1. **Plaintext or clear text:** The messages which are in readable format are known as plaintext. These messages are into its original form before any type of changes into it.
2. **Cipher text:** The messages which are in mangled form are known as cipher text. These messages are in unreadable format and are generated after some changes. It is depend upon the secret key and the clear text. For a given plain text, two or more keys will generate two or more different cipher text.

Cryptography is the mechanism through which we change the plain text into the cipher text and from cipher text to plain text as shown in Figure 1.8. This can be done by two mechanisms that are:

1. **Encryption:** Encryption is the mechanism through which we can change the message from plain text to unreadable format that is cipher text.
2. **Decryption:** Decryption is the reverse of encryption that is it is the mechanism through which we can change the message from unreadable format that is cipher text to readable format that is plain text.

Cryptographic algorithm involves both the mechanism with a secret value. This secret value called as **key**. The use of key is similar to the combination lock as we know into the combination lock we use the secret numbers to open the lock into a correct sequence , we cannot open a lock without having knowledge of correct combination. Similarly we

cannot read the encrypted message without the use of key and we cannot encrypt a message without a key.

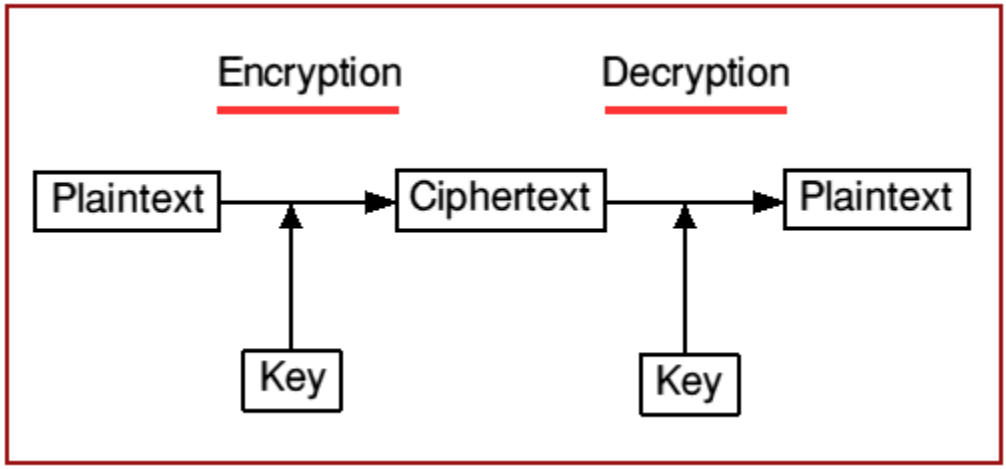


Figure 1.8 Cryptography Mechanisms

The secret key is given as a input with the plain text and this key if not depend on the plain text. The encryption algorithm will generate the different result which depends on the secret key. The transformation and substitution of message is depends upon the key which is performed by the algorithms.

1.15 Public key Cryptography

In our model, we use the public key cryptography algorithms in which we use two keys one is private key while other is the public key. Private Key is known only to the particular person while public key is known to the entire person who participates into the communication. Public key cryptographic is also known as the asymmetric cryptography. Public key is used for the encryption purpose in which we change the plain text to the private text while the private key is used for the decryption purpose in which we change the cipher text to the plain text. Unlike private key cryptography, public key cryptography does not need any shared secret among the participating nodes but public key cryptography is much slower in comparison with private key cryptography as shown in Figure 1.9.

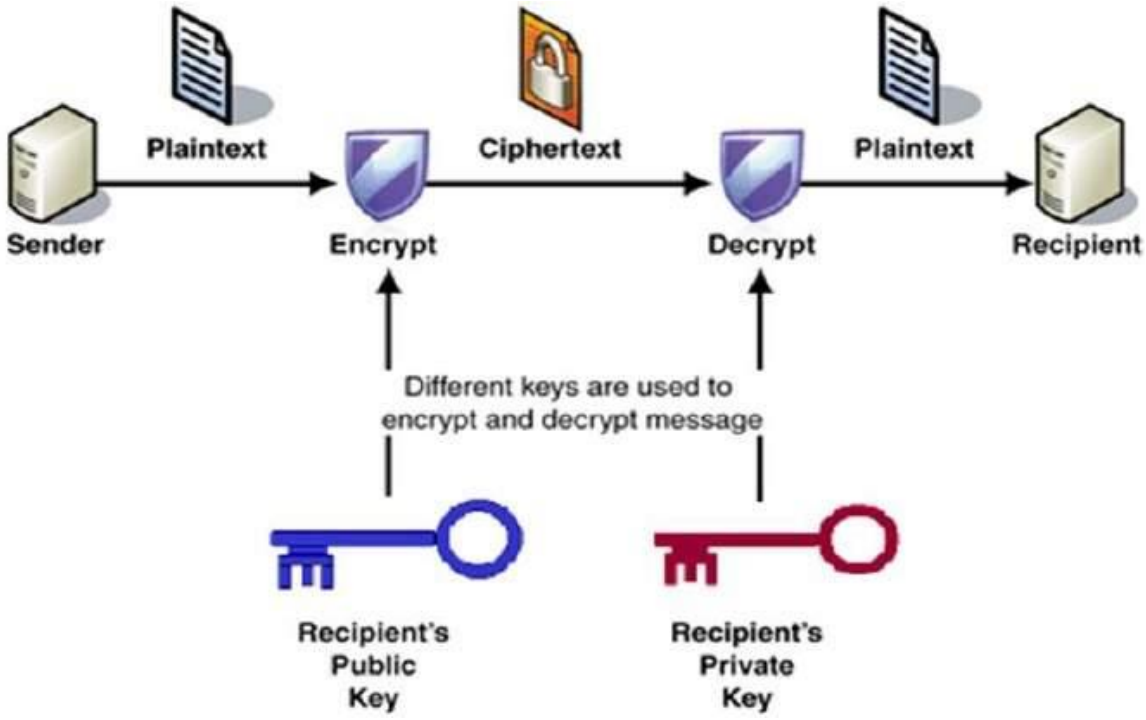


Figure 1.9 Public Key Cryptography

In our model, we use two public key cryptographic algorithms which is used for the secure communication that is

1.15.1 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an asymmetric key cryptography algorithm in which those users who participate into communication have two keys that are private key and public key and for the cryptographic operation there is a set of operation linked to it. In ECC domain parameters are some predefined constants value which is requires to known to all the persons participating into the communication. The mathematical equation of ECC over elliptic curve is [14]:

$$Y^2 = X^3 + aX + b$$

In which,

$$4a^3 + 27b^2 \neq 0$$

The different value of 'a' and 'b' provide us particular elliptic curve. All the points(X, Y) that satisfied the mathematical equation of ECC with a point at the infinity lies on the curve of elliptic as shown in Figure 1.10. The private key is a stochastic number and the

public key is calculated by multiply private number with Generator (G) on curve so public key is also the point on the curve.

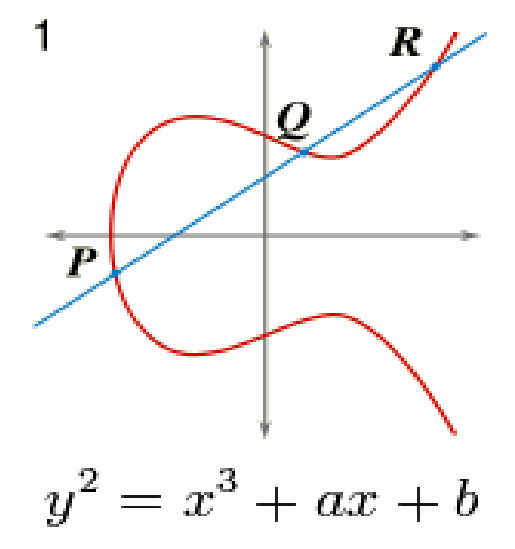


Figure 1.10 Elliptic Curves

The curve parameters (a, b), the generator (G) and few more constant together form the domain parameters of elliptic curve. Due to the small key size generated in ECC that is 160 bit, it provides high security than RSA whose key size is 1024 bit. The security of key is totally depends upon the elliptic curve logarithm problem. Suppose that there are two points A and B on the elliptic curve such that kA= B, where k is a scalar quantity. If k becomes too long, then here A, B will computationally infeasible to calculate k, here k is the logarithm of B to the base A. here main operation of ECC is the point multiplication. Means for the calculation of point B on the curve we have to calculate the multiplication of a point A on the curve to the scalar k. From the ECC, we calculate two key that is public key and the private key. In ECC, private key is generated a random number on the curve while the public key is calculated by multiply the private key to one of domain parameter that is "G". Private Key which is a random selected number should be less than the 'n' here 'n' is one of domain parameter of Elliptic curve.

The domain parameters (P, a, b, G, n, h) are defined over the finite field (F_P) that are used for the Elliptic curve. Where each parameter is defined as:

- "P": It is a prime number which is defined over the field (F_P).

- “a” and “b”: these are parameters which are defined over the elliptic curve equation.
- “G”: It is the generator which is chosen as a point on elliptic curve for operations.
- “n”: It is the order of curve.
- “h”: It is the cofactor which is the total number of points on curve and calculated as:

$$H = \#E(F_P)/n.$$

1.15.2 Elliptic Curve Diffie Hellman (ECDH)

ECDH is key agreement convention that permits two communicating nodes to build up a common secret key which is utilize in private key algorithm. Both the communicating nodes exchange their public data to one another. By using their own private data and public data of another node they calculate a common secret key. By which if any third person who does not know the private details of any communicate node cannot able to calculate the shared secret key from the public data of any node.

Into the ECDH, if we want to calculate the shared secret key between two communicating nodes that is P and Q, and then firstly both the node has to agree upon the common domain parameters. Both the communicating nodes have key pair that is private key “d” and the public key “e”. Let (d_P, e_P) be key pair of P that is the private key-public key. Similarly, (d_Q, e_Q) be key pair of Q that is the private key-public key. Now, following steps are used into the ECDH that are:

- The end P computes $K = (X_K, Y_K) = d_P * e_Q$.
- The end Q computes $L = (X_K, Y_K) = d_Q * e_P$.
- Since $d_P * e_Q = d_P * d_Q * G = d_Q * d_P * G = d_Q * e_P$. it shows that K = L and as a result $X_K = X_L$.
- At the end the shared secret key is X_L .

Chapter 2: Literature Survey

VANET provides the communication in their mobile nodes that is vehicular node and RSUs. The information which is shared between nodes contains some life critical message which are related to any road accident or any other important message. The objective is to secure the communication among vehicular nodes and between vehicular node and RSUs in an adversary environment. Suppose if two vehicles want to communicate with each other in active network in an adversary environment then their first preference is that the message which they transfer to each other should be secure it means it should maintain the authenticity and privacy of their message. Several researchers have done various different research work on how to reach the security goals and gives a secure and user-friendly environment for communication in VANET. Different researcher uses different types of cryptographic algorithm for securing the communication.

2.1 Conventions for Privacy Preservation and Message Authentication

For securing the message transfer in VANET, privacy preservation and authentication is an important factor. The concept of Integrity-based anonymity advent is to get the vehicles untraceable. Rongxing [15] designed a novel efficient conditional protection preservation (ECPP) convention for secure communication between vehicles. The ECPP convention can effectively manage the developing repudiation list while accomplishing conditional traceability by the main authority. Rather than depending on an enormous storage space at each OBU as the majority of the already reported plans did, the proposed convention can keep the required anonymous key storage negligible without losing the security level. In the mean time, the proposed convention picks up benefits in the quick check on security messages and a proficient restrictive protection tracking mechanism, which can serve as a fabulous possibility for the future VANETs. As stated by Rongxing [15], two main models for integrity-based anonymity advances: first is huge anonymous key based (HAB)[16][15][17], second is group signature based(GSB)[18][19].

In HAB, OBU stores a considerable measure of mysterious keys, which are marked by CAs and used to sign security messages by changing the signing key always; it gets to be

harder to track the vehicles. The primary point of interest of HAB is its effortlessness and straightforwardness. In any case it has a few issues one of these issues is that OBU needs a huge storage room for mysterious keys another is that the key management will turn into an issue. Furthermore, preparing a long list of certificate revocation list (CRL) will take a long time. In GSB, the key thought is to permit a group member to sign messages secretly for the benefit of group. The benefits of GSB are twofold: it decreases the quantity of unknown keys and it has a shorter denial list. In any case, the check time of safety messages will become linearly with the quantity of repudiated identities in revocation list.

Both of them can locate the security demand well, like identity revocation, non-repudiation, authentication and conditional anonymity. The group signature utilizes Group-signature-based schemes [20] and each public node would not expose the regular existence of a conventional traffic message [21], [23]. One existential drawback is that order of the amount for marking and authenticating messages is much longer than amount for accepting the conventional public key related signature.

To cut down those aerial, A.Wasef et al. [24] proposed a protocol which is effective distributed certificate-service (DCS) scheme for vehicular adhoc networks. The proposed plan offers adaptable interoperability for certificate service in heterogeneous managerial authorities and an effective route for any installed units like OBUs to redesign its declaration from the accessible framework roadside units (RSUs) in an opportune way. Also, the DCS plan presents a total batch check strategy for confirming certificate based signatures, which essentially diminishes the verification overhead. Security examination and execution assessment exhibit that the DCS plan can diminish the complexity of certification management and accomplish incredible security and efficiency for vehicular message communication.

In DCS, a vehicle could release the document for themselves with the help of a number of keys followed by signing their own messages. It is followed by applying the public-key-based signature due to which there is a decrement in average overhead of message authentication. This proposal concludes an adjustment between traditional PKI based schemes and group-signature-based scheme as shown in Figure 2.1. As vehicles moves

with a very high speed and bandwidth of wireless communication is finite, so it is tough for assign a number of Certificate Revocation list (CRL) for every vehicle.

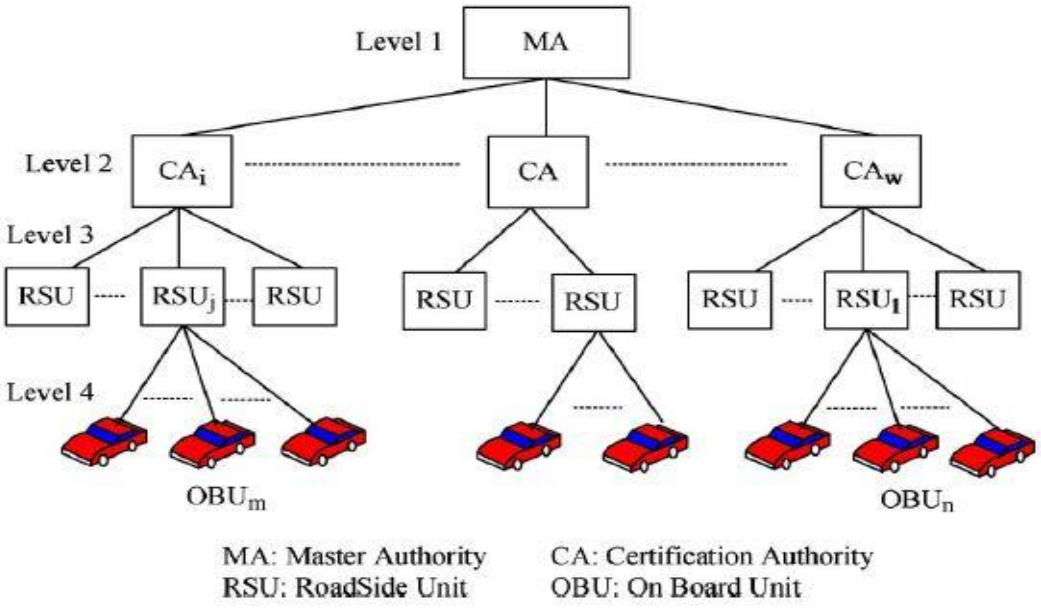


Figure 2.1 Proposed DCS hierarchical architecture.

To reduce the size of CRL, Bellur [21] recommended to breakdown a large place into a number of zones and assigning the certificates depends on their zones with a valid time period for a vehicle. Keeping in mind the goal is to diminish the complexity of dealing with security framework based on Public key infrastructure (PKI), Bellur proposed novel certificate assignment methodologies which will use in the VANET. The methodology includes sectioning a nation into various geographic areas, and the task of locales particular declarations to an OBU which is shown in Figure 2.2. The utilization of area particular certificates is ways which deal with contain compromise since it actually confines the geographic degree of the validity of the authentications.

Idea of Certification authorities of region wise is based upon the judicial boundaries and administrative described in [22]. Its aim is to misuse the spatial region of vehicular communications to decrease the complexity of dealing with security framework of PKI based. The efficient conditional privacy preservation (ECPP) protocol is proposed by Lu et al. [15], is the first protocol which provides support to legitimate vehicles to restoring Pseudonymous certificates for short time from the RSUs quickly.

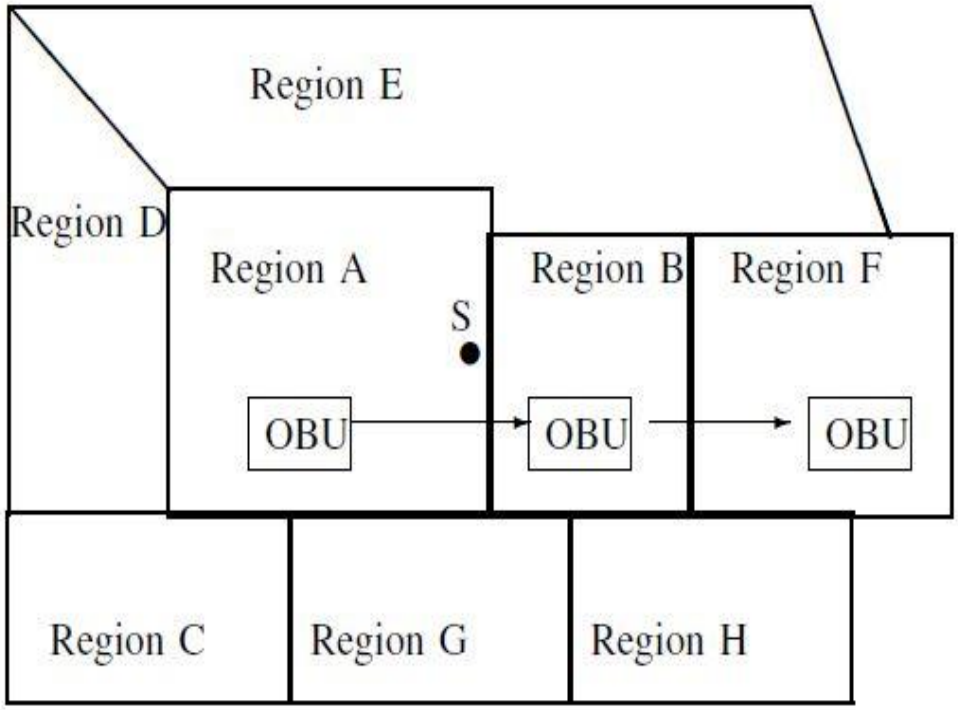


Figure 2.2 Segmentation of a country

2.2 Protocol based on One Way Hash Function and Blind Signature

Chun-Ta Li et al. [25] gave a proposal based on One-Way hash function and Blind Signature. It not only authenticates V2V and V2I communication but also establishes the key for the communication between nodes and also combines blind signature system with proposal allowing vehicular node to connect with the utility of roadside unit. For the issue of privacy and security threats, this proposal claims to complete many security requirements.

There are two basic advantage of this proposal in comparison with other related proposal. First is that it grants anonymity of message communication among the vehicles and vehicle to RSU. Second one is that into their proposal it associate authenticated key establishment by using the methodology of cryptographic algorithm including blind signature, one-way hash function and non-interactive key agreement. Their proposed work is first experiment in VANET which provide a model for secure communication with key establishment protocol, mutual authentication and privacy preservation.

2.3 Authentication Protocol of Message Based on ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) helps as an algorithm for digital signature which works on elliptic curve [26]. Cryptographic method like ECDSA provide key agreement and authentication protocol for the non- wired communication. ECDSA requires less bandwidth in comparison with other cryptographic algorithm. It also requires less computational cost, communicational cost and storage requirement on server side as compared to other algorithm. By using the ECDSA method, using few bits it provide high security than higher bits algorithm by which it makes suitable for communication system in VANET.

S.S. Manvi et al. [27], on the basis of ECDSA proposed a protocol for authentication of message. In this proposed work each vehicle consist of public and private key and the vehicles who want to communicate with each other have to agree upon the domain parameters of elliptic curves. It is an alternative method of digital signature algorithm (DSA) which works on the elliptic curve group. He claimed that he will overcome from some of inherent drawbacks of security and authentication protocols that are existed. The drawbacks are communicational and computational overheads, requirement of storage, processing delay required for authentication at receiver and server side and soon.

2.4 Essential Drawbacks of Existing protocols

The proposals given by current researchers are reliable and efficient. The researchers have made various proposals which prove to be true and up to the mark. In case of VANET security each paper will have their different contributions. But still there are various flaws existing in proposals are:

1. Additional delay in process for authenticating the communication at receiver and sender side.
2. Communicational cost of exchanging the message at both sender and receiver side.

3. Computational cost is high due to encryption and decryption of the message. Continuously updating of list of revoked nodes and broadcasting to all the nodes in network leads to high computation cost.
4. Memory requirement for restoring the updating of revoked list as well as memory also required by each pseudonym for storing and certifying.

Motivated from all these works, we propose a protocol that takes the profit from the exiting protocols and also do the improvement in exiting work to achieve security, conditional privacy and authentication against all the attacks. Our proposed work provides data origin authentication, data integrity, reliability, non-repudiation and efficiency. If we compare our proposed work it is highly secure than other as we use ECC which takes key of 160 –bit while proposal which use RSA uses key of 1024-bit but with less key size ECDSA is highly secure than RSA. ECC requires less space in memory and is faster than others. Also it takes the guaranty of the security because ECDLP is more secure in comparison with its IFP and DLP.

Chapter 3: Problem Statement

Vehicular Adhoc Networks (VANETs) is a new area of mobile adhoc network which have the capability of self-organized network in a decentralized fashion with infrastructure less architecture. VANET are design mainly for the security purpose either to provide safety to driver or to passenger and also to reduce the number of road accidents. It is a part of ITS which provide communication in between the vehicles, vehicle-to-RSU and among the RSU in an adversary environment.

There are various challenging issues in VANET which include technical and economical challenges. But among all the issue, security is a major technical challenging issue in VANET. The information which are exchanged contains life critical information, so we should make sure that these information are not be compromised by attackers and should be delivered on time. We have to provide a strong message integrity and authentication technique. The aim is to provide security services to VANETs such as confidentiality, authentication, availability, integrity and soon. The attacks on security of VANET are impersonate, session hijack, repudiation, denial of service, location tracking, identity revealing etc.

If any vehicles want to communicate with any other vehicle in an adversary environment, then he want that the message which are transferred between them should remain secure that is it should be private and authenticity of message should be maintained. Various researchers proposed their work for securing the communication between vehicles but there are various inherent drawbacks likes communication cost, storage cost and computation cost. So these drawbacks motivate me to work on securing the communication between vehicles with less storage cost, computation cost and communication cost.

Chapter 4 Methodology

Vehicular Adhoc Network (VANET) provides the communication between vehicles to vehicle in which they communicate with each other either by sending the text message or images etc. So, our main aim is to secure the messages which are transfer between vehicles to vehicle. Additionally we have to lower the communication cost, computation cost and storage cost. We have to secure the messages between two communicating vehicles such that any third party cannot access the message or if they access the message they should not read the message or cannot alter the messages. So, we have to propose a mechanism such that message should not be accessible, or attacker cannot read or alter the message. For making the message in unreadable format we have to convert the message into another form which the attacker cannot understand. It means we have to convert the message into such a format which is understood by only communicating vehicles and no one else.

To secure the message and converting it into unreadable format we have to use the cryptographic algorithm. As we know cryptography is the method through which we can secure the message by converting the message into unreadable format. There are two main process of cryptographic that is encryption and decryption. For the both mechanism we have to use the key which is highly secure. Because this key is used in both the encryption and decryption, so security of message is highly depend upon the how secure is our key. Various cryptographic algorithms are used by different researchers for securing the key in order to secure the message which makes secure the communication between the vehicles.

In this proposal we assume that the route is secure means we mainly deal with authentication and integrity of message. Our main work is to authenticate the message that it should come from legitimate vehicles and also we have to secure the message that no one can alter the message. We propose a model for securing the authentication and integrity of message in an adversary environment. In our proposed work, we firstly want to generate the key which is used for encryption and decryption the message. We use asymmetric key generation algorithm in which we generate two keys that is public and private key. These two keys are generated from the certification authority after that we

use another algorithm which is used for the communication purpose means the keys that are generated from certification authority are used in another algorithm for communication purpose.

Our whole model is divided into two phases. First is Registration phase and second is Communication phase.

4.1 Registration Phase

In this phase, each time when the vehicle enters into the VANET and wants to communicate to another vehicle, he has to do registration with the certification authority.

The registration phase includes the generation of public and private key for each vehicle. In our proposal we assume the roadside unit as a certification authority which is used for the registration of vehicles. The registration phase is mainly deal with the public key infrastructure system; in which certification authority provide the public and private key to the vehicle for communication process.

In this registration phase we use the Elliptic Curve Cryptography (ECC) mechanism for the secure key generation that is generation of public and private key for vehicles from Certification Authority (CA). As we know ECC produces a key of very small size and is of high security. Various other researchers used various different algorithms for asymmetric key generation like MD5 and RSA. But we use ECC algorithm because in comparison to other algorithm it produces the key of small size and of high security. If we compare RSA and ECC, then RSA produces key of 1024 bit while ECC produces key size of 160 bit which if of very less size and even of less key size of ECC, its key are highly secure than key generated from RSA.

The security of ECC algorithm highly depends on the problem of Elliptic Curve Discrete Logarithm Problem (ECDLP). By which the security of message is totally depend upon the security of keys as more as our key is strong the more our message will be secure. The two public and private key which are generated from CA, the private key is known to the particular user and public key is known to the all the available users which take part in communication.

Mathematical equation of ECC :

$Y^2 = X^3 + aX + b$

in which,

$4a^3 + 27b^2 \neq 0$

Here we use different elliptic curve for different values of (a, b). All the points(X, Y) that satisfied the mathematical equation of ECC with a point at the infinity lies on the curve of elliptic. The private key is a stochastic number and the public key is calculated by multiply private number with Generator (G) on curve so public key is also the point on the curve.

Suppose that "d" is a private key then public key (Q) is obtained as

$$\boldsymbol{Q = d * G}$$

In Elliptic Curve Key Pair Generation, we use domain parameters ***(P, a, b, G, n, h)*** over finite field (Fp) as input parameters and public and private key is output generated by them.

There are basically four steps through which a vehicle gets its public and private key from Certification Authority that is RSU which are shown in Figure 4.1 and they are:

1. Suppose a vehicle "V1" send a request message for private key to the certification authority in encrypted form. The encryption is done with public key of certification authority and request message contains ID of driver "A", ID of vehicle (V1), domain parameters for Elliptic Curve (EC) and time stamp.

$$\boldsymbol{E_{K(CA)}[ID_A||ID_{V1}||(P, a, b, G, n, h)||N1]}$$

2. Now CA will send the private key "d(A)" to the vehicle "V1" in the encrypted form with ID of driver "A".

$$\boldsymbol{E_{K(CA)}[ID_A||d(A)]}$$

3. Again the vehicle “V1” send a request message for the generator (G) to the certification authority and request message contains ID of “A” with time stamp which is encrypted with private key of “A” which again encrypted with public key of CA.

$$E_{K(CA)}\ [E_{d(A)}[ID_A \,||\, N_2]]$$

4. Now the CA will send the Generator (G) to vehicle “V1” with ID of A and time stamp which is encrypted with public key of CA which again encrypted with private key of A.

$$E_{K(CA)}\ [E_{d(A)}[ID_A \,||\, N_2 \,||G]]$$

Now Vehicle “V1” have both private key “d(A)” as well as generator(G) by which he calculates his own public key “Q(A)”.

$$Q(A) = d(A)*G$$

Similarly vehicle “V2” get its public and private key from Certification Authority so, at the end of registration phase both vehicle ”V1” and ”V2” having private key and public key.

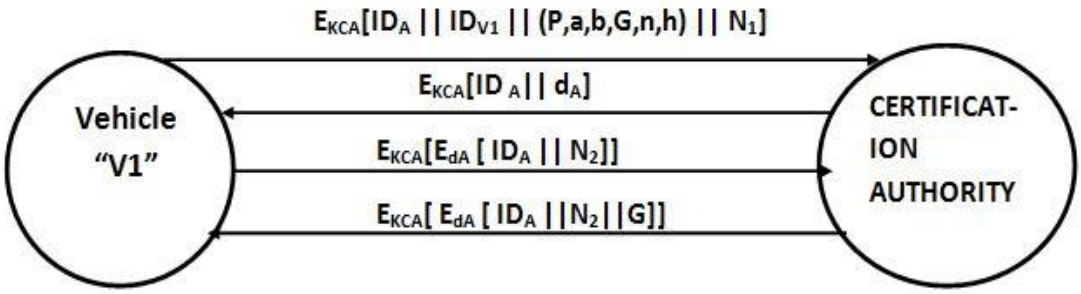


Figure 4.1 Registration phase

4.2 Communication phase

In this phase both the vehicle “V1” and “V2” want to communicate with each other and both vehicles want to secure the authenticity and integrity of their messages. So for securing the communicational phase we use Elliptic Curve Diffie Hellman (ECDH) approach. ECDH is a protocol in which both the vehicles have to agree upon a shared Secret key that use as a private key algorithm. As both the vehicle exchange their own private message with the public data in an adversary environment, both vehicle can calculate the shared secret key but any other vehicle who doesn’t know the secret information of both the car unable to calculate the shared secret key by which communication remains secure as shown in Figure 4.2.

In this phase both vehicle “V1” and “V2” have to agree upon Elliptic Curve Domain Parameters for generating a shared secret key and both vehicle have their own public and private key pairs.

Suppose vehicle “V1” have key pair (d(A) &Q(A)) where d(A) is private key and Q(A) is public key of V1. Similarly vehicle “V2” have key pair (d(B) & Q(B)) where d(B) is private key and Q(B) is public key of “V2”. The following steps involved into the creation of secret shared key:

- Vehicle “V2” sends its public key QB to vehicle ”V1”, then vehicle ”V1” computes-

$$K = (X_K, Y_K) = d(A)*Q(B)$$

- Vehicle “V1” sends its public key QA to vehicle “V2”, then vehicle “V2” computes-

$$L = (X_L, Y_L) = d(B)*Q(A)$$

- Now as we know

$$Q(B) = D(B)*G \text{ and } Q(A) = d(A)*G$$

Since

$$d(A)*Q(B) = d(A)*d(B)*G = d(B)*d(A)*G = d(B)*Q(A)$$

Therefore

$$k = L$$

And here

$$X_K = X_L$$

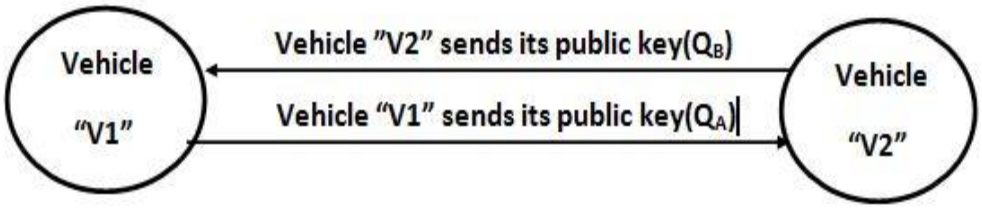


Figure 4.2 Communication Phase

- So shared secret key between two vehicles is X_K.

Chapter 5: Implementation Details with Performance analysis

5.1 Installation

Following are the software that install before begin:

5.1.1 Java and Net beans IDE Installation:

a. First we downloaded Java and installed it in our system.

b. After Java installation we need to install Net beans IDE.

5.2 Implementation

Our main aim into the proposed work is to secure the communication between communicating vehicles into the adversary environment with the low computation cost, communication cost and storage cost. Computation cost is totally depends upon the computation time. Computation time is the time taken for the encryption/decryption purpose. So, for calculating Computation time we have to calculate the time taken in executing the encryption/decryption code.

Firstly we create the code of encryption of ECC into the java language into the Net beans editor and then compile and run our java code. The time taken in execution of our encryption code is **1.21s.** So this is the computation time of Encryption code of ECC. As in our proposed work, we have used 4 times the encryption technique so, in our proposed work total computation time is total time taken into running the encryption code four times.

So, total computation time = 1.21s * 4 = **4.84 s**.

5.3 Performance Analysis

In this category, we do performance analysis of our proposed model and compare it with the performance of other related works. We do the performance analysis on the basis of computational costs. In [28], He et al. gave a proposal based on an authorized-anonymous-ID-based scheme. The security of their proposal is dependent on RSA cryptosystem and blind signature. Further, in [29], Yang et al. suggested an efficient

and protected authentication protocol for granting communication channel in wireless structure by not using asymmetric cryptosystems. The performance analysis of our proposed model, Chun-Ta Li et al.'s scheme [25], Yang et al.'s scheme[29] and He et al.'s scheme[28] are compared and result are shown in Table 5.1 and 5.2.

For calculating the computational costs we use different parameters which include:

1. **CT_E -** emphasize the time taken for modular exponentiation.
2. **CT_H -** emphasize the time taken for hashing operation.
3. **CT_S -** emphasize the time taken for symmetric encryption.
4. **CT_{AS} -** emphasize the time taken for asymmetric encryption.
5. **CT_X -** emphasize the time taken for XOR operation.

TABLE 5.1 Comparison of Communication Cost

Parameter	**Proposed Scheme**	**Chun- Ta-Li's scheme [25]**	**Yang et al's scheme [29]**	**He et al's scheme [28]**
CT_{AS}	4	5	0	6
CT_S	0	0	8	6
CT_E	0	0	17	0
CT_H	0	9	0	5
CT_X	0	9	4	0
Total computation Costs	$400CT_S$	500 CT_S	1028 CT_S	602 CT_S

For example, symmetric encryption is faster than asymmetric encryption by a factor of 100. A modular exponentiation is approx 60 times of symmetric encryptions. Hence, for one way hashing it requires 0.0005s and 0.0087s for symmetric encryption**.**

TABLE 5.2 Performance analysis of proposed model

	Proposed Scheme	**Chun- Ta-Li's scheme [25]**	**Yang et al's scheme [29]**	**He et al's scheme [28]**
Registration phase	$4CT_{AS}$	$9CT_X + 9CT_H + 5CT_{AS}$ + 5 random numbers	$4CT_X + 17CT_E + 8CT_S$ + 10 random numbers	$6CT_S + 5CT_H + 6CT_{AS}$ + 2 random numbers
Computation costs	$400CT_S$	500 CT_S	1028 CT_S	602 CT_S
Computation time (s)	4.84s	5.97s	8.94s	6.52s

A. Computational Overhead

From table 1, it can be analyzed that our proposed scheme shows better performance than the other three schemes. In our scheme we mainly deal with the asymmetric encryption, so there is less computational overhead than other three schemes as they use modular exponentiation, hashing, symmetric and xor operations.

B. Communication Overhead

When any two vehicles want to communicate with each other, the proposed model requires only four steps by which they generate the secret shared key which is used for communication between them. Our proposal completes the requirement of message integrity and mutual authentication and also provides less overhead for the communication.

C. Storage Overhead

Into the Registration phase, the proposed model gains low storage overheads because the service provider does not need to maintain all the details of each user. Service provider only needs to store the key pair and some credential data of each user. The information stored by the service provider is secure.

Chapter 6: Conclusion and Future Scope

A proposed approach for securing the communication in VANET with less computation and communication cost is concluded in this chapter. In Future there are some of the points that can be considered.

6.1 Conclusion

In this paper, our main aim is to design a model for efficient and secure communication in VANET. Here we proposed a model which contains two phases of registration and communication phase for transferring secure message. We use ECC for the the registration phase which provide public and private key to the vehicle and in communication phase we use ECDH, by which we generate a shared secret key which used for communication between vehicles. The model which we propose requires less communication and computational costs. As we use ECC and ECDH, so here key generation is of less size with better security. Our Model gives the security to communication with low Computation Cost and low Communication Cost. Hence the proposed model provides security into an adversary environment when two vehicles want to communicate with each other.

6.2 Future Work

There are some of the points that can be explored further are as follows

a) To explore more security feature of the proposed scheme.

b) Parameters like Storage Overhead, Communication Cost, and Computation Cost can also be considered for the future work.

c) Implementation of whole work with more parameters can be done on Network simulators.

References

[1] S. Samba, Y. Zongkai and H. Jianhua, "A survey on mobile ad hoc wireless network", *Information Technology Journal*, vol. 3, no. 2, pp. 168--175, 2004.

[2] M. SS, K. MS, P. Jeremy and R. Alex, "Multi agent systems as a platform for VANETs", *International conference on autonomous agents and multi agent systems (AAMAS)*, pp. 35--42, 2006.

[3] C. Marco and G. Silvia, "Multihop ad hoc networking: The theory", *Communications Magazine, IEEE*, vol. 45, no. 4, pp. 78--86, 2007.

[4] S. Zeadally, R. Hunt, Y. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", *Telecommunication Systems*, vol. 50, no. 4, pp. 217-241, 2010.

[5] F. Jose Maria, G. Ana Isabel and R. Arturo, "Overview of security issues in Vehicular Ad-hoc Networks", *IGI Global*, 2010.

[6] S. Biswas, R. Tatchikou and F. Dion, "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety", *IEEE Commun. Mag.*, vol. 44, no. 1, pp. 74-82, 2006.

[7] Y. Toor, P. Muhlethaler, A. Laouiti and A. La Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues", *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 74-88, 2008.

[8] R. Maxim, "The Security of Vehicular Ad Hoc Networks", SASN'05, Alexandria, Verginia, USA, pp. 11-21, 2005.

[9] H. Moustafa, Y. Zhang," Vehicular networks: Techniques, Standards, and Applications". CRC Press, 2009.

[10] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks", *IEEE Commun. Mag.*, vol. 46, no. 6, pp. 164-171, 2008.

[11] F. Jose Maria, G. Ana Isabel and R. Arturo, "Overview of security issues in Vehicular Ad-hoc Networks", *IGI Global*, 2010.

[12] Murthy, C. S. R.,Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON,ISBN 81-317-0688-5, (2011).

[13] “Cryptography” Internet: https://en.wikibooks.org/wiki/Cryptography/Introduction

[14] H. Darrel, H. Julio Lopez and M. Alfred, "Software implementation of elliptic curve cryptography over binary fields", *Springer*, pp. 1--24, 2000.

[15] 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,, april 2008, pp. 1229 1237.

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

[17] Y. Jiang, M. Shi, X. Shen, and C. Lin, ”Bat: A robust signature scheme for vehicular networks using binary authentication tree,” Wireless Communications, IEEE Transactions on,, vol. 8, no. 4, pp. 1974 1983, april 2009.

[18] 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, nov. 2007.

[19] C. Giorgio, P. Panos, H. Jean-Pierre and L. Antonio, "Efficient and robust pseudonymous authentication in VANET", *ACM*, pp. 19--28, 2007.

[20] B. Dan and S. Hovav, "Group signatures with verifier-local revocation", *ACM*, pp. 168--177, 2004.

[21] B. Bhargav, "Certificate assignment strategies for a pki-based security architecture in a vehicular network", *IEEE*, pp. 1--6, 2008.

[22] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks", *JCS*, vol. 15, no. 1, pp. 39-68, 2007.

[23] J. Chae Duk, S. Chul, P. Youngho and R. Kyung-Hyune, "A robust conditional privacy-preserving authentication protocol in Vanet", *Springer*, pp. 35--45, 2009.

[24] A. Wasef, Yixin Jiang and Xuemin Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks", *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533-549, 2010.

[25] C. Li, M. Hwang and Y. 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.

[26] A. M, S. B and K. CK, "An elliptic curve cryptography based authentication and key agreement protocol for wireless communication", *Citeseer*, 1998.

[27] M. SS, K. MS and A. DG, "Message authentication in vehicular ad hoc networks: Ecdsa based approach", *IEEE*, pp. 16--20, 2009.

[28] Qi He, Dapeng Wu and P. Khosla, "The quest for personal control over mobile location privacy", *IEEE Commun. Mag.*, vol. 42, no. 5, pp. 130-136, 2004.

[29] C. Yang, Y. Tang, R. Wang and H. Yang, "A secure and efficient authentication protocol for anonymous channel in wireless communications", *Applied Mathematics and Computation*, vol. 169, no. 2, pp. 1431-1439, 2005.

List of Publications

Accepted:

[1] Rajeev Singh, Sumit Miglani, "Secure and Efficient Message Transfer in VANET," International Conference on Inventive Computation Technologies (ICICT 2016), August 26-27, 2016.

Video Link

[1] https://youtu.be/ZsK_zERVjUU

Plagiarism Certificate

plag_test

ORIGINALITY REPORT

14%	9%	9%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	airccj.org Internet Source	2%
2	www.reverse-engineering.info Internet Source	1%
3	Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering, 2010. Publication	1%
4	dspace.nitrkl.ac.in Internet Source	1%
5	X. Shen. "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", 2008 Proceedings IEEE	1%