Enhancement of secure data transmission in VANETs (Vehicular Ad-hoc Networks)

DISSERTATION-II

Submitted in partial fulfillment of the
Requirement for the award of the Degree
of

MASTER OF TECHNOLOGY IN
Electronics and Communication Engineering

By

Misbah Shafi (11612907)

Under the Guidance of
Ms. Jyoti Kohli
Assistant Professor, L.P.U

School of Electronics and Electrical Engineering
Lovely Professional University
Phagwara, Punjab

December, 2017

CERTIFICATE

This is to certify that **Misbah Shafi** bearing Registration no. 11612907 have completed objective Base Paper implementation of the thesis titled, **"Enhancement of secure data transmission in VANETs"** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of thesis has ever been submitted for any other degree at any university.

JYOTI KOHLI
Assistant Professor
School of Electronics and Communication
Lovely Professional University
Phagwara, Punjab

Date:
29th
Nov
2017

ACKNOWLEDGEMENT

I would like to express deepest gratitude and appreciation to my parents for their encouragement and endless support. I would like to take this opportunity to express heartfelt gratitude to my guide, Ms. Jyoti Kohli for her excellent guidance, encouragement, constant support, suggestions, and patience and help to complete my research. She has contributed towards my understanding and I have learned a lot from her. She inspired and motivated me from time to time to work in this field of research.

Last but not least, I would like to acknowledge with much appreciation to all those who gave me the possibility to complete this work. I also would like to thank to all my postgraduate friends who motivated, encouraged and helped me.

I am also indebted to all authors of the research papers and books referred to, which have helped me in carrying out the research work.

Misbah Shafi

Reg. No: 11612907

DECLARATION

I declare that this report entitled “Enhancement in secure data transmission in VANETs (Vehicular Ad-hoc Networks)” is the result of my own research except as cited in the references. This report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Misbah shafi

Reg. No.
11612907

ABSTRACT

Vehicular ad hoc network (VANET) is a prominent type of a Mobile ad hoc networks (MANETs) in which network terminals are mostly road vehicles. It provides an efficient mechanism to enhance the safety for vehicle passengers, drivers and to the public and enables to improve traffic management techniques. It establishes distant communication between vehicles, roadside infrastructure units and traffic management centers. VANETs provides a great significance in accessing an enormous variety of applications to the vehicle passengers. With its increase in number of applications and services provided by it, it is also associated with an increase in susceptibility of vulnerable attacks in inter-vehicular communications and services resulting an increase in number of threats and security attacks. It has been evolved as operative field of exploration, standardization, progress with an extreme capability to enhance road, vehicle and passenger safety, traffic efficiency, ease as well as amenity to drivers, passengers, and public. This dissertation is dedicated to establish an organized and thorough summary of the previous research advances on security of VANETs and perform simulations accordingly to overcome the limitations.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER - 1
INTRODUCTION

1.1Introduction

Due to the rapid increase of numerous kinds of uncountable applications of internet, one of the demanding requirement is the internet access for vehicles such as car navigation using global positioning system (GPS), and web browsing etc. The vehicular ad hoc network (VANET) is meant for this purpose, enables vehicles to have the capability to access the internet by establishing a communication between vehicles and the communication between vehicles and infrastructure. Since there are several techniques that can be used to provide the internet access to the vehicles. One of such techniques are cellular based access techniques which involves third generation, long term evolution etc. Although these techniques can provide secure and widespread internet access but these techniques cannot fulfill rapid increase of mobile data traffic and are costly. Thus we switch over to next technique involving wireless local area network (WLAN) systems (e.g., WiFi). This system provides various advantages in terms of cost, performance etc. as compared to other techniques. Also recent research has evolved that mobile vehicles using WiFi can access internet via Wifi hotspots [1]. Therefore, Vehicular Ad hoc Network is defined as a network in which user vehicles are furnished with a service of information exchange with other adjacent vehicles wirelessly by making use of transceivers. For those vehicles that are not in a direct communication range, data exchange occurs via neighboring vehicles as shown in fig 1.1[2].

Figure 1.1 : Segment of road in VANETs

Vehicular ad hoc networks (VANETs) provides various interesting features because of attracting applications such as collision avoidance systems, driving assistance systems etc. It allows people to access internet, share information to other people by making use of active data

streaming. It secures and supports the exchange of data which permits applications that can save lives such as position based navigation applications, path combination based information applications etc. Exclusively it also provides various advantages such as; de-acceleration warning, congestion detection, public safety applications, traffic management applications, traffic coordination and assistance applications, traveler information support applications, broadband services etc.(see fig 1.2)[3]

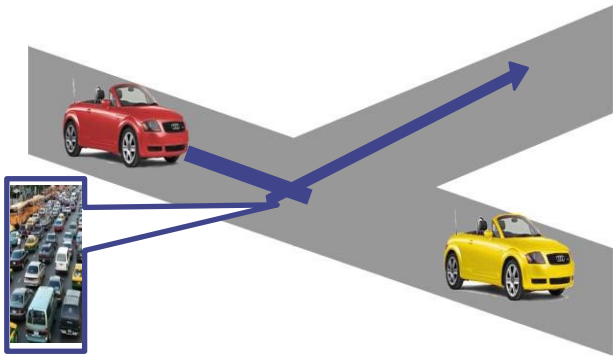

Figure 1.2 congestion detection using VANETs

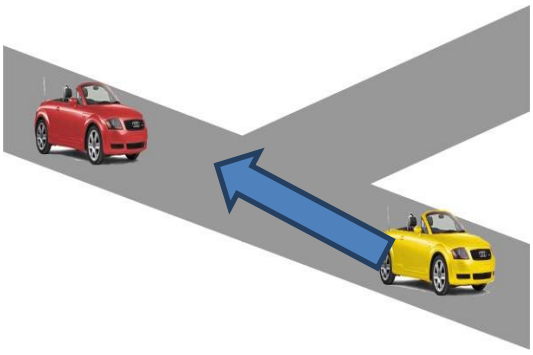

Figure 1.3 de-acceleration warning

Irrespective of these numerous advantages VANETs, it is also associated with several challenging characteristics specifically in the field of privacy, security and large scale rapidly changing topology. Due to less enhanced authentication features there is a lack of authenticated data present in the network which increases the chance of malicious attacks and abuse of services, therefore can impose a threat to the public, passengers and to the drivers. These challenges can overcome by improving primary security essentials such as; integrity, authenticity and availability needs to be properly developed before implementing it practically [4]. Each vehicle in the network consists of a set up known as on board unit (OBU) used for the purpose of integrating the functionality of vehicle in wireless communication, embedded systems, micro-sensors used for sensing various environmental conditions, Global positioning system used for the purpose of providing positioning information of the vehicles. Vehicles involved in this network can not only communicate with each other but also with other infrastructural units including road side units (RSU) such as; traffic lights, traffic signs etc. results in an improvement in safety and driving experience of the participating drivers. The messages that are exchanged between vehicles are concerned to provide real-time traffic conditions to make the drivers aware about present knowledge of driving environment in order to make a proper mechanism for rare situations as quick as possible [5].

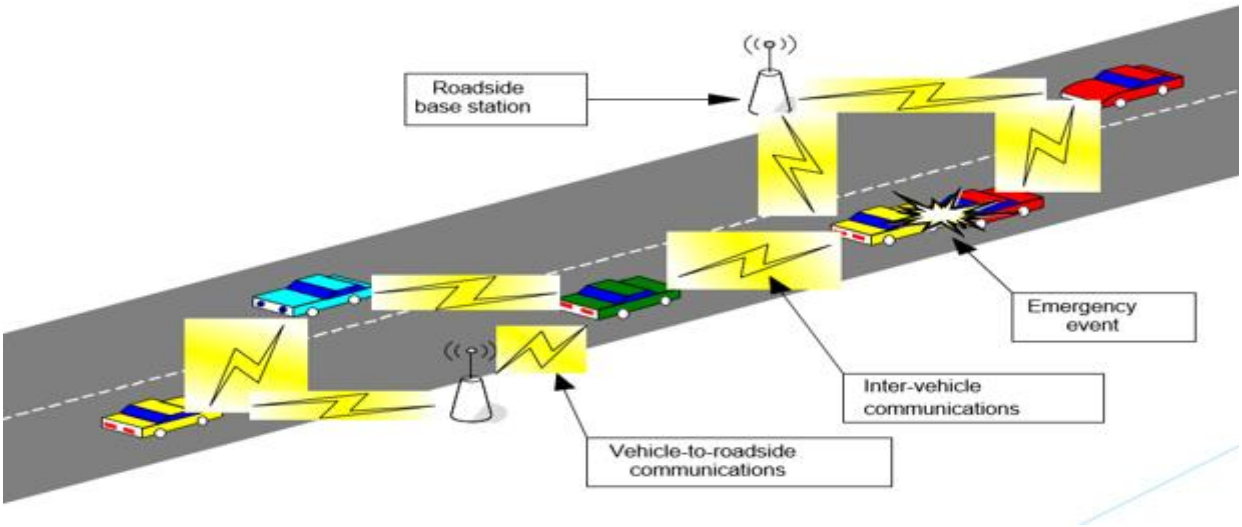

Figure 1.4: Overview of VANETs Vehicular ad hoc network)

1.2VANETs (Vehicular ad-hoc networks) Architecture

This portion gives the detailed architecture of vehicular ad-hoc networks. On the basis of domain the basic components of VANETs architecture is explained first followed by network architecture and then the communication architecture. Referring to the IEEE1471-2000[10,11] and ISO/IEC42010[12] architecture guidelines and standards, VANETs system architecture can be divided into following three domains:

- Mobile domain.
- Infrastructure domain.
- Generic domain.

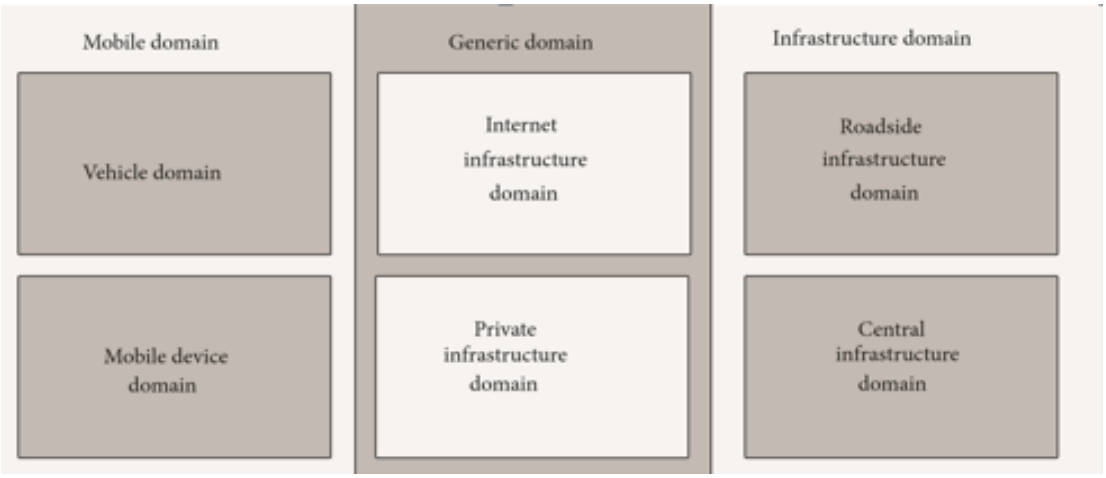

Figure 1.5: Domain architecture.

- Mobile domain

  It is further divided into two parts: the mobile device domain and the vehicle domain. The mobile device domain consists of all types of portable devices smart phones and personal navigation devices. The vehicle domain consists of all types of vehicles like buses, cars etc.

- Infrastructure domain

  It is further divided into two parts: the central infrastructure domain and the roadside infrastructure domain. The central infrastructure domain consists of vehicle management centres and infrastructure management centres for example traffic management centres (TMCs).

- Generic domain

  It is further divided into two parts: the internet infrastructure domain and the private infrastructure domain [6].

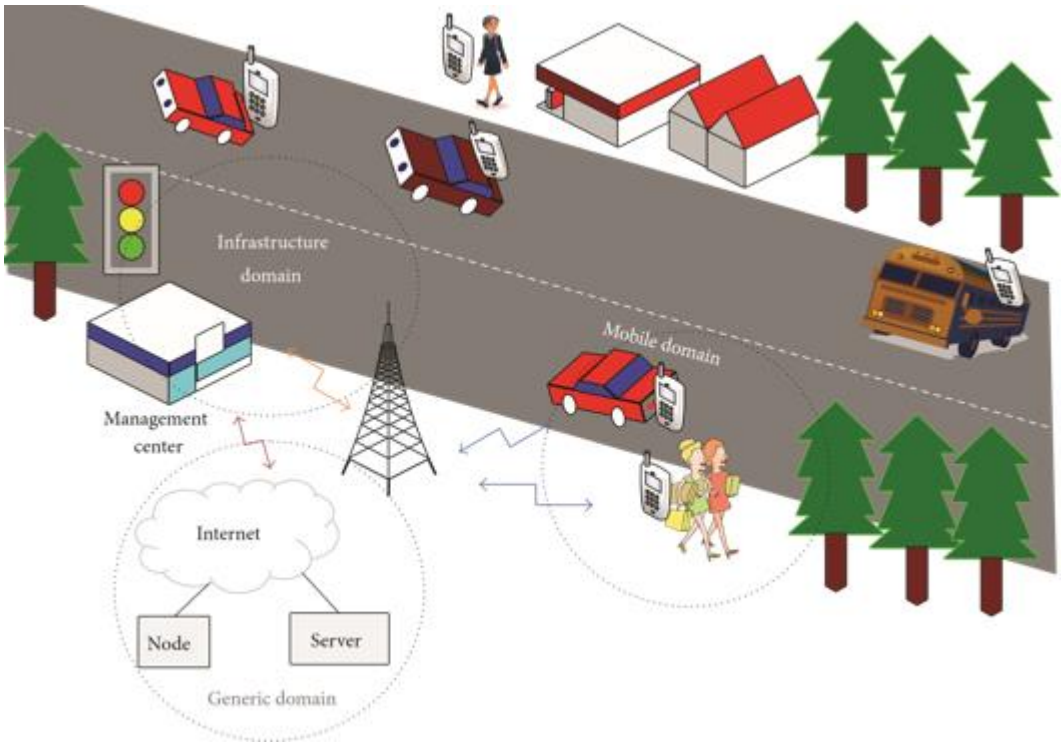

Figure 1.6: Domain Architectural view of VANETs

Though the growth of architecture of VANETs varies from one region to another. Figure 1.5 depicts the fundamental network architecture of VANETs.

It has the following basic components:-

1. On board Unit (OBU) equipped on vehicles.
2. Road Side Unit (RSU) distributed over the infrastructure of the network.
3. Trusted Authority(TA)

Communication can take place between vehicles that is vehicle to vehicle and between vehicle and infrastructure. Each vehicle's on board unit consists a group of sensors to obtain the information such as velocity, breaking information etc. Roadside unit acts as a router to cover wider area as compared to that of the area covered by vehicles. Vehicles are equipped with global positioning system to provide the information related to the positioning of the vehicles, electronic license plate (ELP) to provide the information related to the identification of the vehicles, (RADAR) radio detection and ranging or light amplification by stimulated emission of radiation (LASER) can also be used to provide the information related to the positioning of the vehicles. The trusted authority equipments are equipped in the back end. The on board units and road side units communicate in a wireless manner using Dedicated Short Range Communications protocol with an operating bandwidth of 75 Mhz at 5.9 Ghz frequency. Each roadside unit is connected with each other which in turn are connected with the Trusted Authority (TA) by means of a wired connection. The Trusted Authority maintains the VANET system model.

1. **On board Unit (OBU):-** On Board Unit (OBU) is a transceiver equipped on vehicles for the exchange of information with the transceivers (OBU) of other vehicles including the computational device and with the Road Side Unit (RSU). The basic components of an OBU are resource command processor (RCP) for the purpose of computation, storage and retrieving of an information, DSRC (Dedicated Short Range Communication) based on a radio technology IEEE 802.11p standard for the purpose of wireless communication. OBUs obtains its power from the battery of a car. Each vehicle is equipped with sensors such as Global Positioning System (GPS) receiver, Event Data Recorder (EDR), Tamper Proof Device (TPD), forward and rear sensors to provide the input to the OBU, speed sensors etc. The sensors obtain the information from the surroundings of the vehicle, GPS receiver provides the information about physical position of the vehicle. The Event Data Recorder (EDR) records the information of vehicle crashes or accidents. The Tamper Proof Device (TPD) stores the critical data including private key, identification proof of vehicles and group key. The speed sensors obtain the information related to the velocity of the vehicles.

The forward and rear sensors collect the information related to the activities occurring around the vehicle by monitoring in the front and back side of the vehicle. This collected information is then forwarded as a message to the neighboring vehicles by making use of wireless medium.

2. **Road Side Units (RSUs):-** These are usually stationary, these devices are fixed on the sides of the road or on the specific places such as road curves, parking places etc. It consists of an antenna, sensors, processor, and transceiver. These units on the sides of the road provide the services to the vehicles such as, road intersection is used to control the traffic in that particular intersection and to reduce accidents. Each RSU makes use of directional antenna or an omnidirectional antenna for the purpose of wireless communication based on DSRC (dedicated short range communication) IEEE 802.11p technology. To transmit a message to a particular location RSU makes use of a directional antenna. RSU possesses the capability of storing information obtained from OBU of vehicles and from the TA (trusted authority).
3. **Trusted Authority (TA):-** It is meant for the registration of RSU, vehicle users and the OBU of vehicles. It verifies the authentication and authorization of OBU of vehicles and vehicle users in order to prevent the entry of malicious vehicle into the VANET system. It provides high capability of storage and computation. It possesses the ability to uncover the real identity of OBUs when malicious messages are being broadcasted or when it shows a malicious behaviour [7].

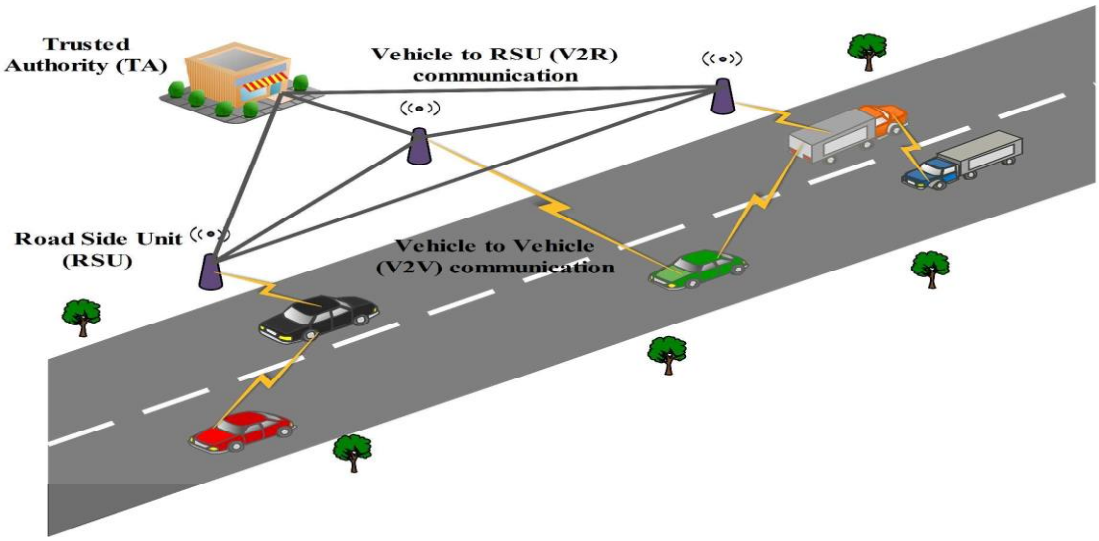

Figure 1.7: Network Architecture of VANET system.

1.3 Communication Architecture

Communication taking place in VANETs can be classified into following four categories. This type of an architecture describes the functions of communications occurring in VANETs system.

1. **In-vehicle communication**

   It refers to the communication in vehicle domain. It is responsible of collecting an information related to the vehicle's performance. It detects the exertion, drowsiness etc. of the driver meant for the safety of public, passengers, and the driver himself.

2. **Vehicle to vehicle communication (V2V)**

   It refers to the communication between vehicles for the exchange of information including warning messages etc. between them. This type of communication provides an assistance to the driver.

3. **Vehicle to roadside infrastructure (V2I) communication**

   It refers to the communication between vehicles and infrastructural units. It provides the information related to the current updates of weather, traffic etc. it possesses the ability to monitor and sense environmental conditions.

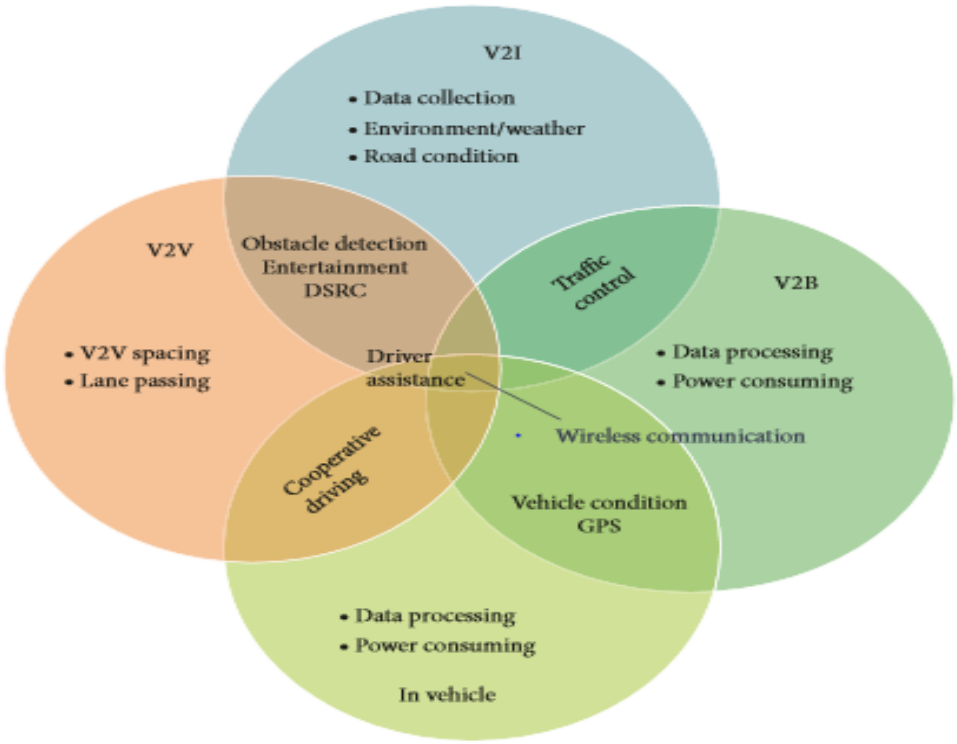

Figure 1.8: Key functions of each communication types.

4. **Vehicle to broad cloud (V2B) communication**

   It refers to the communication between vehicles by making use of broadband (for example 3G or 4G). It includes the traffic information, monitoring data etc. This type of communication provides the real-time and an active assistance to the drivers and is also responsible for vehicle tracking [6].

1.4 VANETs (Vehicular ad-hoc Networks) applications

VANET based communication can used tremendously in numerous applications. It provides the capability to handle highly diverse requirements. Under broader sense applications of VANETs can be broadly classified into three categories which are safety directed, convenience directed and commercial directed.

Safety directed applications monitors the surroundings of the road, vehicles, curves of the road etc. Convenience application involves the management of the traffic. Commercial applications handles services provided to the driver. These services include the service of entertainment, web services, streaming of audio and videos etc. Based on the representation and requirement of applications, certain applications are identified below:-

1. **Traffic signal**

   It is possible to create a communication from the traffic lights by making use of technologies embedded in VANETs. Slow or stop vehicle advisor (SVA) meant for safety applications provides an information about the slow or motionless vehicle by broadcasting alert messages to their neighborhood. In order to notify the road congestion, congested road notification (CRN) detects the road congestion, on the basis of which journey and route is being planned.

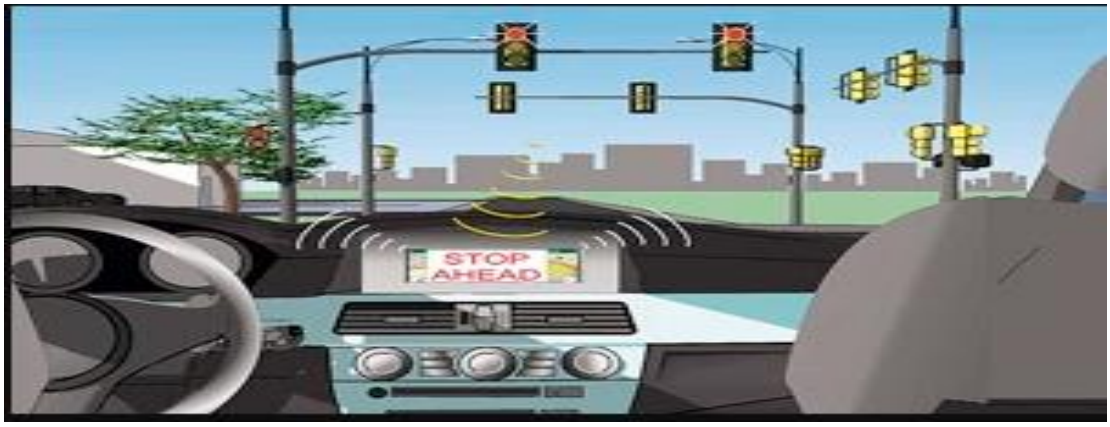

Figure 1.9: Traffic signal control.

The toll collection at the toll booths without interrupting the vehicles is another type of application of VANETs. Vehicular networks are particularly useful in management of traffic. However VANETs for the road tolling is widely deployed.

2. **Weather and other hard conditions**

   It consists of vehicle sensors such as wiper movement sensor, thermometer present outside to collect and update the weather information by making use of an application through DSRC (dedicated short range communication). During an accident, when a vehicle is involved in an accident a warning message is being generated which would be broadcasted to the nearby travelling vehicles so that this information is passed on to the highway patrol for support. It also provides us the capability to notify the space availability in a parking lot for a specific geographical area by making use of Parking Availability Notification (PAN). It also possesses maps of highway and urban areas in order to avoid the traffic jam, conditions for an accident and to provide the shortest path in critical situation leading to an efficient usage of time.

3. **Vision enhancement**

   It provides the clear view of vehicles and obstacles and enhances the vision during the heavy fog conditions. It provides an ability to the drivers to recognize the existence of vehicles hidden behind obstacles, buildings and by other vehicles.

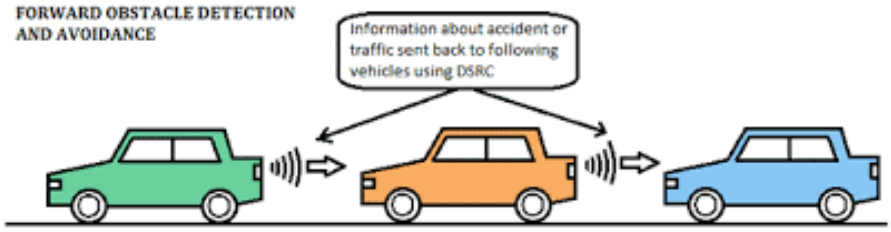

Figure 1.10: Obstacle detection.

4. **Assistance to the Driver**

   VANETs provide the ability to support exercises in military driving by giving an information to the drivers. Since vehicles may exhibit driving patterns in an abnormal way including dramatic change of direction, broadcast message to inform cars that are present in their locality, therefore, drivers can be warned by letting them know about the potential hazards in order to prevent accidents and get time to react. Thus, provides a

support to the driver in decision making.

5. **Automatic parking**

   This type of application involves parking of a vehicle itself without any need of driver's interference. In order to perform such an action a vehicle needs an installation of distance estimator, a sub meter precision and a localization system.

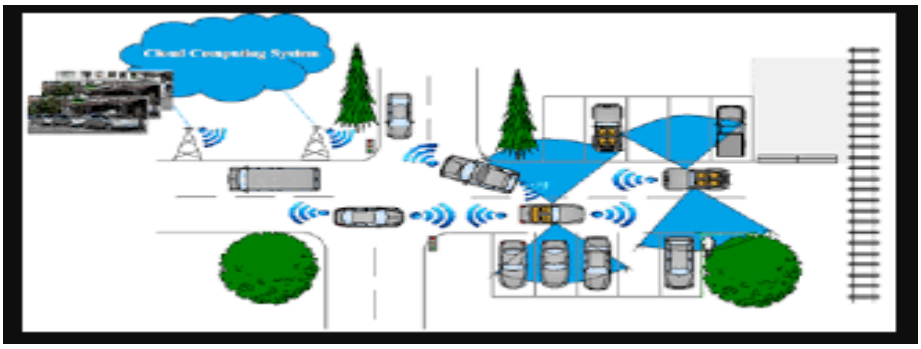

Figure 1.11: Automatic parking using VANETs.

6. **Information of roadside locations**

   It provides the ability to search roadside location and also provides the direction to the vehicles. Thus, for passengers which are unknown to any particular location helps them to find the specific location (for example; shopping centres, hotels, hospitals, etc.) in that area. It makes the use GPS, database from the nearest roadside base station, sensors makes them able to perform such functions by calculating information.

7. **Entertainment**

   Since number of applications are involved to make the entertainment of passengers who are going to spend a long time in travelling. Entertainment is provided in the form of internet access, communication between passengers in car's vicinity, games.

8. **Safety**

   It involves collision warning, obstacle detection and prevention, road condition warning, cooperative driving (such as lane merging warning), sign movement assistance, collision prevention of highway or railway, turn assistance, changing of lane warning.

Figure 1.12: Traffic management control to provide safety.

Table 1.1 indicates the comparison among various applications based on latency, priority, message transmission range and network traffic. Since main applications of VANETs comes under safety applications and non-safety applications. Safety applications involve the communication that are of broadcasting mode while as non-safety applications are based on demand and request response and includes gaming, internet surfing, multimedia etc.[8, 9].

Table 1.1 : Comparison of various applications [8].

Applications	Priority	Network Traffic	Allowable Latency (ms)	Message Range(m)
Life-Critical Safety	Class1	Event	100	300
Safety Warning	Class 2	Periodic	100	50-300
Electronic Toll Collection	Class 3	Event	50	15
Roadside Service Finder	Class 4	Event	500	300
Automatic parking	Class 4	Event	500	300
Internet Access	Class 4	Event	500	300

1.5 VANET Protocols

VANET possesses certain characteristic features including highly mobile road topology, size of the network in an unbounded form, support of infrastructure differentiating it from MANETs. The main aim of routing protocols is to obtain an optimum paths from the point of source node to the point of destination node with an ability to possess minimum overheads in various verticals. On the

basis of various categories such as underlying architecture, scenario etc. routing protocols can be categorized into the following six types in VANETs as described below [20, 22]:-

Routing protocols based on topology

These types of protocols are used to create and maintain the route before the sender is able to start the transmission of data. These types of protocols are classified as: proactive protocols, reactive protocols, hybrid protocols [22].

- **Proactive protocol**

  The proactive routing protocol indicates information of routing including the information about forward hop maintenance in spite of the requests occurring during communication at the background. It provides the information about the topology, to all the nodes prevailing in the network. It provides a great efficiency to all the applications requiring low latency. One of the disadvantage of this protocol is that it provides low inactiveness in case of constant applications. [21]. This protocol is based on standard strategies of distance-vector routing, link- state routing. It updates and maintains the routing information between all the nodes present in a network, even the information about the paths that are not in use currently. This route information updates are performed periodically regardless of bandwidth constraints, size of network, load of the network. The major drawback of this approach is that it occupies a notable amount of available bandwidth for the maintenance of unused paths [14].

  There are various routing protocols based on this type of a protocol as shown below:-

- **Optimized Link State Routing Protocol (OLSR)**

  It provides routes when required that is; routes are available always when needed. It provides an optimization of link state protocol used for the purpose of mobile ad-hoc networks. Each node present in a network possesses the capability to select a particular set of neighboring nodes known as Multipoint relays (MPR) that provides the retransmission of its data packets. The neighboring nodes that are not included in multipoint relay set possess the ability of reading and processing the packets. It results in the reduction of requirements of retransmission in a broadcast manner [22, 21].

- **Fisheye state routing (FSR)**

  It possess the similarity with the link state routing protocol (LSR). Each node occupies a topology on basis of latest updated information obtained from neighboring nodes. It makes

use of varying exchange period for the purpose of different entries in case of routing table so that the size of messages are reduced in a large network. The major limitation of a FSR routing is that routing table size gets increased with an increase in size of the network. Discovery of a route fails if the source node is unable to find the destination node. However, because of high mobility of nodes in VANETs route recognition becomes less accurate [22].

- **Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)**

  This protocol is based on the link-state routing in case of ad-hoc networks. By making use of topology table every node is able to construct a source tree that includes paths towards all reachable nodes. Periodic updation of nodes takes place to make the nodes aware about current state, this process takes place by using a HELLO message. Thus, messages meant for routing are smaller and can be frequently sent to its neighbors [22].

- **Reactive Routing**

  These protocols are also known as on-demand that is ; discovering of node starts to take place If one node wants to communicate and send data on another node, thus periodic flow of data is not necessary. These protocols maintains only those routes which are in use currently, therefore decreasing the burden of the network. Since communication taking place between vehicles uses only a limited number of routes, thus it is suitable for application scenario.

  These protocols are classified as:

- **DSR (Dynamic Source Routing protocol)**

  This protocol is considered as the reactive or on demand protocol for routing. It makes use of multi-hop in wireless ad-hoc networks for the purpose of efficient routing and easily designed specifications. This protocol based network allows self-sorting and designing without the requirement of its existing organization base.

- **AODV (Ad-hoc On-demand Distance Vector)**

  This type reactive routing protocol is developed for the purpose of sending data in which nodes in a network acts as a router. It makes use of customary steering tables so that one section is meant for each destination. This protocol possesses a major advantage of making an overhead for the efficient use of bandwidth.

- **Dynamic MANET on Demand (DYMO)**

  This protocol is considered as the reactive or on demand, unicast, multi hop routing protocol. This protocol does not update information about routes periodically. It acts as a small memory that stores information of routing and makes creation of control packets during the reception of data packets from the path of route. Here this protocol is designed for ad hoc networks in which nodes suffer the disconnection of transmission frequently. It provides number of advantages that are well suited for sparse traffic and for the networks having large number of nodes.[21,22]

- **Hybrid protocol**

  This protocol involves the routing technique with elements better from reactive and proactive routing protocols. Table driven procedure is applied when the destination node are at specific distance [20]. It provides the combination of reactive routing protocols and proactive routing protocols together in order to decrease the overhead routing and delay because of disclosure of route process. The major advantage of this protocol is the enhanced scalability and higher efficiency. The major limitation of this protocol is the increased latency for the purpose of recognizing and locating new routes.

  It involves following protocols [21]:-

  a) **Zone routing protocol (ZRP)**

  This protocol involves division of network into several overlapping zones. Network of nodes in a zone radius forms a zone. Zone size is determined by the some parameters including radius of length ‘a’ where ‘a’ denotes the hop number to the zone perimeter. For an intra-zone communication proactive routing protocol is used and for an inner-zone communication reactive routing protocol is used. Data is sometimes directly sent to the destination when both are in the same zone of routing. It makes use of broadcast method for the purpose of multicasting query packets [22].

  b) **HARP**

  This protocol involves distinction of network into several non-overlapping zones. In order to overcome the problem of delay, a stable route is established from a source to a destination. It makes use of discovery of routes between zones to prevent flooding condition in the network and opt the most suitable route on the basis of stability. Here the routing takes place in two forms depending on the destination position.

i) Intra- zone

ii) Inter zone.

It makes use of reactive and proactive protocols in inter and intra zones respectively. Its major limitation is that it cannot support highly mobile ad-hoc networks thus is not applicable for higher mobility nodes.

1.6 Challenges of Vanets

There are certain kind of challenges that limits the characteristics of VANETs in numerous ways. These challenges reduces the efficiency of VANETs. These challenges are classified below:-

1.6.1 Dynamic change in topology of the network with frequent disconnection

Due to the frequent and rapid change in the movement of vehicles, topology of the network also changes frequently. In a network, connections are meant for the exchange of information or data packets. But because of the rapid and frequent change of speeds of the vehicles, maintenance of the established connection is very difficult. Network topology also changes when an immediate neighboring node present in the network moves out of the range for wireless transmission. In this scenario the current sending or source node needs to look for some other node in order to make connections in the network. There are some situations where the source node is not able to detect the neighboring node for the purpose of continuing the network connections. This kind of case arises when the neighboring node density is quite low or the nodes are not in the range of transmission. This problem can be solved by pre-deploying various relay nodes across the roads for maintaining the connectivity in the network.

1.6.2 Computing capabilities of energy and storage

Since each node in the network of VANET should possess the large amount of capacity to store and process the received data from the neighboring nodes. For the proper processing and storage of received data or transmitting data nodes must be equipped units that of power generation and data storage. Electric power is being generated by the rechargeable batteries equipped in the vehicles.

1.6.3 Geographical location of vehicles and communication

Vehicles are required to be equipped with GPS (Global Positioning System) receivers in order to provide the information about the location of vehicles for the support of communication with the neighboring vehicles present in that particular geographical area.

This is also helpful in routing packets and forwarding them to other vehicles.

1.6.4 Different communication environments

Vehicles need to perform their functions in various environments surrounded by various building blocks, building constructions, highways preserved with fast, slow or stopped traffic. Vehicles need to encounter each environmental scenario to establish a wireless communication in VANETs.

1.6.5 Real- time transmission and delay constraints

Some of the vehicles are equipped certain kind of sensors that can sense collisions, unexpected brakes, pre-crash. Such vehicles need to make alerts for other automated vehicles and drivers. Such situations are required to be handled in an accurate manner by providing the information without delays, as delays may result in accidents and collisions

1.6.6 Variable network density

Density of networking nodes varies from one location to another location. Density of traffic will be predominant in various scenarios such as traffic jam, traffic in the morning etc. and less in other situations such as traffic in nights etc. vehicles need to function properly in these varying densities [20].

1.6.7 Privacy and security

In Vanet, privacy and security is one of predominant issue in communication between various nodes for various purposes through wirelessly. An unauthorized node can create a decrease in the performance of the network, networking vehicles, passengers and can misuse the information corresponding to that of the network. Besides the trade-off between the privacy and security is one of biggest challenge in maintaining the efficiency of the network [6].

1.6.8 Quality of Service

Maintaining QOS is another significant challenge due to various reasons such as highly dynamic topology, high mobility, out of range for the transmission or reception to occur, frequent disconnections. Requirements for maintaining QoS is to maintain the parameters such as available bandwidth, transmission success ratio, delay jitter, packet delivery ratio, throughput etc. these parameters are mathematical properties for considering the quality classified broadly as multiplicative, additive, concave. It is a research challenge issue to possess adaptability, capability of self-configuration and utilization of resource available

for maintaining QoS in bandwidth.

1.6.9 Routing protocols

Traditional protocols of routing are not appropriate because of the highly dynamic topology which needs to be promoted in the field of research of routing data packets with efficiency up to the maximum including effective utilization of energy resources, efficient throughput, better utilization of available bandwidth, efficient packet delivery ratio, and minimum hop count.

1.6.10 Broadcasting

Protocols of broadcasting plays an significant role in various situations of VANET such as information of traffic, information of weather, emergency information, alert message before collision, sudden brakes, information of road condition, advertisements etc. these protocols are required to be rapidly executed, robust and reliable in safety applications in order to provide necessary information to drivers and other vehicles within the time limits. These protocols are required to be able to broadcast the information related to the safety in both low and high density in VANETs.

1.6.11 High speed Wireless Communication technologies

High speed wireless technologies of communication is another essential issue in VANETs for the purpose of supporting fast speed of vehicles in the network. Since numerous cellular technologies can be used to communicate with enhanced abilities of communication and bandwidth such as 2G, 2.5G, 3G, 4G. but it will result in the high cost, latency, limited usage of bandwidth, lack of broadcast communication etc. therefore these up-graded technologies were not considered as base for communication in VANETs.

1.6.12 Architecture

Reliability and flexibility of an architecture is yet an another necessary aspect in designing an integrated system for the architecture of VANETs as there is a possibility of up-grading the system, which may result in the combination of various technologies such as WiMAX, WiFi, radio spectrum 5.0, DSRC IEEE 802p, Bluetooth, WAVE, IRA,3G/4G , ITS G5, and heterogeneous vehicular networks.

1.7 Requirements of security in VANETs

Requirements of security are the estimations that determines the extent of secure network. The prevalent requirements of security include authentication, integrity, availability, confidentiality, non-repudiation, data verification, privacy. The absolute characterization of these security requirements are mentioned below as follows [5, 16, 26].

1.7.1 Authentication

Authentication in VANETs ensures that the message is actually signed and sent by a registered authorized vehicle of a system without any modification. It guarantees that produced message is sent by an approved member of the system.

1.7.2 Integrity

It means the ability of not altering or modifying the sent information (message) without an authorization by an unauthorized user from the time this information was sent. The modification of this information can be done either intentionally in a deliberate manner by an active attacker or unintentionally in an accidental manner, because of the faulty devices present in a vehicle. Integrity ensures messages or information are not altered by an assailant.

1.7.3 Availability

It indicates that the system must be approachable to the verified member of the system anyhow devoid of attacks or being utilized in many ways by an attacker.

1.7.4 Confidentiality

It defines the capability of a system to stop and prevent the access of sent message or an information to an unauthenticated and illegal users.

1.7.5 Non-Repudiation

It defines the ability in which a node whether in a sending mode or receiving mode can prove that the transmission or reception of information or massage from a node and is able to prevent the node from denying its transaction [25, 26].

1.7.6 Data verification

It provides the capability to a node that message or information sent by the sending node is confirmed and the receiving node confirms this received information or message by a confirmation check to know whether this received information or message is ruined or not [5].

1.7.7 Privacy

It denotes that the data concerned with the driver i.e; an individual data must not be available to the unauthenticated vehicle [32, 36].

1.8 VANET attacks

This section summarizes the various types of attacks on the security of VANETs. Attacks in VANETs are widely divided into three main classes viz attacks that create a menace to availability, attacks that impose menace to authenticity, those attacks that create a menace to confidentiality [3, 7, 14].

1.8.1 Menace to availability

a) Black hole attack

It is that type of an attack where an area is formed where nodes discard to take part in the network or where participant node drops out from the established network resulting in the loss of data packets. Whenever the node drops out from the established network, all routes made by this node are broken which results in the failure of propagating information or messages.

b) **Denial of service Attack**

It is that type of attack where the attacker sends number of dummy messages to other participating nodes and RSU to create congestion in the channels, which results in the reduction of performance and efficiency of the network. This type of attack is carried by network participants or network non-participants [23].

c) Distributed Denial-of-Service

This type of attack is similar to the denial-of service attack. Here several malicious nodes take part in the attack on the confirmed node. Usually these attackers participate per time slot in the attack.

d) **Spamming**

An attacker attacks the network by creating the presence of spam messages that demotes the latency of transmission and creating jam and delay of propagating information.

e) Malware

This type of attack involves the introduction of malware which includes viruses or worms in the network. This causes the critical reduction in performance of VANET. This type of attack is usually executed by network participants and is introduced in the network when RSU and OBU software updating is performed.

f) **Broadcast tempering**

A network participant acts as an attacker, who introduces fake safety messages in the network to create serious damages including accidents that occurs because of traffic warnings or to manage the traffic flow along a particular route.

1.8.2 Menace to Authenticity [11, 18]

a) Replay Attack

It is an active type of an attack where the malicious attacker re-introduces the already received message or information in the network. Here the attacker saves the received packet and uses it further for replaying that is; sending the same packet again and again creating an unnecessary route changes, stopping and traffic jams [30].

b) Masquerading

It is an active type of an attack where an attacker personifies itself as a legitimate and confirmed participant of the network by providing fake ID. It attacks the network. The attackers acts as a 'man in the middle' between two communicating vehicles and obtains the information, further can modify the information before forwarding it to the other vehicles [15].

c) Global Positioning System (GPS) Spoofing

In this attack an attacker creates the false reading of vehicles on global positioning system devices by making use of Global Positioning satellite simulator that generates stronger signals, which are more powerful signals than those generated by genuine satellite. This attack results in traffic jam and fake position representation of vehicles [27].

d) Sybil attack

This type of an attack is an active attack where a malicious attacker in the network pretend and claim of being multiple nodes and connects the network. Thus operation of the network becomes insecure and the attacker possesses the ability to divide the network and can make the transmission of event driven safety message restricted [29].

e) Tunneling

In this type of attack the malicious attacker takes an advantage of momentary loss of information about the position of the vehicle whenever a vehicle takes an entry in the tunnel. When this vehicle is about to receive the authentic information about the position the malicious attacker introduces the fake information into the OBU.

CHAPTER 2
SCOPE OF STUDY

Since the rate of increasing vehicles increases day by day, therefore there is an increase in the probability of accidents. Conferring from the NHTSA (National Highway Traffic Safety Administration), it has been observed there are approximately 43000 deaths per year, an average of 2.7 million injured people per year which amounts to a cost of $230 billion. Therefore, there is a requirement of making our vehicle intelligently active in order to respond towards the increasing probability of accidents. This mechanism is implemented in the vehicles by making the use of VANETs (Vehicular Ad-hoc Networks) based on DSRC (Dedicated Short Range Communication) and a standard of IEEE 802.11p WAVE (Wireless Access for Vehicular Environment). The standard of IEEE 802.11p based on WAVE (Wireless Access for Vehicular Environment) involves the allocation of band of spectrum for DSRC (Dedicated Short Range Communication) as 5.9 GHz, having a bandwidth of 75 MHz operating in an 1000m of approximate range. The basic fundamental aim of IEEE standard 802.11p and DSRC is the outlining of rules for recognition of fast network, distinction of applications for emergency use and normal use and connection setup with minimum delay. This results in the effective communication between vehicles during an emergency. We can take an example of an information exchange between vehicles in case of an accident, where message of alerting is transmitted between vehicles is required be much faster which is controlled by the infrastructural unit. However, the communication between vehicles must be secured, as the VANET security is an essential aspect, as its presence re-counts the situations which are critically threatening to life. It is domineering that the fundamental information that is to be communicated must not be modified or introduced by the malicious attacker. The system is required to be capable of determining the liability and maintaining the privacy of drivers that are participating in the network. Another aspect in addition to that of the traffic safety and is the improvement in the efficiency of the traffic by making use of the effective communication between vehicle which can be affected by the computational time required by the vehicle to execute the communication occurring between vehicles or between vehicle and infrastructural unit. To execute such a secure provision in Vehicular Ad-hoc networks (VANETs), it is mandatory to perform the authentication procedure of vehicles. Furthermore, the confidential information of a vehicle can be

leaked during the process of setting up the communication. A security mechanism is required to make the system devoid of such leakage of information. These troubles are complicated to solve due to limited boundaries of the VANETs such as size of the network, vehicle speed, geographical position of the vehicles, and connectivity randomness between the nodes. Therefore, we are proposing a mechanism which provides an efficient and effective security mechanism to fulfillment the necessities including authentication, processing speed, confidentiality, integrity, privacy, power consumption, and authorization for the protected communication between nodes. The major factor that is mandatory to be taken into consideration is the high mobility of nodes in VANETs (Vehicular Ad-hoc Networks). There are several types of attacks in contradiction of the messages that are to be communicated are: Bogus information attack, replay attack, Denial of the service attack etc. The reliability and consistency of a system where information that is to be communicated is first gathered and then shared among various nodes of the VANETs creates a concern towards the authenticity of the vehicles. A malicious attacker can transmit misrepresented observation to obtain the benefit such as encouraging other vehicles not to opt a particular route by sending a false observed report of jammed desired route by traffic, thus offering a less congested road of the desired route. Also, malicious node can impersonate the identity of authenticated vehicles to generate safety hazards. Vehicles that participate in the network can reduce this threat by making use of proper authentication mechanism by which nodes follow a proper procedure of authentication and create a trusted network enhancing the capability of resisting the maximum attacks and providing the security to the VANETs (Vehicular Ad-hoc Networks). There are most probable frameworks of VANETs which are creating the widespread research region with an availability of extensive number of cases that are to be implemented. The qualities of VANETs stands both problems and opportunities in achieving secure transmission of information.

CHAPTER 3
OBJECTIVES OF STUDY

3.1 Introduction

This chapter discusses about the leading objectives that effectively influence the quality of service in the operating network of VANETs. Furthermore, it is already mentioned in chapter-1 defining fundamental challenges in VANETs that are currently existing in day-to-day scenario. Among them following limitations are considered and are taken into consideration to overcome the degradation of the efficiency in the operating network of VANETs.

3.1.1 Secure

It implies that the individual data to be transmitted and received must be kept up secured against the unauthorized vehicles and is required to be protected to prevent loss of confidentiality. Secure communication in VANETs is one of the noteworthy issue that is required to be resolved. In order to preclude the attackers and confirm the integrity and confidentiality of the exchanging information between vehicles, these vehicular nodes are required to be authenticated by following proper authentication procedures and the encrypted transmission of messages. Most appropriate mechanisms are required to be followed that specifies the standardized algorithm for the secure exchange of message from one vehicle to another without affecting the other reliable parameters of the network.

3.2 Overheads

It is one of fundamental limitation that is needed to be omitted especially in case of VANETS where accuracy of time is essentially to be maintained. Overheads not only creates increased delay of communication but also makes loss of energy and power. One of the most significant way to reduce overheads is the introduction of clustering, possessing a potential to minimize the time of processing by decreasing the burden of certificate authority. As the nodes in VANETs are comparatively highly mobile and regular change of the topology of the network creates an instability of nodes, thus providing a tremendous increase of overheads. For such maintenance of the stability of the network clustering can reduce the overheads in a very significant way.

3.3 Power Consumption

One of the main factor that is required to be considered in VANETs, as the nodes are mobile, power usage must be limited to lower value. One of the important parameters that affects the power consumption is the processing which inturn is related to the computational time. Optimizing the network to reduce the number of overheads, computational time will ultimately result in the reduction of power consumption. We need to perform such mechanism that fulfills the significant requirements of security at a low usage of power, so that there will a significant progresses over the standard alignments for the use of power without any noteworthy loss in the QOS (quality of service).

3.4 Computational time

This parameter in VANETs is necessarily needed to be restrained as it effects the quality of service of the network. Computational time is required to be much condensed to provide the accurate transmission and prevent accidents. Since computation time can be defined as the total time required for the accomplishment of a computational process. There are several factors that affect the computational time of VANETs. Numerous approaches are defined that can improve the performance by decreasing the computational time, in case of VANETs computational time is mostly affected by the decision of routing and the encryption and decryption involved in data transmission.

CHAPTER 4
LITERATURE REVIEW

4.1 Introduction

This chapter will explain about the review of the works from other researchers that were related to the development and enhancement of VANETs, which is "Vehicular Ad-hoc Networks". The literature review is continuous part that should be done until this dissertation is successfully simulated with good enhanced results. Identifying the features, system architecture and the weaknesses from the existing system will enable the improvement on VANETs could be done in this thesis to produce a better and secure transmission in the operating network of VANETs.

4.2 Related study

J. Sun, C. Zhang, Y. Zhang and Y. Fang, 2010, proposed a mechanism, the trusted authority has an access of master secret key and master public key. The user gets its secret key from the trusted authority on the basis of its identity. The user is put to test for identification by the claimed identity and the master key. This mechanism differs in the sense that user validates message by signing it instead of verifying identity. Signature verification needs master public key and signer identity. [34] The concept of ID based mechanism is based on the use of known information representing user identity responsible for digital signature verification. This information may be an address of the network, email address, name of the user or these identities in combined form. This mechanism provides the generation of pseudonyms and can be altered when required. This mechanism also allows a user to make use of more than one pseudonyms. It provides various advantages over PKI, as trusted third party does not need the storage, fetching and verification of public key certificates, mitigates time delays and CRL cost. The main limitation of this mechanism is the problem of privacy. To generate a pseudonym it must be ensured that the pseudonym is valid to same entity only that generates it [38].

D. Huang, S. Misra, M. Verma and G. Xue, 2011 performed a mechanism allowing the nodes in VANETs to make use of pseudonyms instead of their respective real identity in order to obtain confidentiality and privacy in good range. In this mechanism vehicles communicate with infrastructure unit for the generation of pseudonyms for the occurrence of communication anonymously. This mechanism requires a set up in which pseudonyms are only identified to vehicle nodes and are unknown to the other entities in the network. This mechanism also possesses the capability for the revocation mechanism to occur efficiently so that the malicious vehicles could be identified and thus revoked from the network. This mechanism thus provides the privacy and confidentiality among the vehicles in the system as the vehicles appear anonymous to the malicious vehicles as long as they undergo revocation mechanism [21].

H. Sedjelmaci, S. M. Senouci and M. A. Abu-Rgheff, 2014, implemented a mechanism involves the implementation of a light-weight and efficient intrusion mechanism of detection and protection of the network against various kinds of attacks which includes false alarm generation, integrity attack, denial of service attack. This mechanism consists of a set of rules for the detection of malicious attackers accurately and quickly. It is based on a set of rules for detection for each attack to recognize and model behavior whether anomalous or normal behavior of a vehicle. It also enables to evaluate level of trustworthiness of a vehicle by observing behavior and the provided information by the vehicle. It starts with the process of estimating the number of detection intrusion agents which are placed within the range of radio link. As every vehicle in the network possesses the ability to recognize and activate an agent of intrusion detection to make a watch to its neighbors and to each attack apply rules of detection. This detection is based on detection policies consisting of rules corresponding to above mentioned attacks. At the end of the mechanism VBE (vehicle's behavior evaluation) protocol is presented with the capability to assign level of malicious behavior in the form of malicious level (ML) to the attacker vehicle. On the basis of ML(malicious level) vehicle can be grouped into one of below mentioned class:- trustworthy, untrustworthy node, uncertain node [22].

M. C. Chuang and J. F. Lee, 2014 proposed a mechanism, in order to overcome the previous limitations known as TEAM (trust extended authentication mechanism). In this mechanism an authentication takes place in a decentralized manner for communication between vehicles. Here procedures of authentication are performed without the existence of centralized authority. This mechanism makes use of only hash functions and XOR computations, therefore results in low computational cost. Inspite, of its low computational cost it compensates requirements of security as, Replay attack, problem of clock synchronization is omitted, man in the middle, privacy of location, anonymity, increased pace of error detection, resistance to attacks. Because of it less computations this mechanism requires only few space for storage as compared to other mechanisms. The vehicles in this mechanism does not require to store information about authentication such as public keys. Since vehicles in Vanets can be classified as Law executor (LE), Trustful vehicle (TV) and a Mistrustful vehicle (MV). As a Law executor, an authorized public transportation or a police car can be defined as a mobile authentication server (AS). The Law executor is considered to be trust worthy permanently. However, vehicles other than LE are considered to be trust worthy only if they are successfully authenticated, if not then are considered as MV. Also, a TV can become MV in case when the lifetime of a key over. A vehicle is required to register its OBU with the AS to join the Vanet. A vehicle must necessarily follow the log in procedure to access the service followed by the authentication state examined by the OBU. If the key lifetime is mitigated to zero, the vehicle is considered to be mistrustful otherwise not. This procedure is followed by the trust-extended authentication or general authentication procedure performed by MV. The key updation procedure is performed by TV with LE whenever the lifetime of a key falls below the beforehand threshold. The major limitation of this mechanism it is not resistible to inside attacks [37].

Lina Bariah, Dina Shehada, Ehab Salahat and Chan Yeob Yeun in 2015 have evaluated the necessity for enhancing VANET security by describing the measures of establishing a network which is secure. These measures of enabling the network to be secure must satisfy integrity, authentication, availability, confidentiality and non-repudiation. They have examined the several types of adversaries with a capability of effective abilities of

communication to intrude attacks of privacy and security in the established network. In addition to it they have explained the motivation of adversaries including revenge, money, intellectual challenges, and cyber warfare. Moreover, attacks taking place in VANETs involve traffic analysis, replay, snooping, repudiation, masquerading, spamming, tunneling, jamming, and Sybil attack. Since authentication and non-repudiation are the two main necessities for the accomplishment of the security, they have assessed the operation of two fundamental mechanisms of security such as PKI (Public Key Infrastructure) and ID-Based cryptosystem [3].

FengzhongQu, Zhihui Wu, Fei-Yue Wang and Woong Cho in 2015 estimated the progress in the VANET security by utilizing the security enhancing measures, requirements of privacy, measures of privacy, and requirements of security. The maintenance of privacy and security are the needs that are required to be acquired at the same time. This creates an insignificant trade-off between security and privacy. The resultant trade-off between security and privacy is required to be taken into accurate and proper account measures. As the network of the VANETs is self-organizing consisting of distributed, highly mobile network of nodes with number of speedy vehicles. They have explored several types of attackers which is necessary for the prevention of various types of malicious attacks. In addition to it they have also explained the attack adversaries for the indication of needs for security and privacy that must be fulfilled. The main work involves the procedure of authentication in the network by utilizing the technique of cryptography for the secure exchange of information from one node to another node without any variation of data that has been transmitted. However, the authentication scheme gets cancelled in case when the malicious attacker pretends as an authenticated entity modifying the data that has been sent or the transmitted information from other entities [4].

M.Azees1, P.Vijayakumar1, L. Jegatha Deborah in 2015 conveyed a relative analysis of numerous problems of security that occur in VANETs and have projected services of security in VANETs. they have evaluated and considered different solutions for the enhancement of availability of service in VANETs. They have offered the mechanism of privacy preservation for the enhancement of authentication performance in VANETs by

observing the few current work that is available for the confidentiality in order to preserve the data from the access user which is not authorized. Another important parameter that is required to be satisfied is the data integrity. For such feature reliability and the exactness of the network is required to be improved so that the fundamental parameter of data integrity gets fulfilled [7].

Ashritha M and Sridhar C S, 2015, proposed a mechanism considering, One of the fundamental factor that effects the efficiency of Vanets is its computation cost. The inter vehicle communication and vehicle to infrastructure communication must compute low computational cost as much as possible which intern results in mitigation of delay and latency of response in real- time. This mechanism first involves the association of vehicle with RSU. A random number sequence is generated by RSU and makes use of time stamp for the arriving vehicle. The random number sequence and the time stamp generated by RSU is operated with hash function known as symmetric key Hash Message Authentication Code (HMAC). The resultant is then transmitted to the vehicle. The vehicle receives this message and creates pseudo-id, which is sent to the RSU again. On reception of this pseudo-id, generation of real-id of the vehicle takes place by the RSU. RSU sends again RSUID, time stamp, secret key to the vehicle on authentication. The main limitation of this mechanism is number of authenticated vehicles decrease with an increase in the speed of vehicle. Since Vanets are co-related with speed and dense network which results in frequent delay of completion of authentication mechanism and limits the number of authenticated vehicles. Another limitation of this mechanism is the high computational cost [35].

Aakash Luckshetty, Sindhu Dontal, Shrikant Tangade and Sunilkumar S.Manvi in 2016 have explained the relative study of VANET attacks, its applications, security and privacy. As the VANET security needs the satisfied approach of availability, authentication, privacy, non-repudiation and data integrity. They have explained a VANET security attacks including impersonate attack where the malicious attacker transmits the information to other nodes that are participating in the network which may result in the jamming, congestion of main routes. Other attacks such as identity revealing attack where an attack

can reveal the identity of the vehicle including the details of vehicle, tracking of the location and Denial of Service (DOS) attack are considered to be mandatory as the attacker makes the authenticated user unable to access the data. In order to enhance authentication and overcome these disadvantages they have made the use of cryptographic mechanism that only allows the authenticated receiver to exchange information with the authenticated transmitter. Since in case of PKI (Public Key Infrastructure), use of key pairs for cryptography which includes the private and public keys for the secure exchange of information. However, PKI (Public Key Infrastructure) does not satisfy the main necessary parameter of VANETs as it takes a lot of time for the completion of the confirmation process [5].

Mayank Dixit et al. in 2016 have explained the fundamental architecture of VANETs, routing protocols, characteristics of the VANETs, challenges in VANETs, algorithms including the genetic algorithm and other bio-motivated methodologies which are now utilized in different circumstances of VANET applications. In addition to it they have also described the tools of simulation for VANETs. They have discussed the mechanism of information exchange between vehicles defined by the architecture of communication. They have described certain characteristics of VANETs that are challenging the boundaries of VANETs. They have categorized the different algorithms of routing to perform the mechanism of finding path of routing which is optimum from source node to the destination node [20].

Khaoula Jeffane and Khalil Ibrahimi, in 2016 explained the mechanism of detection and identification of attacks in the operating network of VANETs. This mechanism of detection and identification is established on the basis of PDR (Packet Delivery Ratio) that takes various values while performing a communication in the operating network. For ideal conditions, the packets sent from the transmitter for communication with the receiver are needed to be received at the receiver end more precisely and accurately. This condition is fulfilled when the communication between vehicles is free from obstacles. A vehicle is measured under the danger of an attack when the PDR value decreases below the optimized and fixed threshold value while travelling on the roads. By this method they can detect and

evaluate the DOS (Denial of Service) attack by utilizing the information of changing values of PDR (Packet Delivery Ratio). The main limitation of this mechanism is that it can perform the detection of an attack only till attack occurring on a vehicle is active [18].

Hong Zhong et al. in 2016 have proposed the mechanism of conditional authentication and privacy in VANETs involving information or data security that is to be communicated, user privacy, power consumption of a vehicle while performing computations. The mechanism proposed for authentication for enhancing security in VANETs can be utilized for the communication between vehicle to unit of infrastructure or vehicle to vehicle communication. The proposed mechanism involves three main phases viz initialization of the system, generation of pseudonyms and keys, signing of the transmitting message. This mechanism provides the security to the user identity of the vehicle and allows the communication of information related to the traffic in an arrangement of messages [11].

Ahmed Shoeb Al Hasan etal. in 2016 have described the solutions and mechanisms of defense for the avoidance of threats. They have also explained the privacy and security mechanisms such as the methods of public key including PKI (Public Key Infrastructure), methods of hybrid symmetry including hybrid system having both symmetric key and public key, methods of certificate revocation. In this mechanism they have described the maintenance of security by the execution of security checks when a node switches from one RSU (Road Side) to the next RSU. Use of an internet on roads for the cause of emergency execution of communication, protocols are needed to be created for the maintenance of confidentiality and the profiles of the users from malicious attackers [23].

S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang and M. K. Khan, 2017, executed a mechanism that provides a greater efficiency in VANETs for vehicle to infrastructure and vehicle to vehicle communication. Since it is more efficient to verify the several message signatures at a time rather than verifying them one by one. This mechanism requires constant pairing of numbers, computational point multiplication, free from message signature number. This mechanism involves three stages such as system initialization, unknown identity creation, signing of message, verification of message. In system

initialization, trusted authority initializes and preloads parameters of the system for each vehicle and RSU. In unknown identity creation or anonymous identity generation tamper proof device is responsible for generation of anonymous identities and message signing. In message verification, RSU or vehicle makes a check of the received message to ensure dissemination of false messages. This mechanism results in the reduction of cost, time on verification of abundant message signatures. This mechanism obtains the privacy preserving, traceability required by vehicles trust authority. It also results in the satisfaction of the security requirements which includes message authentication, non-repudiation, unforgeability, integrity, resistance to replay attacks. In addition, it provides mitigation in computation delay and transmission overhead. The major limitation of this mechanism is the less efforts to recognize the illegal signatures, as when an attacker attacks by sending a message which is invalid, this mechanism loses its efficiency [26].

From the above mentioned survey we can conclude that there are numerous disadvantage that are required to be omitted from the current technology of VANETS. However, the most necessarily requirement is the removal of limitations where time management is compromised. The main factor that leads to the improper time sequence in VANETs is the increased burden of over heads. Secondly, we have observed is the power consumption in above mentioned models. Thirdly is the cost effectiveness, as the model is required to be less costly. In our scheme we have proposed such a model where overheads are very much reduced and the power consumption will limited, which intern results in the decreased cost.

CHAPTER 5
PROPOSED METHODOLOGY

5.1 Introduction

This chapter will discuss about the technique that has been planned to solve the problem for the intelligent traffic management system operating in the form of VANETs. This technique will follow the method, phase by phase. This technique consists of phase of authentication, phase of clustering, phase of encryption and decryption to make the improvement VANETs systematically improved.

5.2 Authentication mechanism

A Bloom Filter (BF) is an assembled dataset consisting of the collection of elements that can be utilized as a check for the membership of any element in a given data set. The set containing elements are hashed with k hash functions. Each hash function provides an output which occupies a position in m-bit vector, where these k-positions are set to 1. Though, if selected element is already set to 1 on the basis of the previous attachment, these symbols are ignored and are considered to be 1. To verify the membership, the element which is to be verified is hashed with k-hash functions results in k positional vector, which is then compared with the Bloom Filter (BF). If the result derives that all k-positions are set to 1, then the given element has been approved and accepted in the membership test. The advantage of the BFs is the reduction of the overhead at the cost of false positive rate. In our methodology, we make use of standard bloom filter where k and m are selected on the basis of the numeral figure of elements of the data set (n). BF provides a support to the insertion and addition of new elements in the data set but is devoid for the support of deletion, it does not support deletion, as one symbol can be required by numerous elements. In case if all elements get deleted form the data set a new Bloom Filter is required to be constructed from the scratch. Compressed BF-deltas are used for updates when the elements of the BF are changed partially or fully in case of either deletion of elements or deletion of elements. This results an efficient and effective way of recognizing the differences amongst new BFs and old BFs with reduced overheads. Our mechanism provides an efficient way of authentication by using Bloom Filters (BFs) for the validation of vehicles on the basis of the pseudonyms. The PCA (Pseudonymous Certificate Authority) generates BFs based on the validated current existing

pseudonyms allotted to the corresponding nodes. Pseudonymous list is updated when latest pseudonyms were provided as result of the previous requests or when revocation of pseudonym occurs. Nodes are allowed to download the BF once the list is built, from the pseudonymous certificate authority (PCA). Vehicles can periodically download the latest versions form the PCA. After the completion of downloading of BF, Vehicles validate the received pseudonym with BF whose processing cost is much cheaper than the validating cost using digital signatures by the PCA (Pseudonymous Certificate Authority). In case if a pseudonym is not included in the BF and fails in the test performed by BFs for the newly allotted pseudonyms which is not included in the list, we can choose fallback approach for the validation of the vehicle. However, this fallback approach increase the probability of the risk for the entry of malicious vehicle, as an assumption all vehicles that cannot pass the test are completely neglected to follow either approach of validation. Here we assume that almost all vehicles are preloaded with pseudonyms aimed at a period Γ (e.g., 20 hours) resulting in the coverage of [tstart, tstart+Γ]. In our assumption we also assume that the pseudonyms are demanded before tstart in advance. BF is generated by PCA that contains the pseudonyms ranging [tstart, tstart + Γ]. We do not reside on the choice of tstart therefore a vehicle sends a request for pseudonyms, performs downloading of new BFs when parked. Pseudonyms can be included either in a overlapping lifetime (for example: 100 pseudonyms valid for 24 hours for each vehicle) or non-overlapping lifetime (for example: 144 pseudonyms valid for each 10minutes for each vehicle). An element is considered as the public key in the BF in the previous case while using a pseudonym, however in the second case element is considered as the combination of the corresponding pseudonym lifetime and the public key of the pseudonym. Though PCA keeps the maintenance of the counting BF, only in case of a standard BF is published. Counters are meant for the purposes of supporting deletion and insertion to the BF. BF possesses the capability of exhibiting the false positive rate, by the use of a brute force search certain fake pseudonyms were discovered that might pass the test even if they were not allotted by the Pseudonymous Certificate Authority (PCA). The solution for this is the dual verification check, so that a double check is made to verify the pseudonym. If a vehicle is verified as fake, it is informed to the VPKI (Vehicular Public Key Infrastructure) and is issued in a FPL (Fake Pseudonymous List). A Fake Pseudonymous List (FPL) consists of a detected list of fake pseudonyms that can pass the test of Bloom Filters. Authentication process using Bloom Filters to validate pseudonym involves the testing of a pseudonym from the existing available version of the BF. If the test is successful from

the BF. Second test is performed for the given pseudonym against the Fake Pseudonymous List (FPL), the pseudonym is accepted and hence validated if this given pseudonym is not present in the FP List.

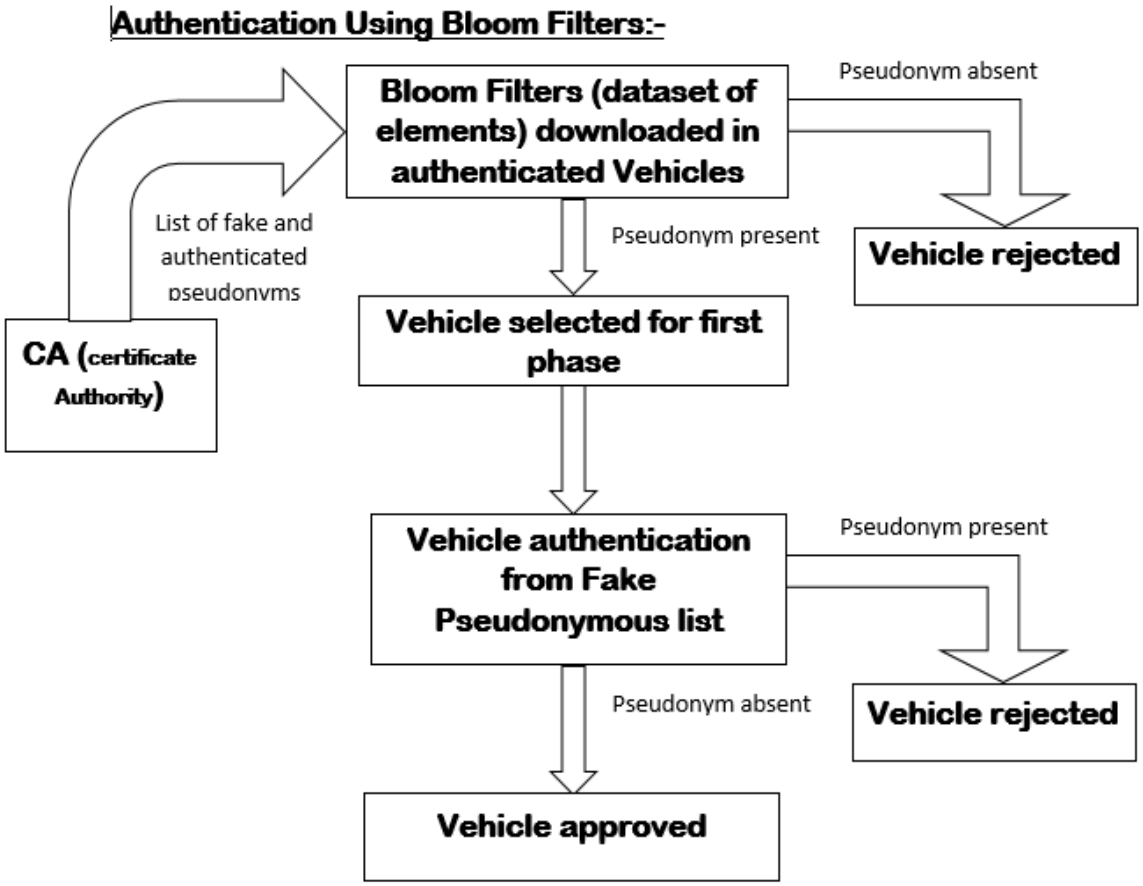

Figure 5.1 : Flow chart of authentication process.

5.3 Clustering

The Second phase of our proposed mechanism involves the clustering of the nodes. In order to overcome problems of power consumption where consideration of extra battery level intern the cost limitations are very much mitigated by selecting the group heads from the authenticated vehicles. After this a hybrid cryptographic algorithmic scheme consisting of a Elliptic Curve and Diffie-Hellman Cryptographic algorithms are executed for the secure transmission of data. The main fundamental aim of mechanism is the up-gradation of the security for the secure data

transmission. After the completion of the authentication process performed by the BFs, clustering is implemented which is briefly discussed below.

5.3.1) In this progression after validation of the nodes, we first make the choice of group heads, as group heads are chosen from numerous bunches. The group head is selected based on reliable hubs and on the previously performed communication. There is at-least one group head for each group. However the number of group heads in each bunch depends on the quantity possessed by each bunch.

5.3.2) An expert exceptional key is given to the each group head given by the certificate authority (CA). One kind of these keys are circulated by every group head to each hub.

5.3.3) An affirmation power is submitted once each individual hub gets their individual key. After the submission of an affirmation power, the certificate authority (CA) reserves the keys in its database, so that during exchange it can perform the check of the keys.

5.3.4) Now for the establishment of the communication between the source node and the destination is made when the source hub directs the demand to their neighbouring hubs together with keys. Further this neighbouring hub to its neighbouring hub until the destination is achieved. After the accomplishment of achieving the destination, it too sends the progress answer alongside the keys. By this mechanism secured data transmission is chosen for communication.

5.3.5) After the completion of choosing a path for the transmission of an information, information is encrypted before it is transmitted from the source node.

5.4 Encryption and decryption of data for the transmission between vehicles

The encryption and decryption of data for the transmission between vehicles involves following procedure. Since the VANETs is mainly concerned with the communication between vehicles. Therefore, our main goal is the secured transmission of the information from one vehicle to another vehicle. For securing the information that is to be transmitted, keys are required to be secure which are used for encrypting and decrypting the information. In our methodology, we are making use of BF authentication and clustering technique which results in the secure route for the transmission of the messages. The prime focus now is the integrity and authentication of the information or the message. To provide such secured transmission of the message our model for encryption and decryption involves the communication phase. Since our registration phase is already completed during the authentication using bloom filters and during the clustering process.

Our mechanism makes use of the ECC (Elliptic Curve Cryptographic algorithm) for the generation of key in a protected manner for the nodes forming the network from the CA (certificate authority) as ECC is responsible for generating 160-bit key for providing the security of information to the same extend as the RSA mechanism can provide for 1024-bit key. The security of the ECC (Elliptic Curve Cryptography) is influenced by the problem of ECDLP (Elliptic Curve Discrete Logarithm Problem). In case of Elliptic Curve Cryptography we use the asymmetric key mechanism of cryptography, utilized for the creation of public key and the private key. As private key is known only to the few users, however public key is known to all users participating in the network for the purpose of information exchange.

Mathematically, we can write the equation of the ECC as :

$$Z_2 = Y_3 + aY + b \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Where, $4a_3 + 27b_2 \neq 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$

Diverse elliptic curves are being utilized for various values of a and b. Here, we consider the stochastic number as the private key that remains confidential from one cluster to another unless communication is required between the two clusters. The Public key is considered as the pseudonym for the vehicle and is calculated by the multiplication of the generation point called as the generator (G) with the private number which is observed as a point on the curve, so the point is considered as the point on the elliptic curve that is to evaluated. Consider “c” as the private key then we can obtain the public key ‘Q’ as :

$$Q = c * G \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

In our mechanism of Elliptic curves, generation of keys require certain parameters viz p, a, b, G, n, h defined as the finite field domain parameters. These parameters are considered as the input parameters. From these parameters we can generate our private key and public key which are to be allocated among the vehicles participating in the network. Distribution of private key and public key among different vehicles from the RSU (roadside unit) acting as Certificate Authority (CA) involves following procedure:

5.4.1) Since the vehicles operate in a cluster format, each cluster is operating on the basis of a particular private key issued by the certificate authority. Considering a vehicle which acts as a group head sends a request message for the purpose of issuance of the private key from the CA (certification authority) in an encrypted form. As the ECC is the asymmetric

algorithm therefore, the encryption is performed by the public key issued by the certificate authority. The request message that is transmitted for the purpose of the issuing the private key comprises of the driver ID "A", vehicle ID "V1", and the parameters of the particular domain utilized for the elliptic curve cryptography and the time stamp. It can be given as :

EkCA[IDA||IDV1||(P,a,b,G,n,h)||N1]…….(4)

5.4.2) The Certificate Authority transmits the private key (cA) among the group heads of their respective clusters in the encrypted form consisting of the ID of the vehicle, ID of the driver "A".

EkCA[IDA||cA]……(5)

5.4.3) Again the group head transmits the request message for the issuance of the generator (G) to the CA (certificate authority). The request message contains the ID of the driver, time stamp N2 in an encrypted form by using the private key.

[EcA[IDA||N2]……..…..(6)

5.4.4) The CA (Certificate Authority) issues and transmits the Generator (G) to the respective group head along with ID of the vehicle "V1" and the "ID" of the driver and the amount of the time stamp (N2) in an encrypted form by utilizing the private key of "A"

[EcA[IDA||N2||G]]…….(7)

Therefore, each vehicle that are participating in the network have their private key and the public key issued by the CA (Certificate Authority). Thus, at the end of authentication performed by the bloom filters and the completion of the clustering, each vehicle gets its public key which acts as a pseudonym and the private key which is transmitted throughout the cluster by the group head.

The most essential phase of the VANET communication is the phase of the communication. When the two vehicle want to exchange an information in the same cluster or with the vehicle present in different vehicles. Here, the establishment of the communication between the source node and the destination is made when the source hub directs the demand to their neighbouring hubs together with keys. Further this neighbouring hub to its neighbouring hub until the destination is achieved. After the accomplishment of

achieving the destination, it too sends the progress answer alongside the keys. By this mechanism secured data transmission is chosen for communication. After the completion of choosing a path for the transmission of an information, information is encrypted before it is transmitted from the source node. Since, we are making use of the Elliptic Curve- Diffie Hellman (ECDH) for securing the communication between nodes where both the vehicles exchange their secret key by using this proposed algorithm. Both the vehicles perform the calculations of their shared private keys, as any malicious vehicle who is unaware about the exchanged private information between the vehicles of the cluster is unable to perform the calculations for secret key which results in the protected and secured communication between vehicles. For the secure transmission all vehicles participating in the network are required to agree all the parameters based on ECC for secret key generation. Consider a vehicle "V1" having a key pair as (cA,QA), where private key is denoted by the cA and public key is denoted by "QA". Likewise, considering an another vehicle "V2" having a key pair as (cB,QB), where public key is denoted by QB and private key is denoted by cB. Following steps are involved in the exchange of the secret key:

a) Vehicle "V2" transmits its public key QB to the vehicle "V1" , from which vehicle "V1" performs the calculations as:

$$k = (xk,yk) = cA * QB \quad \text{.....(9)}$$

b) Vehicle "V1" transmits its public key QA to vehicle "V2", from which vehicle "V2" performs the calculations as:

$$L = (xL,yL) = cB * QA \quad \text{..... (10)}$$

c) As we know from the expression of the deffie- hellman we can perform the calculations as :

$$QB = cB * G,\ QA = cA * G$$

As $dA * QB = dA * dB * G = dB * dA * G = dB * QA$

From our proposed mechanism we can conclude that the security of our information whether in terms of privacy, confidentiality, integrity or authenticity are well enhanced. Also, computation time is very much reduced as the authentication process involves the bloom filters instead of time consuming processing of digital signatures. Further, in

addition to decreased computational time, power consumption by each node is very much reduced as we are making use of clustering mechanism. Also, we are making use ECC-Deffie hellman algorithm to provide the security to the transmitted information.

The flow chart of the proposed algorithm is shown below:-

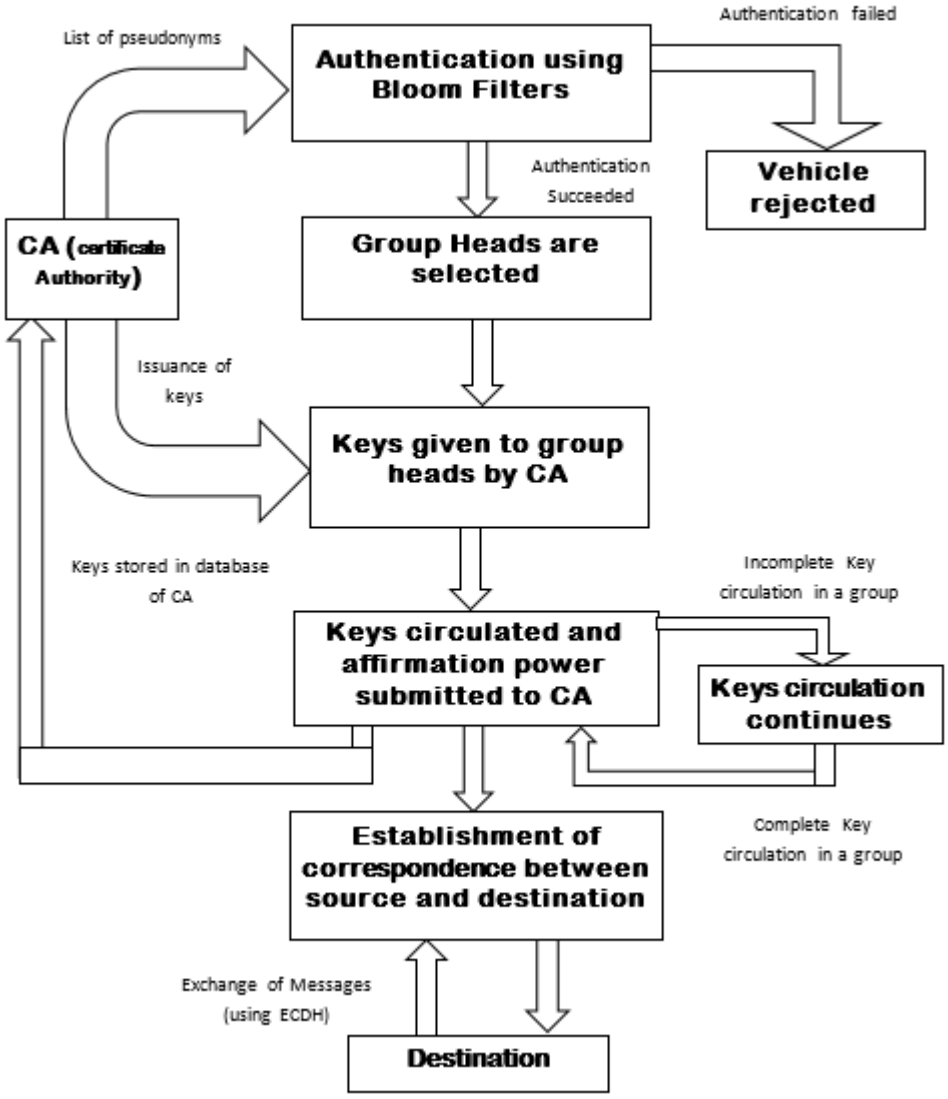

Figure 5.2 :- Flow chart of the proposed algorithm

CHAPTER 6
EXPECTED OUTCOMES

6.1 Introduction

This chapter will discuss about the result that can be obtained by imposing the proposed mechanism for the enhancement of secure transmission of data in VANETS. The parameters that gets effected by this technique include overheads, computational time, power consumption, and ultimately security of the network.

6.2 Decreased Overheads

This mechanism makes use of Bloom Filter (BF) authentication based on the pseudonym scheme. We are following the procedure of downloading the Bloom filter with a tolerable number of overheads for the efficient authentication of the pseudonyms resulting in a minimum false positive rate. Privacy and security in VANETs commands the use of short lived pseudonyms as the nodes very mobile and key-cryptographic pairs. It results in the weighty computational overheads during the procedure of secured communication between vehicles, which could place the safety of people and the vehicles in risk and threat. To overcome such a limitation we are making a use of validation approach of pseudonyms based on Bloom Filters (BFs), which provides the less number of computational overheads as compared to overheads liberating other authentication procedures without any compromise in privacy and security. It provides minimum overheads by validating pseudonyms through the use Bloom Filters (BFs), including all pseudonyms published by the Pseudonymous Certificate Authority (PCA) where these pseudonyms are valid for a particular selectable period. Once the Bloom Filter is being verified and is stored, a vehicle can authenticate itself more efficiently by mapping the pseudonym with the list of stored pseudonym providing a minimum false positive rate. In comparison to other validating procedure of Pseudonymous certificate Authority (PCA) signature for each and all pseudonyms which provides an increased level of overheads.

6.3 Decreased computational time and power consumption

The computational time parameter effects the efficiency and Quality of service in VANETs, as the nodes are mobile and are moving at a very high rate, therefore computational time is required to be balanced to operate the communication between vehicles. As the time required to complete the execution process must be reduced. Our main focus by using the clustering is the decrease of computational time and power consumption. This approach of gathering the nodes follows the selection of group head which considers the parameter of power consumption and computational time, where each group head transmits the key to their respective cluster. There are two computation times associated with clustering, when the communication between the nodes is within the cluster the resultant computational time is less as compared to the computational time required when the communication is to take place between vehicles of different clusters.

6.4 Improved routing

As the problems of efficient routing effects the reliability and scalability over a large network, is the existing issue of intense research. By implementing the approach of clustering in VANETs we can improve the reliability and scalability of routing, as the distribution of nodes in a network forming a structure by assembling the nodes with proper alignment and form groups of vehicle together on the basis of spatial correlated distribution and the velocity of the vehicles in the network.

6.5 Secure transmission

Providing the secure transmission of information from one vehicle to another vehicle is the fundamental aim of our mechanism which can be fulfilled by the implementation of ECC (Elliptic Curve Crytography) – Diffie Hellman algorithm. In the present scenario of enhancing the security of VANETs we can experience the better result by our proposed mechanism of securing the data transmission based on the BF approached secure clustering mechanism, which provides the finest security plan. As the route for transmission is being chosen on the basis of the clustering where all vehicles are authenticated, therefore these authenticated nodes taking part in the transmission provide the secured route. Furthermore, for an instance excluding the concept of secured route, we are making use of encryption and decryption algorithms based on the key pair cryptography which prevents the chance of modifying the information by a malicious attacker.

6.6 Computational Cost

By making use of ECDH (Elliptic Curve and Diffie Hellman) approach which makes use of reduced key size as compared to the RSA which makes use of increased key size although providing the same level of security. Therefore, by using ECDH our requirements of storage and computational processing will also be reduced which in turn results in the decrease of the cost.

CHAPTER 7
RESULTS AND DISCUSSION

7.1 Introduction

This chapter consists of the results and discussion obtained from the simulation of RSA and ECDH. The results will be discussed below to each simulation result. However, the implementation of our simulation are executed in MATLAB. The functionality of these cryptographic algorithm will be operated and the result will be explained briefly in this chapter.

7.2 Simulation results using RSA

```
Implementation of RSA Algorithm

Enter value of p: 11

Enter value of q: 23

The value of (N) is: 253
The public key (e) is: 3
The value of (Phi) is: 220
The private key (d)is: 147

Enter message: lovely professional university
ASCII Code of the entered Message:
  Columns 1 through 23

   108   111   118   101   108   121    32   112   114   111   102   101   115   115   105   111   110    97   108    32   117   110

  Columns 24 through 30

   118   101   114   115   105   116   121
```

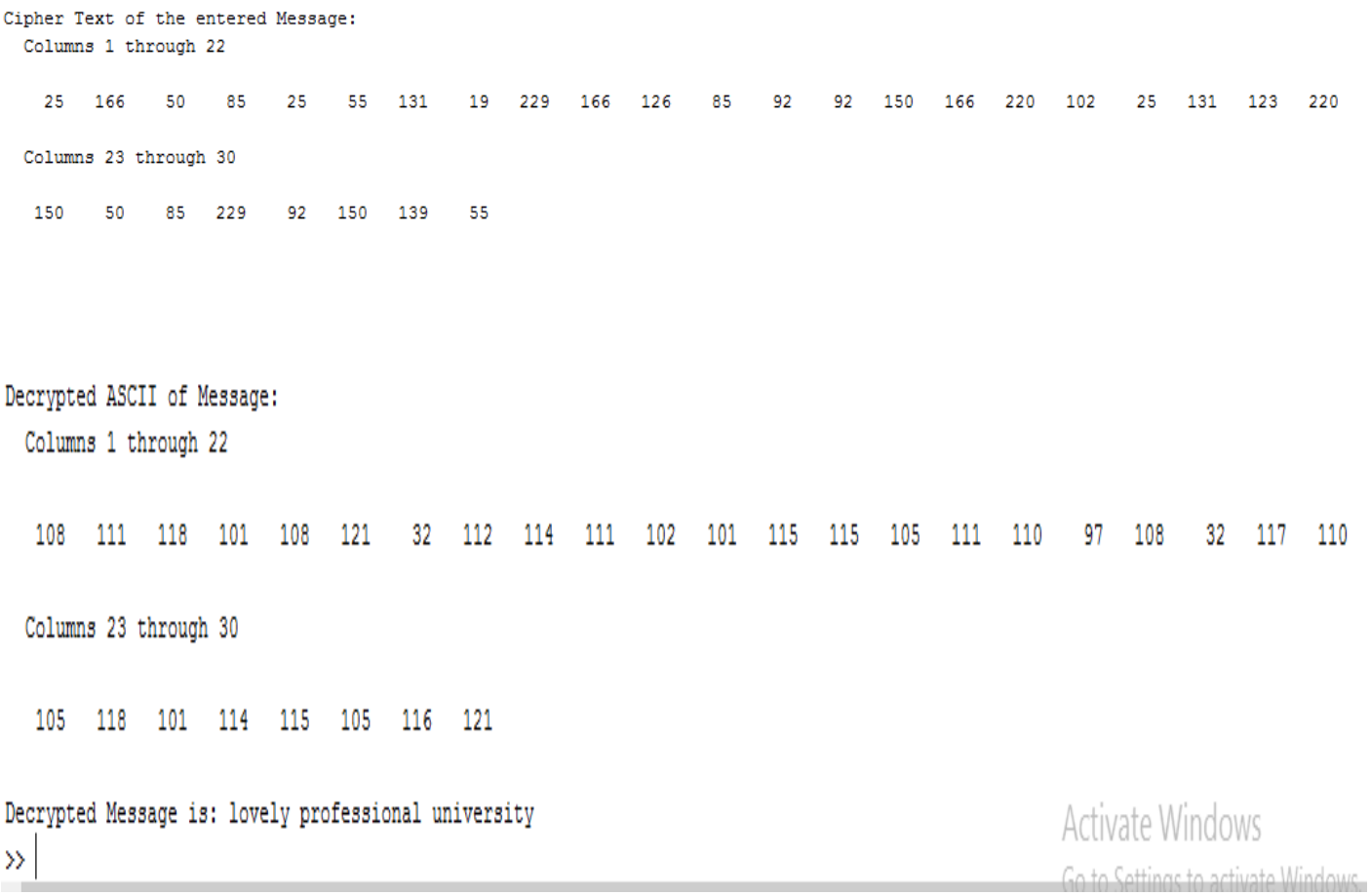

Figure 7.1 : Simulation results using RSA.

Our simulation of RSA involves the three main components which are:

7.2.1 Determination of private and public keys that are to be use for encryption and decryption.

7.2.2 Algorithm for encryption.

7.2.3 Algorithm for decryption.

7.2.1 Determination of private and public keys

Above simulation is performed under following procedure for determining the keys:

a) Two numbers p and q are selected, which are difinitely choosen to be the prime numbers (more larger the prime numbers more it will be challenging to disclose the cipher)

b) Next we perform the computation of p and q such that

$$N = p*q$$

c) Another computation of Phi is computed as

$$Phi = (p-1)*(q-1)$$

d) We choose the value of an integer e such that e < phi and must be prime relatively to phi. This value of e forming a pair with N is sent as a public key.

e) Now we perform the compuations of an integer e such that

$$d = e^{-1} \pmod{(phi)}.$$

This value of d forming a pair with N is considered as a private key.

Now we display these computed values of N, Phi, e and d

7.2.2 Algorithm for encryption

Now we perform the encryption of the message by using the public key as (e,n), where the computation for the ciphertext is calculated as:

$$Ciphertext = (Message)^e \bmod n.$$

7.2.3 Algorithm for decryption

We can obtain the plaintext by performing the computation of ciphertext by using the private key as:

$$Message = (Ciphertext)^d \bmod n.$$

7.3 Simulation results by using ECC-Diffie Hellman (ECDH)

```
enter the value of a 2
enter the value of b 2
0010
0010
enter the value of private number by alice 13

pa =

   442

pb =

   578

k1 =

        7514
```

```
k2 =

       7514
```

```
Enter message: lovely professional university
ASCII Code of the entered Message:
  Columns 1 through 22

   108   111   118   101   108   121    32   112   114   111   102   101   115   115   105   111   110    97   108    32   117   110

  Columns 23 through 30

   105   118   101   114   115   105   116   121
```

```
z =

   108

l =

      4343200

z =

   111

l =

      4343200      4343203

z =

   118

l =

      4343200      4343203      4343210

z =
```

```
   101

l =

     4343200     4343203     4343210     4343193

z =

   108

l =

     4343200     4343203     4343210     4343193     4343200

z =

   121

l =

     4343200     4343203     4343210     4343193     4343200     4343213

z =

    32

l =

     4343200     4343203     4343210     4343193     4343200     4343213     4343124

z =

   112

l =

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204

z =

   114

l =
```

```
     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206

z =

   111

l =

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203

z =

   102

l =

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

z =


   101

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Column 12

     4343193

z =

   115

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194
```

```
  Columns 12 through 13

     4343193     4343207

z =

   115

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 14

     4343193     4343207     4343207

z =

   105

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 15

     4343193     4343207     4343207     4343197

z =

   111

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 16
```

```
    4343193    4343207    4343207    4343197    4343203

z =

   110

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 17

    4343193    4343207    4343207    4343197    4343203    4343202

z =

    97

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 18

    4343193    4343207    4343207    4343197    4343203    4343202    4343189

z =

   108

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 19

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200
```

```
z =

    32

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 20

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124

z =

   117

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 21

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209

z =

   110

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 22

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209    4343202

z =

   105
```

```
l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 22

     4343193     4343207     4343207     4343197     4343203     4343202     4343189     4343200     4343124     4343209     4343202

  Column 23

     4343197

z =

   118

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 22

     4343193     4343207     4343207     4343197     4343203     4343202     4343189     4343200     4343124     4343209     4343202

  Columns 23 through 24

     4343197     4343210

z =

   101

l =

  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 22

     4343193     4343207     4343207     4343197     4343203     4343202     4343189     4343200     4343124     4343209     4343202

  Columns 23 through 25
```

```
    4343197    4343210    4343193

z =

   114

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 22

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209    4343202

  Columns 23 through 26

    4343197    4343210    4343193    4343206

z =


   115

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 22

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209    4343202

  Columns 23 through 27

    4343197    4343210    4343193    4343206    4343207

z =

   105

l =

  Columns 1 through 11
```

```
    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 22

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209    4343202

  Columns 23 through 28

    4343197    4343210    4343193    4343206    4343207    4343197

z =

   116

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 22

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209    4343202

  Columns 23 through 29

    4343197    4343210    4343193    4343206    4343207    4343197    4343208

z =

   121

l =

  Columns 1 through 11

    4343200    4343203    4343210    4343193    4343200    4343213    4343124    4343204    4343206    4343203    4343194

  Columns 12 through 22

    4343193    4343207    4343207    4343197    4343203    4343202    4343189    4343200    4343124    4343209    4343202

  Columns 23 through 30

    4343197    4343210    4343193    4343206    4343207    4343197    4343208    4343213

Cipher Text of the entered Message:
```

```
  Columns 1 through 11

     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194

  Columns 12 through 22

     4343193     4343207     4343207     4343197     4343203     4343202     4343189     4343200     4343124     4343209     4343202

  Columns 23 through 30

     4343197     4343210     4343193     4343206     4343207     4343197     4343208     4343213

transmitted data:
  Columns 1 through 11
     4343200     4343203     4343210     4343193     4343200     4343213     4343124     4343204     4343206     4343203     4343194
  Columns 12 through 22
     4343193     4343207     4343207     4343197     4343203     4343202     4343189     4343200     4343124     4343209     4343202
  Columns 23 through 31
     4343197     4343210     4343193     4343206     4343207     4343197     4343208     4343213      255476

Decrypted ASCII of Message:
  Columns 1 through 22
    108   111   118   101   108   121    32   112   114   111   102   101   115   115   105   111   110    97   108    32   117   110
  Columns 23 through 30
    105   118   101   114   115   105   116   121

ans =

lovely professional university
```

Figure 7.2: ECDH key exchange with encryption and decryption.

7.3.1 Exchange of keys by using elliptic curves is accomplished in the folllowing way as given below :

We are considering a large integer q which must fulfill either the condition of being a prime number or must be of the form 2^m and the elliptic curve parameters u, v for the euation given as:

$$y^2 = x^3 + ux + v$$

Or $$y^2 + xy = x^3 + ux^2 + v$$

These two equations describe the elliptic group of points $E_q(u,v)$

Now we are selecting a base point g = (a, b), considered as a point on the elliptic curve. Further the exchange of keys using ECDH from one user A to another user B is accomplished by performing these simulations.

The user A chooses a value for 'na' as an integer. This value of na is chosen as the private key for user A. User A also generates the public key by the calculations performed as :

$$Pa = na * g$$

Like wise we peform the similar computations for user B by selecting an integer nb and calculating the value for public key as:

$$Pb = nb * g$$

Calculations are performed by the user A and user B for evaluating the secret key as:

By user A

$$K1 = na * Pb$$

By user B

$$K2 = nb * Pa$$

7.3.2 Encryption and decryption process:

For the encryption of the message 'M' and we perform the calculations using the keys K1 by the user A and creates the ciphertext as consisting of the calculation for pair of points:

Ciphertext = [y , l]

Where y = K1* g,

l = z + v ; z = C(j) : j = 1, 2,…. Length of the message, v = K1* Pb.

Where C(j) denotes the ASCII code for the transmitting message M.

For decryption of the message user B performs the following calculations:

$$z + v - nb * (y) = z + K2*(nb*g) - nb\ (K1*g)$$
$$= z$$
$$= C(j)$$
$$= M$$

Where M is the required message at the reciever end of the user B.

CHAPTER 8
SUMMARY AND CONCLUSION

Security of data that is to be transmitted is very fundamental measure towards the safety application of Vehicular Ad-hoc Network. Critical and serious challenges of unsteady topologies and the alignment of uncoordinated transmission of data arises because of the distributed and mobile nature of VANETs. Since the wireless standard has shown the fundamental part form last few years in the field of communication. VANETs (Vehicular Ad-hoc Networks) being a part of such an essential area where the vehicles are provided with the capability of exchanging an information from one vehicle to another vehicle or from one vehicle to the road side unit (RSU) in the network. An important and fundamental issue related to VANETs is the security which is compromised by the highly mobile nodes of the network. Thus this issue is required to be resolved as the network of the VANETs provide both the non-safety and safety applications to the user of the vehicle. Diverse research on the security of VANETs have been imposed by the researchers however, there still remains an issue of communication of the message. To overcome such limitations in VANETs we propose a model where RSU (Road Side Unit) performs as the CA (Certificate Authority) generating the pseudonyms, keys and the selects the group heads among the clusters. We have proposed a latest secure transmission mechanism involving the proper authentication by using Bloom Filters (BF) based on a pseudonyms, secure route formation by performing the mechanism of clustering and finally the secure transmission of information is achieved by the implementation of ECC-Diffie Hellman algorithm. Therefore, proposing a mechanism where our network of vehicles possesses the capability of enhancing the security of VANETs and enabling the secure transmission of information without the effect of any intruder. The keys are generated by the CA using the phenomenon of ECC (Elliptic Curve Cryptography), whereby, transmission of an information from one vehicle to another vehicle takes place by using the phenomenon of Elliptic Curve - Diffie Hellman (ECDH). In our mechanism our basic aim is the secure and proficient communication in the network of VANETs. Our mechanism involves the three phases. Our first phase involves the authentication of the vehicles using BF (Bloom Filters). Our second major phase involves the formation of clusters and selection of group heads, and our third main phase involves the communication phase, where the key is shared between vehicles that are taking part in the communication involving two different clusters. The communication phase

makes use of ECDH which results in the less computational cost as the key size in case of ECDH is much less than the RSA, although providing the same level of security. Thus, our proposed model offers more enhanced and proficient model of security in VANETs where two nodes accomplish the secure communication.

REFERENCES

[1] B. Zhang, X. Jia, K. Yang and R. Xie, "Design of Analytical Model and Algorithm for Optimal Roadside AP Placement in VANETs," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7708-7718, Sept. 2016.

[2] C. Cooper, D. Franklin, M. Ros, F. Safaei and M. Abolhasan, "A Comparative Survey of VANET Clustering Techniques," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 657-681, Firstquarter 2017.

[3] L. Bariah, D. Shehada, E. Salahat and C. Y. Yeun, "Recent Advances in VANET Security: A Survey," 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, 2015, pp. 1-7.

[4] F. Qu, Z. Wu, F. Y. Wang and W. Cho, "A Security and Privacy Review of VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, Dec. 2015.

[5] A Security and Privacy Review of VANETs FengzhongQu, Senior, Zhihui Wu, Fei-Yue Wang, and Woong Cho, IEEE 2015

[6] Review Article Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rong fang Bie College of Information Science and Technology, Beijing Normal University, Beijing100875, China, International Journal of Distributed Sensor Networks Volume 2015, Article ID 745303.

[7] A Comprehensive Survey on Security Services in Vehicular Ad-Hoc Networks (VANETs) M.Azees1, P.Vijayakumar1,*, L.Jegatha Deborah1 1 Department of Computer Science and Engineering, University College of Engineering Tindivanam, Melpakkam, Tamilnadu, India-604 001

[8] Global Journal of Computer Science and Technology GJCST Computing Classification C 2.1, C 2.m VANET Parameters and Applications: A Review Kamini1 Rakesh Kumar2

[9] Applications of VANETs: Present & Future Vishal Kumar1, Shailendra Mishra1, Narottam Chand.

[10] C. Wu, S. Ohzahata, Y. Ji and T. Kato, "How to Utilize Interflow Network Coding in VANETs: A Backbone-Based Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2223-2237, Aug. 2016.

[11] H. Zhong, J. Wen, J. Cui and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," in Tsinghua Science and Technology, vol. 21, no. 6, pp. 620-629, Dec. 2016.

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

[13] M. Hashem Eiza, T. Owens and Q. Ni, "Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETs," in IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 1, pp. 32-45, Jan.-Feb. 1 2016.

[14] Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan -2012

[15] Vehicular Ad hoc Networks (VANET) Engineering and simulation of mobile ad hoc routing protocols for VANET on highways and in cities Rainer Baumann, ETH Zurich 2004

[16] Y. Xie, L. Wu, Y. Zhang and J. Shen, "Efficient and Secure Authentication Scheme with Conditional Privacy-Preserving for VANETs," in Chinese Journal of Electronics, vol. 25, no. 5, pp. 950-956, 9 2016.

[17] A. Wasef, R. Lu, X. Lin and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]," in IEEE Wireless Communications, vol. 17, no. 5, pp. 22-28, October 2010.

[18] K. Jeffane and K. Ibrahimi, "Detection and identification of attacks in Vehicular Ad-Hoc NETwork," 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, 2016, pp. 58-62.

[19] R. Hajlaoui, H. Guyennet and T. Moulahi, "A Survey on Heuristic-Based Routing Methods in Vehicular Ad-Hoc Network: Technical Challenges and Future Trends," in IEEE Sensors Journal, vol. 16, no. 17, pp. 6782-6792, Sept.1, 2016.

[20] M. Dixit, R. Kumar and A. K. Sagar, "VANET: Architectures, research issues, routing protocols, and its applications," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 555-561.

[21] D. Huang, S. Misra, M. Verma and G. Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 3, pp. 736-746, Sept. 2011.

[22] H. Sedjelmaci, S. M. Senouci and M. A. Abu-Rgheff, "An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks," in IEEE Internet of Things Journal, vol. 1, no. 6, pp. 570-577, Dec. 2014.

[23] A. S. A. Hasan, M. S. Hossain and M. Atiquzzaman, "Security threats in vehicular ad hoc networks," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, 2016, pp. 404-411.

[24] D. B. Rawat, M. Garuba, L. Chen and Q. Yang, "On the security of information dissemination in the Internet-of-Vehicles," in Tsinghua Science and Technology, vol. 22, no. 4, pp. 437-445, Aug. 2017.

[25] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari and A. Tyagi, "Vehicular Security Through Reputation and Plausibility Checks," in IEEE Systems Journal, vol. 8, no. 2, pp. 384-394, June 2014.

[26] S. F. Tzeng, S. J. Horng, T. Li, X. Wang, P. H. Huang and M. K. Khan, "Enhancing Security and Privacy for Identity-Based Batch Verification Scheme in VANETs," in IEEE Transactions on Vehicular Technology, vol. 66, no. 4, pp. 3235-3248, April 2017.

[27] B. Pradeep, M. M. M. Pai, M. Boussedjra and J. Mouzna, "Global Public Key Algorithm for secure location service in VANET," 2009 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST), Lille, 2009, pp. 653-657.

[28] A. Wasef, R. Lu, X. Lin and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]," in IEEE Wireless Communications, vol. 17, no. 5, pp. 22-28, October 2010.

[29] J. T. Isaac, S. Zeadally and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," in IET Communications, vol. 4, no. 7, pp. 894-903, April 30 2010.

[30] G. Yan, S. Olariu and M. C. Weigle, "Providing location security in vehicular Ad Hoc networks," in IEEE Wireless Communications, vol. 16, no. 6, pp. 48-55, December 2009.

[31] R. Lu, X. Lin, T. H. Luan, X. Liang and X. Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," in IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.

[32] Q. Li, A. Malip, K. M. Martin, S. L. Ng and J. Zhang, "A Reputation-Based Announcement Scheme for VANETs," in IEEE Transactions on Vehicular Technology, vol. 61, no. 9, pp. 4095-4108, Nov. 2012.

[33] Efficient Selective Identity-Based Encryption Without Random Oracles, Dan Boneh, Xavier Boyen, JCryptol-2011.

[34] Security Proofs for Identity-Based Identification and Signature Schemes Mihir Bellare1 , Chanathip Namprempre2 , and Gregory Neven, J-Cryptol-2009.

[35] Ashritha M and Sridhar C S, "RSU based efficient vehicle authentication mechanism for VANETs," 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2015, pp. 1-5.

[36] M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 9, pp. 2467-2476, Sept. 2017.

[37] M. C. Chuang and J. F. Lee, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks," in IEEE Systems Journal, vol. 8, no. 3, pp. 749-758, Sept. 2014.

[38] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[39] M. Nema, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-5.

[40] Y. Liu, L. Wang and H. H. Chen, "Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 64, no. 8, pp. 3697-3710, Aug. 2015.

LIST OF ABBREVIATIONS

VANET – Vehicular Ad-hoc Network

GPS – Global Positioning System

WLAN – Wireless Local Area Network

OBU – On Board Unit

RSU – Road Side Unit

TMC – Traffic Management Center

TA – Traffic Authority

RADAR – Radio Detection and Ranging

LASER – Light Amplification by Stimulated Emission of Radiation

DSRC – Dedicated Short Range Communication

WAVE – Wireless Access for Vehicular Environment

RCP – Resource Command Processor

TPD – Tamper Proof Device

EDR – Event Data Recorder

SVA – Slow or Stop Vehicle Advisor

CRN – Congested Road Notification

PAN – Parking Availability Notification

MPR – Multi-point Relay

OLSR – Optimized Link State Routing Protocol

FSR – Fisheye State Routing

TDRPF – Topology Dissemination based on Reverse Path Forwarding

DSR – Dynamic Source Routing Protocol

AODV – Ad-hoc on Demand Distance Vector

ZRP – Zone Routing Protocol

VBE – Vehicular Behavior Evaluation

HMAC – Hash Message Authentication Code

PDR – Packet Delivery Ratio

ECDH – Elliptic Curve Diffie Hellman

ECC – Elliptic Curve Cryptography

PROPOSED WORK WITH TIMELINE

Week **Month**	**Week-1**	**Week-2**	**Week-3**	**Week-4**
August	Studied various challenges of VANETs	Studied designs on Authentication procedures	Studied designs on authentication procedures with less computational time	Finalized authentication procedure for our mechanism
September	Studied various implementations to reduce power consumption and overheads	Compared various designs that can reduce power	Finalized the procedure for the reduction of overheads and power consumption	Integrating the procedure of reducing power and overheads with the reduced computational time procedure
October	Encryption and decryption algorithms for information exchange	Identifying the drawbacks of the implemented algorithms	Comparison of the different algorithms	Finalizing the encryption and decryption algorithm
November	Review paper	Review paper finalization and submission	Report writing	Report writing